

F R A N S K E U N E

NUMBER FIELDS

**RADBOUD
UNIVERSITY
PRESS**

Number Fields

Frans Keune

Number Fields

Published by RADBOUD UNIVERSITY PRESS

Postbus 9102, 6500 HC Nijmegen, the Netherlands

www.radbouduniversitypress.nl | www.ru.nl/radbouduniversitypress

radbouduniversitypress@ru.nl

Cover design: Frans Keune and Textcetera, The Hague. The design is based on the golden ratio

Print and distribution: Pumbo.nl

Version: 2023-01

Mathematics Subject Classification (2020): 11-01, 11Rxx, 11Sxx

ISBN: 978 94 9329 603 9

DOI: 10.54195/IPVU4488

Free download at: www.radbouduniversitypress.nl

© 2023, Frans Keune

**RADBOUD
UNIVERSITY
PRESS**

This is an Open Access book published under the terms of Creative Commons Attribution-Noncommercial-NoDerivatives International license (CC BY-NC-ND 4.0). This license allows reusers to copy and distribute the material in any medium or format in unadapted form only, for noncommercial purposes only, and only so long as attribution is given to the creator, see <https://creativecommons.org/licenses/by-nc-nd/4.0/>.

Although the utmost care has been taken in the creation of this publication, the author and the publisher accept no liability for any errors and imperfections, nor for the direct or indirect consequences thereof.

Contents

Preface	ix
Introduction	xi
I Basic Algebraic Number Theory	1
1 Integers in a Number Field	3
1.1 Number fields	3
1.2 Algebraic integers	6
1.3 Norm, trace and characteristic polynomial	9
1.4 The norm on a number field	12
1.5 The discriminant	14
1.6 The additive group of the ring of integers of a number field	18
1.7 Norm-Euclidean quadratic number fields	26
Exercises	29
2 Dedekind Domains	33
2.1 Definition	33
2.2 Factorization of ideals	36
2.3 The ideal class group of a Dedekind domain	40
2.4 Fractional ideals	42
2.5 Characterization of Dedekind domains	44
Exercises	47
3 Rings of Integers of Number Fields	49
3.1 Prime ideals	49
3.2 The norm of an ideal	57
3.3 The ideal class group of a number field	59
3.4 Ramification	60
Exercises	62
4 Quadratic Number Fields	65
4.1 The Quadratic Reciprocity Law	65
4.2 Equivalence of quadratic numbers	70
4.3 Equivalence of lattices in \mathbb{C}	73

4.4	Algorithm for the ideal class group of an imaginary quadratic number field	75
4.5	Continued fractions	79
4.6	Continued fraction expansions of real quadratic numbers	84
4.7	Algorithm for the ideal class group of a real quadratic number field	89
4.8	Algorithm for the fundamental unit of a real quadratic number field	92
4.9	The 2-rank of the ideal class group	95
	Exercises	103
5	Geometric Methods	105
5.1	Discrete subgroups of \mathbb{R}^n	105
5.2	Minkowski theory	107
5.3	The Minkowski bound	107
5.4	Dirichlet's Unit Theorem	115
5.5	Regulators	127
	Exercises	129
6	Localization of Dedekind Domains	131
6.1	Discrete valuations	131
6.2	Localization at a prime ideal	133
6.3	Localization at a collection of prime ideals	137
6.4	Localizations of rings of integers of number fields	141
	Exercises	141
7	Extensions of Dedekind Domains	145
7.1	Ramification index, residue class degree	145
7.2	Ramification and discriminant	155
7.3	Decomposition groups and inertia groups	160
7.4	The splitting of a prime ideal in an extension	166
7.5	Ramification groups	169
7.6	Norms of fractional ideals	173
7.7	The Frobenius automorphism of a prime ideal	177
7.8	Galois groups of polynomials and reduction modulo a prime ideal	180
	Exercises	182
8	Analytic Methods	185
8.1	Counting lattice points in a bounded domain	185
8.2	The distribution of ideals over the ideal classes	187
8.3	Dirichlet series	191
8.4	The Dedekind zeta function of a number field	198
8.5	Dirichlet density	201
8.6	Frobenius Density Theorem	206
	Exercises	208

9	Abelian Number Fields	209
9.1	The Kronecker-Weber Theorem	209
9.2	Characters of finite abelian groups	215
9.3	Dirichlet characters	218
9.4	Classification of abelian number fields	222
9.5	Dirichlet L-series	226
9.6	The Gauß sum of a Dirichlet character	232
9.7	The Gauß sum of a quadratic Dirichlet character	234
9.8	Class number formulas	240
9.9	Cyclotomic units	246
	Exercises	251
II	Class Field Theory	253
10	Completions of Number Fields	255
10.1	Absolute values	255
10.2	Completions	261
10.3	Complete archimedean fields	263
10.4	Primes of a number field	265
10.5	Completions of discretely valued fields	269
10.6	Extensions of complete discretely valued fields	272
10.7	Completions of field extensions	274
	Exercises	277
11	Local Fields	279
11.1	Local fields of characteristic 0	279
11.2	The multiplicative group	281
11.3	Extensions	283
11.4	Exponential function and logarithm	285
11.5	The multiplicative group	289
	Exercises	290
12	Galois Modules	293
12.1	Modules over a group	293
12.2	Cohomology of cyclic groups	296
12.3	Galois cohomology of cyclic groups	300
12.4	Galois modules and transfers	305
12.5	$C_p \times C_p$ -Modules	310
12.6	$C_p \rtimes C_q$ -Modules	312
	Exercises	316
13	Ray Class Groups and Dirichlet Characters	319
13.1	Ray class groups	320

13.2 Dirichlet characters of a number field	329
13.3 Counting ideals in ray classes	334
13.4 Dirichlet L-series and the First Fundamental Inequality	337
13.5 The Artin map	340
Exercises	344
14 Artin's Reciprocity Law	347
14.1 The Fundamental Equality	347
14.2 Hasse's Principle	355
14.3 Artin's Reciprocity Law	356
14.4 The dual Artin isomorphism and class fields	361
Exercises	365
15 The Classification Theorem	367
15.1 Reduction steps	367
15.2 Kummer extensions	371
15.3 The Existence Theorem	374
15.4 Chebotarev's Density Theorem	381
15.5 The Complete Splitting Theorem	383
15.6 Local Artin maps	387
15.7 Generalized Artin maps and the group transfer	393
15.8 The Hilbert class field	399
Exercises	405
16 Local Class Fields and Symbols	407
16.1 Local class fields	407
16.2 Norm residue symbols	415
16.3 Hilbert symbols	416
16.4 Power residue symbols	423
16.5 Some classical reciprocities	426
Exercises	435
17 Conductor and Discriminant	437
17.1 Ramification groups of a subextension	437
17.2 The different	448
17.3 Local Artin maps and ramification groups	457
17.4 The Conductor-Discriminant Formula	466
Exercises	469
18 Zeta Function Relations	471
18.1 Norm relations	471
18.2 Norm relations for abelian groups	477
18.3 Relations for Dedekind zeta functions	484
18.4 Some remarks on Artin L-functions	492

18.5 Strongly exceptional groups	497
Exercises	502
19 Infinite Extensions of Number Fields	505
19.1 Infinite products of topological spaces	505
19.2 Topological groups	508
19.3 Inductive and projective limits	510
19.4 Profinite groups	520
19.5 Infinite Galois extensions	524
19.6 Duality	529
Exercises	532
20 Idèlic Class Field Theory	533
20.1 The adèle ring of a number field	533
20.2 The idèle group and the idèle class group	536
20.3 Idèle class groups and moduli	540
20.4 The Classification Theorem (idèlic version)	543
20.5 Local and global reciprocity	548
Exercises	550
References	551
Notations	553
Index	563

Preface

This book is a textbook for algebraic number theory. It grew out of lecture notes of master courses taught at the Radboud University over a period of more than four decades. It is self-contained in the sense that it uses only mathematics of a bachelor level, including some Galois theory, as for example treated in *Galois Theory* [35]. To some extent the language of categories is used, especially in later chapters.

Part I contains topics in basic algebraic number theory as they may be presented in a beginning master course on algebraic number theory. The theory in Part II is more advanced. It contains in particular full proofs of the main theorems of class field theory using a ‘classical’ approach to class field theory, which is in a sense a natural continuation of the basic theory in Part I. The advantage for students is that no more prerequisites are needed. Each approach has its own advantages, so for specialists in algebraic number theory it is advisable to have knowledge of more than just one. For specialists of other areas of pure mathematics who want to use it, the exposition as given here might very well suffice. The last two chapters provide the connection to the more modern and more advanced idèlic version of class field theory.

It is not the purpose of this book to present up to date information on the state of the art. The section References is just what it says: it contains references made in the text and is not an exposition of the vast literature on the subject.

Many students were so kind to report on typos. Merlijn Keune has read large parts of the manuscript and I profited a lot of his dozens of comments. Undoubtedly, several typos and errors remained undetected. Suggestions for improvements are welcome: keune@math.ru.nl.

Nijmegen, February 2023

Frans Keune

Introduction

Number theory is a part of mathematics and is as old as mathematics itself. Many number problems come down to solving algebraic equations in integers. Their solutions are algebraic numbers. This has led to the introduction of abstract algebraic structures such as groups, rings, fields and modules. Abstract algebra dates from the beginning of the nineteenth century and developed rapidly since then. As a result the focus in number theory shifted from algebraic numbers to (algebraic) number fields, finite extensions of the field of rational numbers. The study of algebraic structures arising in number theory is known as algebraic number theory.

A deep and highly developed part of algebraic number theory is class field theory, a theory of the abelian extensions of number fields. Its origin lies in the various reciprocity laws discovered in the nineteenth century, the oldest being the well-known quadratic reciprocity law of Gauß, which is strongly related to quadratic number fields, quadratic extensions of the rationals. For the field of rational numbers as the base field the theorem of Kronecker and Weber is fundamental: every abelian number field is a subfield of a cyclotomic field. For an arbitrary number field as base field the situation is much more complicated. How to generalize already is a problem, proving the generalization is an even bigger problem. All of this was realized by Takagi and Artin in the first half of the twentieth century. Later, new insights have led to new and powerful approaches, especially via group cohomology.

For the transfer of mathematical knowledge to students choices have to be made for the level of abstraction, especially in case of a subject with a long history. Unlike other sciences, mathematics is cumulative: what has been shown to be true remains true forever. Luckily however, the organization of mathematics does change. New insights lead to new concepts and more efficient, more elegant proofs. For a student this means that there is no need to digest the complete history of a theory. On the other hand, to master a highly developed theory, it is advisable for reasons of motivation to have it somehow based on its origins. At the same time one can profit from knowledge of modern concepts as they are nowadays standard in the mathematics curriculum of a university. This is the main idea behind the organization of this textbook.

In developing a course choices have to be made at which stage to introduce new concepts. For algebraic number theory this applies especially to notions of localization, Dedekind domain, discriminant, different, completion, zeta function, group

cohomology and idèle. In this book a new concept is introduced at the moment it makes a real difference to have it available. Further features are:

- In chapter 2 is chosen for a definition of a Dedekind domain which is directly related to the unique factorization property of nonzero ideals.
- Quadratic number fields get special attention. In chapter 4 algorithms are given for their ideal class groups as well as for the fundamental unit in the real quadratic case. Based on these algorithms the formula for the 2-rank of the ideal class group is derived. This computation is quite technical. A second proof is in the exercises of chapter 12. Using class field theory the formula is easily derived: a third proof is in chapter 15, showing the power of class field theory.
- Localization of Dedekind domains is defined in chapter 6 using discrete valuations of the field of fractions. It is used in the next chapter when studying the relative case of an extension of number fields: decomposition, inertia and ramification groups, Frobenius automorphisms. This all will be used for the theory of abelian number fields in chapter 9. For later use the theory is given in a more general algebraic setting: extensions of Dedekind domains, not just of rings of integers of number fields.
- Analytic methods are introduced in chapter 8, especially the theory of zeta and L -functions. They are used for class number formulas for abelian number fields in chapter 9. Analytic methods are used in later chapters on class field theory as well.
- Chapter 9 is devoted to abelian number fields. It contains a proof of the Kronecker-Weber Theorem: every abelian field is contained in a cyclotomic field. The proof uses ramification groups and discriminants. In chapter 15 this theorem will be just an easy example in class field theory. Chapter 9 contains the classification of abelian number fields by finite groups of Dirichlet characters. Class number formulas for abelian number fields are derived using Gauß sums of Dirichlet characters.
- The chapters 10, 11 and 12 prepare for class field theory. In chapter 10 the completion of valued fields is treated in a general setting and in chapter 11 local fields are studied. Chapter 12 is about the Galois cohomology for cyclic groups. It contains computations needed in the proofs of the main theorems of class field theory in later chapters. Only a small self-contained part of group cohomology is needed for the proofs of the main theorems of class field theory.
- Global class field theory is treated in the chapters 13, 14 and 15. Dirichlet characters of number fields are defined as characters on the monoid of nonzero ideals of the ring of integers. By focussing on primitive Dirichlet characters, it

is often possible to suppress the choice of a modulus of the field. It generalizes the use of Dirichlet characters of the field \mathbb{Q} in chapter 9.

- Local class field theory is derived as a consequence of global class field theory. Local fields are introduced in chapter 11, the local Artin map in chapter 15. Local class field theory is treated in chapter 16, where it is applied to Hilbert symbols. It is shown how classical reciprocity theorems follow from global class field theory via Hilbert's Reciprocity Theorem.
- In chapter 17 the behavior of ramification under restriction to a subextension is treated. The close connection between ramification groups and local Artin maps is described. It uses the different of an extension, which is defined for this purpose in this chapter. The Conductor-Discriminant Formula for an abelian extension is proved. It expresses the discriminant as the product of the conductors of the associated Dirichlet characters.
- The Brauer-Kuroda formula is a relation between the Dedekind zeta functions of the intermediate fields of a Galois extension of number fields. The formula is derived in chapter 18 by direct computation using the Euler products expressing the Dedekind zeta functions. It is based on a study of the relations between the norms of subgroups in the group ring of a finite group. Though Artin L -functions of Galois extensions of number fields are introduced, here they are not used in the proof of the Brauer-Kuroda formula.
- In the last chapter, chapter 20, the idèlic Global Classification Theorem is derived from the ideal-theoretic version in chapter 15. It is used to clarify the connection between global and local reciprocity. The main tools used in the theory based on idèles are treated in chapter 19: some topological algebra and in particular profinite groups. Moreover, in this chapter results on finite number field extensions are extended to infinite algebraic extensions.

Examples of excellent textbooks on algebraic number theory are *Number Fields* [28] by D.A. Marcus and *Algebraic number theory* [12] by A. Fröhlich and M.J. Taylor. In [28] localization and completion are avoided, whereas in [12] these concepts form a fundamental part of the theory. Both [28] and [12] contain a treatment of zeta functions and L -functions. The last chapters of these books contain an introduction to respectively class field theory (in [28]) and an exposition of Artin L -functions (in [12]). *Algebraic Theory of Numbers* [33], a translation from the French [32], by P. Samuel is a well written concise introductory text on algebraic number theory and includes the necessary Galois theory. Another good textbook is *Number Theory* [3] by Z.I. Borevich and I.R. Shafarevich, translated from the originally Russian text. It contains a lot of interesting information on the subject.

There are various approaches to global class field theory, the theory of abelian extensions of a number field. The modern way is by using idèles. This concept was introduced by Chevalley and is especially useful for the passage from local to global class field theory. The 'classical' approach of Tagaki and Artin is through

rings of integers in number fields and their ideals. It is classical in the sense that it came first. This is the approach taken for the textbook *Algebraic Number Fields* by Janusz [20] as well as for this book. Essentially, the route to class field theory taken in this book is also followed in the Parts One and Two of Lang's *Algebraic Number Theory* [25]. However, Lang's exposition is quite different: new concepts are introduced far earlier, the style is more compact, less self-contained and it does not contain exercises other than leaving proofs to the reader as an exercise. Lang's book goes deeper into the subject: it has a Part Three on analytic methods. In [20] the modern approach to class field theory is not explained. Textbooks on class field theory usually start with a short overview of some standard algebraic number theory. Neukirch's *Algebraic Number Theory* [31] is organized this way. It gives an excellent axiomatic treatment of class field theory and in the last chapters the classical version of class field theory is deduced from the idèle-theoretic version. For a clear introduction in the subject read *A Brief Guide to Algebraic Number Theory* [36] by H.P.F. Swinnerton-Dyer.

Idèles are useful for theoretical purposes, for computation in concrete cases it is usually more convenient to use the classical notions. Moreover, knowledge of the classical approach is helpful for obtaining a better understanding of modern developments. This was also Hasse's idea behind the publication [17] in 1967 of his 1932/33 lecture notes on class field theory.

Books suitable for further reading which go much deeper into the subject than this textbook:

Algebraic Number Theory [31] by Neukirch, already mentioned above.

Algebraic Number Theory [7] by Cassels and Fröhlich (eds.), proceedings of an instructional conference in 1965 in Brighton. It contains many expositions of new developments in algebraic number theory. Contributions by Serre and Tate, among others.

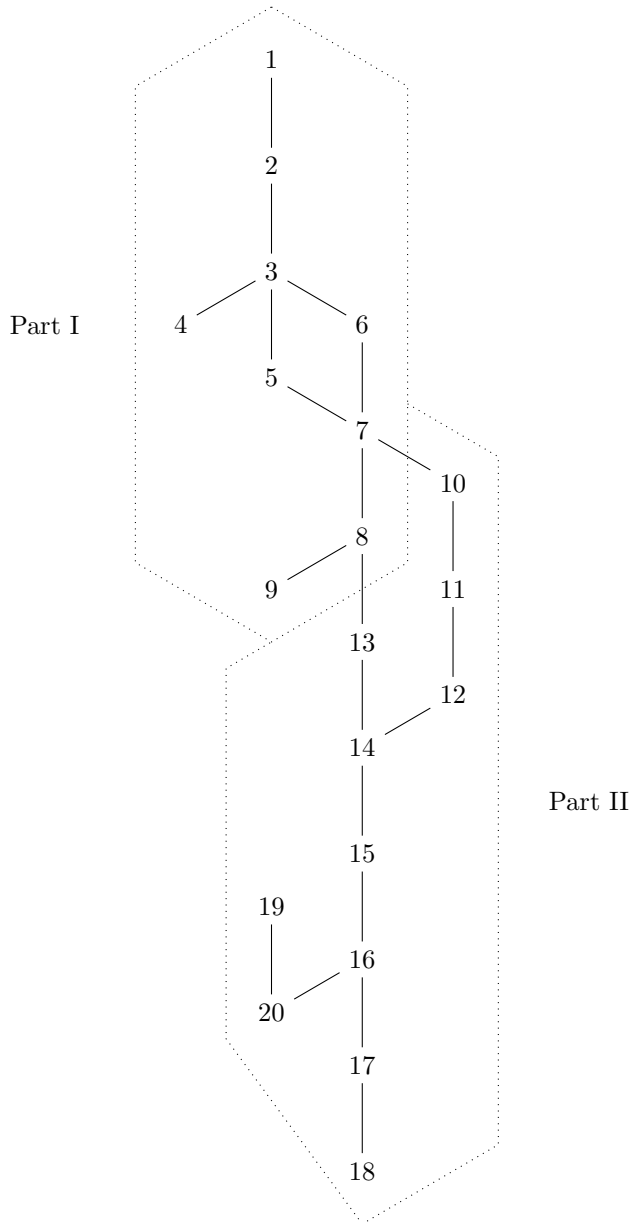
Introduction to Cyclotomic Fields [37] by Washington, the book for the theory of abelian number fields.

Class Field Theory [14] by Gras. No proofs of the main theorems of class field theory, but a lot on the consequences of these theorems.

Introduction to Modern Number Theory [27] by Manin and Panchishkin. From the preface: 'We present many precise definitions, but practically no complete proofs.' It is their interpretation of the word 'introduction'. It is good for getting an impression of the state of the art.

This book focusses on the abstract theory and not on the algorithmic aspects and applications in cryptography. For algorithms consult *A Course in Computational Algebraic Number Theory* [8] by Cohen. The reader is advised to use the free open-source mathematics software system *SageMath*, <https://www.sagemath.org>, in which implementations of many algorithms in number theory are available.

Logical dependence of chapters



The dependence does not apply to the examples given in the chapters.

Part I

**Basic Algebraic Number
Theory**

1 Integers in a Number Field

Finite extensions of the field \mathbb{Q} are called number fields and in each number field there is a subring, the ring of integers of the number field. The idea is to do arithmetic in a number field analogously to what we are used to in case of \mathbb{Q} and its subring \mathbb{Z} . In this chapter number fields and their rings of integers are considered in general, especially the additive group of the ring of integers is studied and ways to compute this subgroup of the additive group of the number field are given. Ideally, the ring of integers is a principal ideal domain, but it turns out that this is not the case in general. However, rings of integers are Dedekind domains, rings in which there is not necessarily a unique factorization of elements, but instead a unique factorization of ideals. Dedekind domains are treated in general in chapter 2 and in chapter 3 it is shown that rings of integers of number fields are indeed Dedekind domains. Euclidean domains, integral domains with a norm that makes division with remainder possible, are principal ideal domains. In the last section of this chapter examples of quadratic number fields are given for which the ring of integers is a euclidean domain.

1.1 Number fields

1.1 Definition. A field K of characteristic 0 of finite degree over its prime field \mathbb{Q} is called a *number field*. If $[K : \mathbb{Q}] = n$, the number field is said to be of *degree* n .

Since \mathbb{C} is algebraically closed, such fields are embeddable in \mathbb{C} . In fact, number fields are often given as subfields of \mathbb{C} . Note that embedding in \mathbb{C} may result into different subfields: e.g. the field $\mathbb{Q}[X]/(X^3 - 2)$ is isomorphic to two different subfields of \mathbb{C} .

The field \mathbb{Q} is the only number field of degree 1. There are infinitely many number fields of degree 2. They are parameterized by the squarefree integers $m \neq 1$: such an m corresponds to the field $\mathbb{Q}(\sqrt{m})$. (This is exercise 1 of this chapter.)

1.2 Definition. A number field of degree 2 is called a *quadratic* number field. If it is embeddable in \mathbb{R} , it is called a *real* quadratic number field, otherwise it is called an *imaginary* quadratic number field.

1 Integers in a Number Field

So the real quadratic number fields are the fields $\mathbb{Q}(\sqrt{m})$ with m squarefree > 1 and the imaginary ones those with m squarefree < 0 . Note that a real quadratic number field has two embeddings in \mathbb{R} . An imaginary quadratic number field has two embeddings in \mathbb{C} and no embeddings in \mathbb{R} . In the last case we rather speak of a pair of embeddings since the embeddings are closely related: they interchange under composition by complex conjugation.

The field \mathbb{Q} is a subfield of \mathbb{R} and the ring \mathbb{Z} is a lattice in both in the sense of the following definition.

1.3 Definition. Let V be an n -dimensional \mathbb{Q} -vector space. A subgroup A of the additive group of V is called a *lattice* in V if there is a basis (v_1, \dots, v_n) of V such that $A = \mathbb{Z}v_1 + \dots + \mathbb{Z}v_n$. Similarly for \mathbb{R} -vector spaces. A subring R of a number field K is called a *number ring* of K if R is also a lattice in the \mathbb{Q} -vector space K .

Note that lattices in n -dimensional \mathbb{Q} - or \mathbb{R} -vector spaces are free abelian groups of rank n . Conversely, a free abelian group A of rank n can be embedded in an n -dimensional \mathbb{Q} -vector space by extension of scalars: $A \rightarrow \mathbb{Q} \otimes_{\mathbb{Z}} A$, $a \mapsto 1 \otimes a$. In the same manner A can be embedded as a lattice in a real vector space.

1.4 Examples.

- a) The ring \mathbb{Z} is a number ring of \mathbb{Q} ; it is the only one.
- b) The ring $\mathbb{Z}[i]$ is a number ring of the imaginary quadratic number field $\mathbb{Q}(i)$. We will see that it is maximal in the sense that all number rings of $\mathbb{Q}(i)$ are contained in $\mathbb{Z}[i]$. A simple example is $\mathbb{Z}[2i] (= \mathbb{Z} + \mathbb{Z}2i)$, which is contained in $\mathbb{Z}[i]$ with index 2.
- c) The ring $\mathbb{Z}[\zeta_3]$ is a number ring of the imaginary quadratic number field $\mathbb{Q}(\sqrt{-3})$.
- d) Let $\gamma = \frac{1+\sqrt{5}}{2}$, the ‘golden ratio’. The ring $\mathbb{Z}[\gamma]$ is a number ring of the real quadratic field $\mathbb{Q}(\sqrt{5})$.

Clearly, a number ring R of a number field K is an integral domain and its field of fractions is the field K . We can embed a number field K of degree n into the commutative \mathbb{R} -algebra $\mathbb{R} \otimes_{\mathbb{Q}} K$ of \mathbb{R} -dimension n by extension of scalars:

$$\iota': K \rightarrow \mathbb{R} \otimes_{\mathbb{Q}} K, \quad \alpha \mapsto 1 \otimes \alpha.$$

Under this embedding a \mathbb{Q} -basis $(\alpha_1, \dots, \alpha_n)$ of K is mapped to the \mathbb{R} -basis $(1 \otimes \alpha_1, \dots, 1 \otimes \alpha_n)$ of $\mathbb{R} \otimes_{\mathbb{Q}} K$. In particular, a number ring of K maps onto a lattice in the real vector space $\mathbb{R} \otimes_{\mathbb{Q}} K$.

For the determination of the structure of the real algebra $\mathbb{R} \otimes_{\mathbb{Q}} K$ we consider the n embeddings of K in \mathbb{C} . Let r be the number of embeddings in \mathbb{R} (called *real embeddings*); possibly $r = 0$. Then there are $s = \frac{n-r}{2}$ pairs of nonreal embeddings

in \mathbb{C} (called *complex embeddings*). Let $\sigma_1, \dots, \sigma_r: K \rightarrow \mathbb{R}$ be the real embeddings and $\tau_1, \overline{\tau_1}, \dots, \tau_s, \overline{\tau_s}$ the complex embeddings. Then we have the following embedding in the \mathbb{R} -algebra $\mathbb{R}^r \times \mathbb{C}^s$:

$$\iota: K \rightarrow \mathbb{R}^r \times \mathbb{C}^s, \quad \alpha \mapsto (\sigma_1(\alpha), \dots, \sigma_r(\alpha), \tau_1(\alpha), \dots, \tau_s(\alpha)).$$

This embedding ι we will frequently use. It depends on some choices: the order of the embeddings and the choice of a complex embedding for each pair of complex embeddings. It agrees with the embedding ι' given earlier in the following sense: the \mathbb{R} -algebra homomorphism $\varphi: \mathbb{R} \otimes_{\mathbb{Q}} K \rightarrow \mathbb{R}^r \times \mathbb{C}^s$, given by $\lambda \otimes \alpha \mapsto (\lambda\sigma_1(\alpha), \dots, \lambda\tau_s(\alpha))$, makes the following triangle commutative

$$\begin{array}{ccc} & & \mathbb{R} \otimes_{\mathbb{Q}} K \\ & \nearrow \iota' & \downarrow \varphi \\ K & & \mathbb{R}^r \times \mathbb{C}^s \\ & \searrow \iota & \end{array}$$

and is actually an isomorphism: take a primitive element ϑ of the field extension $K : \mathbb{Q}$, that is $K = \mathbb{Q}(\vartheta)$ and let $f \in \mathbb{Q}[X]$ be its minimal polynomial over \mathbb{Q} . Then $\sigma_1(\vartheta), \dots, \sigma_r(\vartheta)$ are the r real zeros of f and $\tau_1(\vartheta), \overline{\tau_1(\vartheta)}, \dots, \tau_s(\vartheta), \overline{\tau_s(\vartheta)}$ the s pairs of complex zeros of f . Then over \mathbb{R} the factorization of f is

$$f = f_1 \cdots f_r g_1 \cdots g_s,$$

where $f_i = X - \sigma_i(\vartheta)$ for $i = 1, \dots, r$ and $g_j = X^2 - (\tau_j(\vartheta) + \overline{\tau_j(\vartheta)})X + \tau_j(\vartheta)\overline{\tau_j(\vartheta)}$ for $j = 1, \dots, s$. The map φ is the composition of the following isomorphisms of \mathbb{R} -algebras:

$$\begin{aligned} \mathbb{R} \otimes_{\mathbb{Q}} K &\xrightarrow{\sim} \mathbb{R} \otimes_{\mathbb{Q}} \mathbb{Q}[X]/(f) \xrightarrow{\sim} \mathbb{R}[X]/(f) \\ &\xrightarrow{\sim} \mathbb{R}[X]/(f_1) \times \cdots \times \mathbb{R}[X]/(f_r) \times \mathbb{R}[X]/(g_1) \times \cdots \times \mathbb{R}[X]/(g_s) \\ &\xrightarrow{\sim} \mathbb{R}^r \times \mathbb{C}^s, \end{aligned}$$

where for the third isomorphism the Chinese Remainder Theorem is applied and the isomorphisms $\mathbb{R}[X]/(f_i) \rightarrow \mathbb{R}$ and $\mathbb{R}[X]/(g_j) \rightarrow \mathbb{C}$ are induced by $X \mapsto \sigma_i(\vartheta)$ and $X \mapsto \tau_j(\vartheta)$ respectively.

1.5 Examples.

- a) An imaginary quadratic number field has one pair of complex embeddings. The number rings $\mathbb{Z}[i]$ and $\mathbb{Z}[\zeta_3]$ are lattices in the \mathbb{R} -vector space \mathbb{C} .
- b) A real quadratic number field has two real embeddings. For instance the two embeddings of $\mathbb{Q}(\sqrt{5})$ in \mathbb{R} map $\sqrt{5}$ to $\sqrt{5}$ and $-\sqrt{5}$ respectively. The number ring $\mathbb{Z}[\gamma]$ maps onto a lattice in \mathbb{R}^2 .

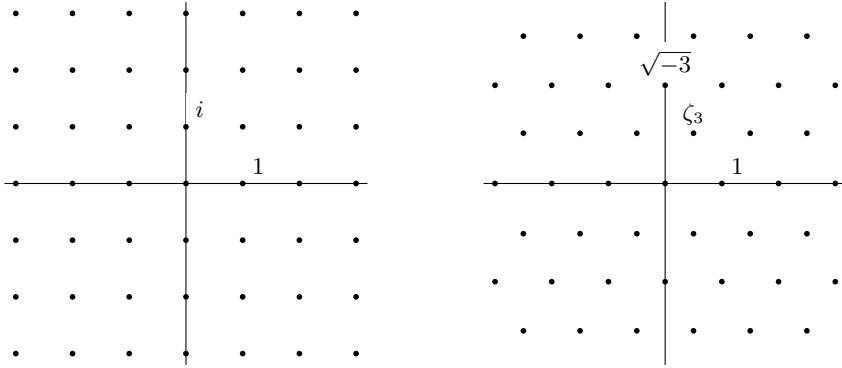


Figure 1.1: The lattices $\mathbb{Z}[i]$ and $\mathbb{Z}[\zeta_3]$ in \mathbb{C}

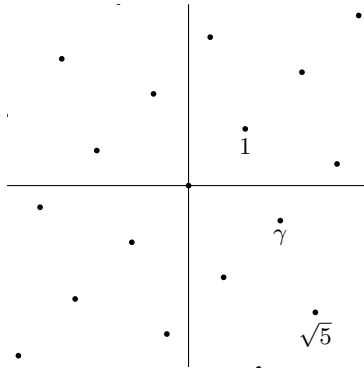


Figure 1.2: The lattice $\iota(\mathbb{Z}[\gamma])$ in \mathbb{R}^2

1.2 Algebraic integers

In this section the notion of integer in a number field is defined and it is shown that the integers in a number field form a subring, the ring of integers of the number field. For later use it is advantageous to introduce integrality in a somewhat more abstract setting.

1.6 Definitions and notation. Let K be a field and R a subring of K . An $\alpha \in K$ is called *integral* over R if there exists a monic polynomial $f \in R[X]$ such that $f(\alpha) = 0$. The set of all α in K which are integral over R is called the *integral closure* of R in K . An integral domain is called *integrally closed* if it coincides with the integral closure of the domain in its field of fractions. An $\alpha \in \mathbb{C}$ is called an *algebraic integer* (or just an *integer*) if α is integral over \mathbb{Z} . The subset of \mathbb{C} of all

algebraic integers is denoted by \mathcal{O} . It is the integral closure of \mathbb{Z} in \mathbb{C} .

Integral closures are defined as subsets. It still has to be shown that they are in fact subrings. To start with let's compute the integers in \mathbb{Q} and the integers in a quadratic number field.

1.7 Proposition. *Let α be an algebraic number and $f \in \mathbb{Q}[X]$ its minimal polynomial over \mathbb{Q} . Then*

$$\alpha \text{ is an algebraic integer} \iff f \in \mathbb{Z}[X].$$

PROOF. Clearly, it suffices to show that $f \in \mathbb{Z}[X]$ if α is an integer. Let α be a zero of a monic $g \in \mathbb{Z}[X]$. Then $f \mid g$ in $\mathbb{Q}[X]$ and so by the Gauß Lemma $f \in \mathbb{Z}[X]$. \square

In the proof we used:

Gauß Lemma. *Let $f \in \mathbb{Z}[X]$ and $f = gh$, where $g, h \in \mathbb{Q}[X]$, then there exists an $r \in \mathbb{Q}^*$ such that $rg, \frac{1}{r}h \in \mathbb{Z}[X]$.*

So if f is monic, then rg and $\frac{1}{r}h$ are monic as well.

1.8 Corollary. $\mathcal{O} \cap \mathbb{Q} = \mathbb{Z}$. \square

So the only integers in \mathbb{Q} are the ordinary integers. Because of this, sometimes they are called rational integers for being more specific.

1.9 Theorem (Integers of a quadratic number field). *Let $m \in \mathbb{Z}$ be squarefree and $\neq 1$. The integers in $\mathbb{Q}(\sqrt{m})$ are the numbers*

$$a + b\sqrt{m} \quad \text{with } a, b \in \mathbb{Z}$$

if $m \equiv 2, 3 \pmod{4}$ and in case $m \equiv 1 \pmod{4}$ the integers are the numbers

$$\frac{a + b\sqrt{m}}{2} \quad \text{with } a, b \in \mathbb{Z} \text{ and } a \equiv b \pmod{2}.$$

PROOF. Let $\alpha = r + s\sqrt{m}$ with $r \in \mathbb{Q}$ and $s \in \mathbb{Q}^*$. Then the minimal polynomial of α over \mathbb{Q} is $X^2 - 2rX + (r^2 - ms^2)$. By Proposition 1.7 we have

$$\alpha \text{ is integral} \iff 2r \in \mathbb{Z} \text{ and } r^2 - ms^2 \in \mathbb{Z},$$

which in fact also holds when $s = 0$. If α is integral, then $r = \frac{a}{2}$ with $a \in \mathbb{Z}$. Then $a^2 - 4ms^2 \in 4\mathbb{Z}$ and so $4ms^2 \in \mathbb{Z}$. Since m is squarefree, it follows that $s = \frac{b}{2}$ with $b \in \mathbb{Z}$. Hence $\alpha = \frac{a+b\sqrt{m}}{2}$ with $a, b \in \mathbb{Z}$. Numbers $\frac{a+b\sqrt{m}}{2}$ with $a, b \in \mathbb{Z}$ are integral exactly when $4 \mid a^2 - mb^2$. For $m \equiv 2, 3 \pmod{4}$ this is equivalent to a and b being both even. For $m \equiv 1 \pmod{4}$ we have $a^2 - mb^2 \equiv (a-b)(a+b) \pmod{4}$, and the condition becomes $a \equiv b \pmod{2}$. \square

1.10 Notation. For squarefree integers $m \neq 1$ put

$$\omega_m = \begin{cases} \sqrt{m} & \text{if } m \equiv 2, 3 \pmod{4}, \\ \frac{1}{2} + \frac{1}{2}\sqrt{m} & \text{if } m \equiv 1 \pmod{4}. \end{cases}$$

1.11 Corollary. *In the notation of Theorem 1.9: the integers in $\mathbb{Q}(\sqrt{m})$ form the subring $\mathbb{Z}[\omega_m]$. \square*

The rings $\mathbb{Z}[i]$, $\mathbb{Z}[\zeta_3]$ and $\mathbb{Z}[\gamma]$ of Example 1.4 are the special cases $m = -1$, $m = -3$ and $m = 5$ respectively.

There are alternatives for the definition of integrality. They can be helpful when establishing integrality in certain cases.

1.12 Proposition. *Let R be a subring of a field K . For $\alpha \in K$ the following are equivalent:*

- a) α is integral over R ,
- b) the subring $R[\alpha]$ is finitely generated as an R -module,
- c) there exists a subring A of K which is finitely generated as R -module such that $\alpha \in A$,
- d) there exists a finitely generated R -submodule $B \neq 0$ of K such that $\alpha B \subseteq B$.

PROOF.

a) \Rightarrow b): If α is a zero of a monic $f \in R[X]$ of degree n , then the subring $R[\alpha]$ of K is generated by $1, \alpha, \dots, \alpha^{n-1}$ as an R -module.

b) \Rightarrow c): Take $A = R[\alpha]$.

c) \Rightarrow d): Take $B = A$.

d) \Rightarrow a): Suppose β_1, \dots, β_n generate B as an R -module. Then, since $\alpha\beta_i \in B$, we have $\alpha\beta_i = r_{i1}\beta_1 + \dots + r_{in}\beta_n$ with $r_{i1}, \dots, r_{in} \in R$, or in matrix notation

$$\alpha \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} = M \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} \quad \text{with } M = (r_{ij}).$$

This means that α is an eigenvalue of the matrix M . Therefore, it is a zero of the characteristic polynomial of M , which is a monic polynomial over R since all $r_{ij} \in R$. \square

1.13 Corollary. *Let R be a subring of a field K . Then the integral closure R' of R in K is an integrally closed subring of K . In particular \mathcal{O} is an integrally closed subring of \mathbb{C} and for a number field K the integers in K form an integrally closed subring of K .*

PROOF. Clearly $1, -1 \in R'$, so for showing that R' is a subring of K it suffices to prove that R' is closed under addition and multiplication. Suppose $\alpha, \beta \in R'$, say $f(\alpha) = 0$ and $g(\beta) = 0$ with $f, g \in R[X]$ monic of degree m and n respectively. Then the subring $R[\alpha, \beta]$ of K is an R -submodule generated by the mn elements $\alpha^i \beta^j$ with $i = 0, \dots, m-1$ and $j = 0, \dots, n-1$. Since $\alpha + \beta, \alpha\beta \in R[\alpha, \beta]$ it follows from Proposition 1.12 that $\alpha + \beta, \alpha\beta \in R'$. The field K contains the field of fractions of R' ; therefore, the ring R' is integrally closed. The set \mathcal{O} is the integral closure of \mathbb{Z} in \mathbb{C} and for a number field K the subset $\mathcal{O} \cap K$ is the integral closure of \mathbb{Z} in K . \square

1.14 Definition. The subring $\mathcal{O} \cap K$ of a number field K is called the *ring of integers* of K . It is denoted by \mathcal{O}_K .

Theorem 1.9 described the ring of integers in a quadratic number field K . It is a number ring of K . In Section 1.6 we will see that this holds for the ring of integers of any number field.

1.3 Norm, trace and characteristic polynomial

For finite field extensions we have the notions of norm and trace. General properties of norms and traces are proved in this section.

1.15 Definitions and notations. Let $L : K$ be a finite field extension, say $[L : K] = n$. For each $\alpha \in L$ we have a K -linear transformation

$$M_\alpha : L \rightarrow L, \quad \xi \mapsto \alpha\xi.$$

Let $\Delta_{M_\alpha}(X) \in K[X]$ be the characteristic polynomial of M_α , that is $\Delta_{M_\alpha}(X) = \det(X \cdot 1 - M_\alpha)$, and let $\text{Tr}(M_\alpha) \in K$ be the trace of M_α . We define

a) the *characteristic polynomial* $\Delta_\alpha^{L:K}(X)$ of α over K :

$$\Delta_\alpha^{L:K}(X) = \Delta_{M_\alpha}(X),$$

b) the *trace* $\text{Tr}_K^L(\alpha)$ of α over K :

$$\text{Tr}_K^L(\alpha) = \text{Tr}(M_\alpha),$$

c) the *norm* $N_K^L(\alpha)$ of α over K :

$$N_K^L(\alpha) = \det(M_\alpha).$$

Thus Tr_K^L and N_K^L are maps $L \rightarrow K$.

1.16 Example. Let $m \in \mathbb{Z}$ be squarefree $\neq 1$. The characteristic polynomial of $\alpha = r + s\sqrt{m} \in K = \mathbb{Q}(\sqrt{m})$, where $r, s \in \mathbb{Q}$, is

$$\Delta_{\alpha}^{K:\mathbb{Q}}(X) = X^2 - \text{Tr}_{\mathbb{Q}}^K(\alpha)X + N_{\mathbb{Q}}^K(\alpha) = X^2 - 2rX + r^2 - s^2m.$$

This polynomial was used in the proof of Theorem 1.9 for the computation of the ring \mathcal{O}_K .

Note that for $[L : K] = n$:

$$\Delta_{\alpha}^{L:K}(X) = X^n - \text{Tr}_K^L(\alpha)X^{n-1} + \cdots + (-1)^n N_K^L(\alpha) \in K[X].$$

Clearly, in the quadratic case the characteristic polynomial is completely determined by the trace and the norm.

1.17 Proposition. Let $L : K$ be a field extension of degree n . Then for all $\alpha, \beta \in L$ and $c \in K$:

- a) $\text{Tr}_K^L(\alpha + \beta) = \text{Tr}_K^L(\alpha) + \text{Tr}_K^L(\beta)$,
- b) $\text{Tr}_K^L(c\alpha) = c\text{Tr}_K^L(\alpha)$,
- c) $\text{Tr}_K^L(c) = nc$,
- d) $N_K^L(\alpha\beta) = N_K^L(\alpha)N_K^L(\beta)$,
- e) $N_K^L(c) = c^n$.

PROOF. These rules follow directly from the following identities for linear transformations: $M_{\alpha+\beta} = M_{\alpha} + M_{\beta}$, $M_{c\alpha} = cM_{\alpha}$, $M_c = c \cdot 1$ and $M_{\alpha\beta} = M_{\alpha}M_{\beta}$. \square

So in particular we have a K -linear function $\text{Tr}_K^L : L \rightarrow K$ and a group homomorphism $N_K^L : L^* \rightarrow K^*$.

The notions of trace and norm are defined for arbitrary finite field extensions. For separable finite extensions we derive formulas for them in terms of the conjugates of an element, i.e. in terms of the roots of its minimal polynomial.

1.18 Theorem. Let $L : K$ be a finite separable field extension of degree n . Let $\sigma_1, \dots, \sigma_n$ be the embeddings of L in a normal closure \bar{L} of $L : K$ fixing the elements of K . Let $\alpha \in L$, $[K(\alpha) : K] = d$ and f the minimal polynomial of α over K . Then we have:

$$\Delta_{\alpha}^{L:K}(X) = f(X)^{n/d} = \prod_{i=1}^n (X - \sigma_i(\alpha)),$$

$$N_K^L(\alpha) = \prod_{i=1}^n \sigma_i(\alpha) \quad \text{and} \quad \text{Tr}_K^L(\alpha) = \sum_{i=1}^n \sigma_i(\alpha).$$

PROOF. Let M'_α be the restriction of M_α to $K(\alpha)$ and let $f(X) = X^d + a_1X^{d-1} + \dots + a_d$ be the minimal polynomial of α over K . The matrix of M'_α with respect to the basis $1, \alpha, \dots, \alpha^{d-1}$ is the companion matrix of f :

$$[M'_\alpha] = \begin{pmatrix} 0 & 0 & \dots & 0 & -a_d \\ 1 & 0 & \dots & 0 & -a_{d-1} \\ 0 & 1 & \dots & 0 & -a_{d-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -a_1 \end{pmatrix}.$$

The polynomial f is the characteristic polynomial of its companion matrix:

$$\begin{aligned} \det(X \cdot 1 - M'_\alpha) &= \begin{vmatrix} X & 0 & \dots & 0 & a_d \\ -1 & X & \dots & 0 & a_{d-1} \\ 0 & -1 & \dots & 0 & a_{d-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & -1 & X + a_1 \end{vmatrix} \\ &= \begin{vmatrix} 1 & X & \dots & X^{d-2} & X^{d-1} \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & 1 \end{vmatrix} \cdot \begin{vmatrix} X & 0 & \dots & 0 & a_d \\ -1 & X & \dots & 0 & a_{d-1} \\ 0 & -1 & \dots & 0 & a_{d-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & -1 & X + a_1 \end{vmatrix} \\ &= \begin{vmatrix} 0 & 0 & \dots & 0 & f(X) \\ -1 & X & \dots & 0 & a_{d-1} \\ 0 & -1 & \dots & 0 & a_{d-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & -1 & X + a_1 \end{vmatrix} = f(X). \end{aligned}$$

Let $\beta_1, \dots, \beta_{n/d}$ be a $K(\alpha)$ -basis of L . Then

$$(\beta_1, \alpha\beta_1, \dots, \alpha^{d-1}\beta_1, \dots, \beta_{n/d}, \alpha\beta_{n/d}, \dots, \alpha^{d-1}\beta_{n/d})$$

is a K -basis of L . The matrix of M_α with respect to this basis is in block form

$$[M_\alpha] = \begin{pmatrix} [M'_\alpha] & 0 & \dots & 0 \\ 0 & [M'_\alpha] & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & [M'_\alpha] \end{pmatrix}$$

and so the characteristic polynomial of $\alpha \in L$ over K is

$$\Delta_\alpha^{L:K}(X) = \Delta_{M_\alpha}(X) = (\det(X \cdot 1 - M'_\alpha))^{n/d} = f(X)^{n/d} = \prod_{i=1}^n (X - \sigma_i(\alpha)).$$

1 Integers in a Number Field

The coefficients of X^{n-1} and X^0 yield the expressions for the trace and the norm. \square

Note that we have (in the notations used above): $N_K^L(\alpha) = (N_K^{K(\alpha)}(\alpha))^{n/d} = (-1)^n a_d^{n/d}$ and $\text{Tr}_K^L(\alpha) = \frac{n}{d} \text{Tr}_K^{K(\alpha)}(\alpha) = -\frac{n}{d} a_1$.

For a tower of field extensions the norm and the trace are transitive, that is they satisfy the rules described in the following proposition. Here we prove this for separable extensions only.

1.19 Proposition. *Let $K_2 : K_1$ and $K_1 : K_0$ be finite separable field extensions. Then for all $\alpha \in K_2$:*

$$N_{K_0}^{K_2}(\alpha) = N_{K_0}^{K_1}(N_{K_1}^{K_2}(\alpha)) \quad \text{and} \quad \text{Tr}_{K_0}^{K_2}(\alpha) = \text{Tr}_{K_0}^{K_1}(\text{Tr}_{K_1}^{K_2}(\alpha)).$$

PROOF. Let L be the normal closure of $K_2 : K_0$. There are exactly $m = [K_1 : K_0]$ embeddings $\sigma_1, \dots, \sigma_m$ of K_1 in L fixing K_0 elementwise and exactly $n = [K_2 : K_1]$ embeddings τ_1, \dots, τ_n of K_2 in L fixing K_1 elementwise. Let $\sigma_1, \dots, \sigma_m, \tau_1, \dots, \tau_n$ be prolongations to automorphisms of L of the equally named embeddings. The restrictions of the $\sigma_i \tau_j$ to K_2 are just the mn embeddings of K_2 in L fixing K_0 elementwise. The formulas are by now easy consequences of Theorem 1.18. \square

1.4 The norm on a number field

Let K be a number field and $\alpha \in K$ with minimal polynomial f over \mathbb{Q} . Since $\Delta_\alpha^{K:\mathbb{Q}}$ is a power of f we have that $\alpha \in \mathcal{O}_K$ if and only if $\Delta_\alpha^{K:\mathbb{Q}} \in \mathbb{Z}[X]$. In particular, it is clear that $N_{\mathbb{Q}}^K(\alpha), \text{Tr}_{\mathbb{Q}}^K(\alpha) \in \mathbb{Z}$ if $\alpha \in \mathcal{O}_K$. In section 1.6 we will show that \mathcal{O}_K is a number ring in K using the \mathbb{Q} -linear function $\text{Tr}_{\mathbb{Q}}^K : K \rightarrow \mathbb{Q}$. In this section the homomorphism $N_{\mathbb{Q}}^K : K^* \rightarrow \mathbb{Q}^*$ is considered, especially in relation to \mathcal{O}_K^* , the group of units. In section 5.4 the Dirichlet Unit Theorem will be proved, a theorem which fully describes the structure of this group.

We have embedded a number field K into the real algebra $\mathbb{R}^r \times \mathbb{C}^s$, r being the number of real embeddings of K and s the number of pairs of complex embeddings. The norm on K can be extended in a natural way to a multiplicative map $N : \mathbb{R}^r \times \mathbb{C}^s \rightarrow \mathbb{R}$.

1.20 Definition. The *norm* N on the \mathbb{R} -algebra $\mathbb{R}^r \times \mathbb{C}^s$ is defined as follows

$$N : \mathbb{R}^r \times \mathbb{C}^s \rightarrow \mathbb{R}, \quad (x_1, \dots, x_r, z_1, \dots, z_s) \mapsto x_1 \cdots x_r z_1 \bar{z}_1 \cdots z_s \bar{z}_s.$$

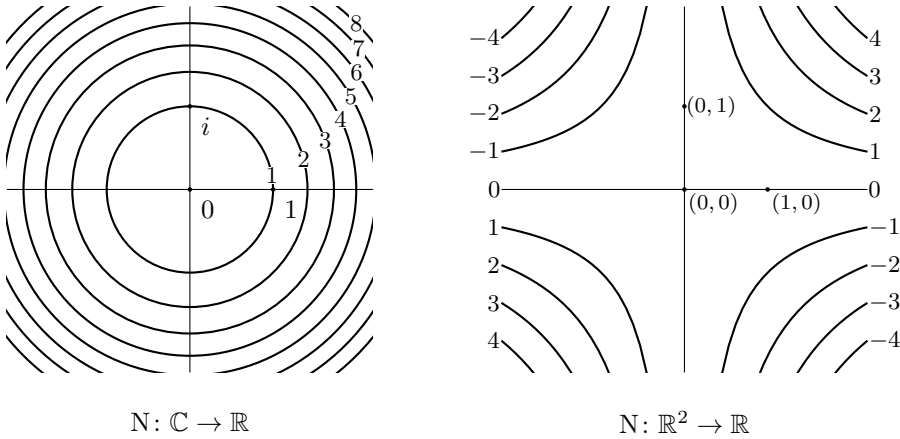


Figure 1.3: The norm on \mathbb{C} and on \mathbb{R}^2

The diagram

$$\begin{array}{ccc}
 K & \xrightarrow{\iota} & \mathbb{R}^r \times \mathbb{C}^s \\
 \downarrow N_{\mathbb{Q}}^K & & \downarrow N \\
 \mathbb{Q} & \xrightarrow{\subseteq} & \mathbb{R}
 \end{array}$$

clearly commutes: let $\sigma_1, \dots, \sigma_r$ be the real embeddings and let τ_1, \dots, τ_s represent the pairs of complex embeddings of K , then for all $\alpha \in K$

$$\begin{aligned}
 N\iota(\alpha) &= N(\sigma_1(\alpha), \dots, \sigma_r(\alpha), \tau_1(\alpha), \dots, \tau_s(\alpha)) \\
 &= \sigma_1(\alpha) \cdots \sigma_r(\alpha) \tau_1(\alpha) \overline{\tau_1(\alpha)} \cdots \tau_s(\alpha) \overline{\tau_s(\alpha)} = N_{\mathbb{Q}}^K(\alpha).
 \end{aligned}$$

1.21 Example. We have embedded imaginary and real quadratic number fields in \mathbb{C} and \mathbb{R}^2 respectively. Elements with a given norm in these \mathbb{R} -algebras form circles and hyperbolas respectively, see Figure 1.3.

Note that the restriction $N: (\mathbb{R}^*)^r \times (\mathbb{C}^*)^s \rightarrow \mathbb{R}^*$ is a group homomorphism. For the computation of units of a ring of integers the following is useful.

1.22 Proposition. Let K be a number field. Then for $\alpha \in \mathcal{O}_K$ we have

$$\alpha \in \mathcal{O}_K^* \iff N_{\mathbb{Q}}^K(\alpha) = \pm 1.$$

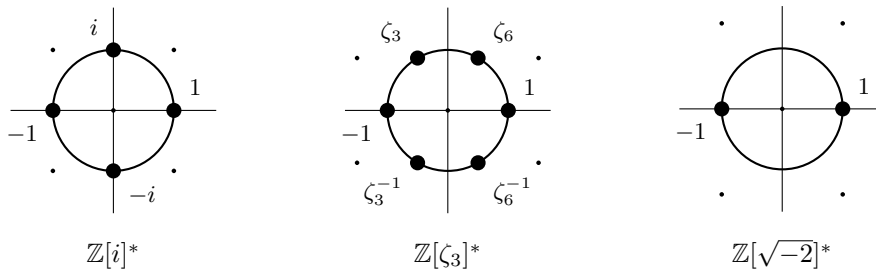


Figure 1.4: The units of $\mathbb{Z}[i]$, $\mathbb{Z}[\zeta_3]$ and $\mathbb{Z}[\sqrt{-2}]$

PROOF.

\Rightarrow : Since $\alpha, \frac{1}{\alpha} \in \mathcal{O}_K$, we have $N_{\mathbb{Q}}^K(\alpha), N_{\mathbb{Q}}^K(\frac{1}{\alpha}) \in \mathbb{Z}$ and $N_{\mathbb{Q}}^K(\alpha)N_{\mathbb{Q}}^K(\frac{1}{\alpha}) = 1$.

\Leftarrow : The characteristic polynomial of α over \mathbb{Q} is of the form $Xg(X) \pm 1$, where $g(X) \in \mathbb{Z}[X]$. It follows that $\alpha g(\alpha) = \pm 1$. \square

1.23 Example. For K an imaginary quadratic number field we have $\mathcal{O}_K^* = \{\pm 1\}$ if $K \neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3})$, whereas $\mathbb{Z}[i]^* = \langle i \rangle$ and $\mathbb{Z}[\zeta_3] = \langle \zeta_6 \rangle$, see Figure 1.4.

1.24 Example. Let K be a real quadratic field, say $K = \mathbb{Q}(\sqrt{m})$ with $m \in \mathbb{Z}$, $m > 1$ and squarefree. Suppose we have an $\varepsilon \in \mathcal{O}_K^*$ with $\varepsilon > 1$. Let σ be the nontrivial automorphism of K . Then of the four units $\varepsilon, -\varepsilon, \sigma(\varepsilon)$ and $-\sigma(\varepsilon)$ the unit ε is the greatest. Hence $\varepsilon = a + b\sqrt{m}$ with $a, b > 0$ and $a, b \in \mathbb{Z} \cdot \frac{1}{2}$ (or $a, b \in \mathbb{Z}$ if $m \equiv 2, 3 \pmod{4}$). For such a unit ε the set of all $c + d\sqrt{m} < \varepsilon$ with $c, d > 0$ and $c, d \in \mathbb{Z} \cdot \frac{1}{2}$ is finite; therefore, in the interval $(1, \varepsilon)$ there are only finitely many units. It follows that, if there is a unit > 1 , there also is a least one. If ε is the least unit > 1 of \mathcal{O}_K , then $\mathcal{O}_K^* = \langle -1, \varepsilon \rangle$. Later, in chapter 4 and again in chapter 5, we will see that units $\neq \pm 1$ do exist. The least one > 1 is called the *fundamental unit* of the real quadratic field K . The number $1 + \sqrt{2}$ is the fundamental unit of $\mathbb{Q}(\sqrt{2})$ and γ is the fundamental unit of $\mathbb{Q}(\sqrt{5})$. See Figure 1.5.

1.5 The discriminant

For a finite field extension $L : K$ the trace map $\text{Tr}_K^L : L \rightarrow K$ is a K -linear function on L . It is used to define a K -bilinear form on L :

1.25 Lemma. *Let $L : K$ be a finite field extension. Then the map*

$$L \times L \rightarrow K, \quad (\alpha, \beta) \mapsto \text{Tr}_K^L(\alpha\beta)$$

is a symmetric K -bilinear form on L . \square

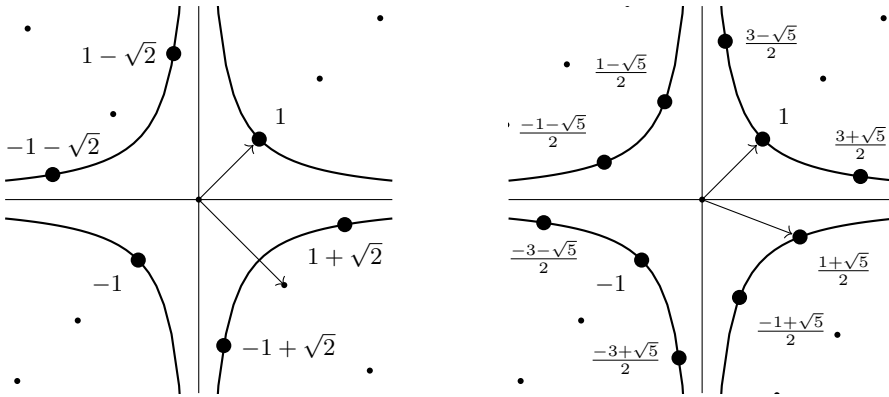


Figure 1.5: The groups $\mathbb{Z}[\sqrt{2}]^*$ and $\mathbb{Z}[\gamma]^*$

A bilinear form on a finite dimensional vector space has a matrix with respect to a basis of the vector space. In this case its determinant is called the discriminant:

1.26 Definition. Let $L : K$ a field extension of degree n and let $(\alpha_1, \dots, \alpha_n)$ be a K -basis of L . The element

$$\text{disc}_K(\alpha_1, \dots, \alpha_n) = \det(\text{Tr}_K^L(\alpha_i \alpha_j))$$

of K is called the *discriminant* of the K -basis $(\alpha_1, \dots, \alpha_n)$ of L . Usually it is clear which field is the base field and then we often write disc instead of disc_K .

Discriminants of different bases differ by a factor which is a square:

1.27 Proposition. Let $L : K$ be a field extension of degree n and let $(\alpha_1, \dots, \alpha_n)$ and $(\beta_1, \dots, \beta_n)$ be K -bases of L . Then

$$\text{disc}(\beta_1, \dots, \beta_n) = \det(T)^2 \text{disc}(\alpha_1, \dots, \alpha_n),$$

where T is the transition matrix from $(\beta_1, \dots, \beta_n)$ to $(\alpha_1, \dots, \alpha_n)$.

PROOF. This follows from

$$(\text{Tr}_K^L(\beta_i \beta_j)) = T^t (\text{Tr}_K^L(\alpha_i \alpha_j)) T. \quad \square$$

If $\beta_i = \sum_j a_{ij} \alpha_j$ for $i = 1, \dots, n$, then $T = (a_{ji})$. It is called the transition matrix from the β -basis to the α -basis since it satisfies $T[x]_\beta = [x]_\alpha$, where $[x]_\beta \in K^n$ stands for the column of β -coordinates of $x \in L$. Multiplication by T transforms the β -coordinates to the α -coordinates.

For separable extensions there is another description of the discriminant:

1.28 Proposition. *Let $L : K$ be a separable field extension of degree n and let $\sigma_1, \dots, \sigma_n$ be the n embeddings of L in a normal closure of $L : K$ which leave the elements of K fixed. Then for K -bases $(\alpha_1, \dots, \alpha_n)$ of L we have*

$$\text{disc}(\alpha_1, \dots, \alpha_n) = \det(\sigma_i(\alpha_j))^2.$$

PROOF. By Theorem 1.18 we have

$$(\sigma_j(\alpha_i))(\sigma_i(\alpha_j)) = (\text{Tr}_K^L(\alpha_i \alpha_j))$$

and from this the proposition follows. \square

Powers of a primitive element of a finite field extension $L : K$ form a K -basis of L . The discriminant of such a basis is equal to the discriminant of the minimal polynomial:

1.29 Proposition. *Let $K(\vartheta) : K$ be a separable field extension of degree n and let f be the minimal polynomial of ϑ over K . Then*

$$\text{disc}(1, \vartheta, \vartheta^2, \dots, \vartheta^{n-1}) = \text{disc}(f) = (-1)^{\frac{1}{2}n(n-1)} N_K^{K(\vartheta)}(f'(\vartheta)).$$

PROOF. Let $\sigma_1, \dots, \sigma_n$ be the embeddings of $K(\vartheta)$ in a normal closure of $K(\vartheta) : K$ which leave the elements of K fixed. (This normal closure is a splitting field of f over K .) By Proposition 1.28 we have

$$\begin{aligned} \text{disc}(1, \vartheta, \vartheta^2, \dots, \vartheta^{n-1}) &= \det(\sigma_i(\vartheta)^{j-1})^2 \\ &= \prod_{i>j} (\sigma_i(\vartheta) - \sigma_j(\vartheta))^2 \quad (\text{Vandermonde}) \\ &= (-1)^{\frac{1}{2}n(n-1)} \prod_{i \neq j} (\sigma_i(\vartheta) - \sigma_j(\vartheta)). \end{aligned}$$

By definition $\text{disc}(f) = \prod_{i>j} (\sigma_i(\vartheta) - \sigma_j(\vartheta))^2$. We also have

$$N_K^{K(\vartheta)}(f'(\vartheta)) = \prod_{i=1}^n \sigma_i(f'(\vartheta)) = \prod_{i=1}^n f'(\sigma_i(\vartheta)) = \prod_{i \neq j} (\sigma_i(\vartheta) - \sigma_j(\vartheta)). \quad \square$$

1.30 Corollary. *Let $L : K$ be a separable field extension of degree n and let $(\alpha_1, \dots, \alpha_n)$ be a K -basis of L . Then $\text{disc}(\alpha_1, \dots, \alpha_n) \neq 0$.*

PROOF. Since the extension is separable, it has a primitive element ϑ . By Proposition 1.29 we have $\text{disc}(1, \vartheta, \dots, \vartheta^{n-1}) \neq 0$ and by Proposition 1.27 also $\text{disc}(\alpha_1, \dots, \alpha_n) \neq 0$. \square

This corollary states that for a separable finite field extension $L : K$ the K -bilinear form $(\alpha, \beta) \mapsto \text{Tr}_K^L(\alpha\beta)$ is nondegenerate. This is equivalent to $L \rightarrow L^{\text{dual}}$, $\alpha \mapsto \text{Tr}_K^L(\alpha-)$ being an isomorphism of K -vector spaces, where the notation L^{dual} stands for the dual vector space of the K -vector space L . In case of characteristic 0 we could have proved the nondegeneracy also by showing directly that the map $\alpha \mapsto \text{Tr}_K^L(\alpha-)$ is injective: if $\alpha \neq 0$, then $\text{Tr}_K^L(\alpha \cdot \frac{1}{\alpha}) = \text{Tr}_K^L(1) = n \neq 0$.

1.31 Definition. Let $L : K$ be a finite separable field extension of degree n . Then the K -bilinear form $L \times L \rightarrow K$, $(\alpha, \beta) \mapsto \text{Tr}_K^L(\alpha\beta)$ is nondegenerate and so for each K -basis $(\alpha_1, \dots, \alpha_n)$ of L there exists a unique K -basis $(\beta_1, \dots, \beta_n)$ of L such that

$$\text{Tr}_K^L(\alpha_i\beta_j) = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases}$$

The basis $(\beta_1, \dots, \beta_n)$ is called the *dual* basis of $(\alpha_1, \dots, \alpha_n)$ (with respect to the given bilinear form on L).

The discriminant of the dual of a basis is simply the inverse of the discriminant of that basis:

1.32 Proposition. Let $L : K$ be a finite separable field extension of degree n and $(\beta_1, \dots, \beta_n)$ the dual of a K -basis $(\alpha_1, \dots, \alpha_n)$. Then

$$\text{disc}(\beta_1, \dots, \beta_n) = \text{disc}(\alpha_1, \dots, \alpha_n)^{-1}.$$

PROOF. For $\alpha = x_1\beta_1 + \dots + x_n\beta_n \in L$ with $x_1, \dots, x_n \in K$ we have for $i = 1, \dots, n$:

$$\text{Tr}_K^L(\alpha\alpha_i) = x_1\text{Tr}_K^L(\alpha_i\beta_1)\beta_1 + \dots + x_n\text{Tr}_K^L(\alpha_i\beta_n) = x_i.$$

So

$$\alpha = \text{Tr}_K^L(\alpha\alpha_1)\beta_1 + \dots + \text{Tr}_K^L(\alpha\alpha_n)\beta_n$$

and in particular for $i = 1, \dots, n$

$$\alpha_i = \text{Tr}_K^L(\alpha_i\alpha_1)\beta_1 + \dots + \text{Tr}_K^L(\alpha_i\alpha_n)\beta_n.$$

So the matrix $(\text{Tr}_K^L(\alpha_j\alpha_i))$ is the transition matrix from the α -basis to the β -basis. Hence by Proposition 1.27

$$\text{disc}(\alpha_1, \dots, \alpha_n) = \text{disc}(\alpha_1, \dots, \alpha_n)^2 \text{disc}(\beta_1, \dots, \beta_n). \quad \square$$

The following proposition is helpful when calculating discriminants.

1.33 Proposition. Let $M : L$ and $L : K$ be finite separable field extensions, $(\alpha_1, \dots, \alpha_n)$ a K -basis of L and $(\beta_1, \dots, \beta_m)$ an L -basis of M . Then

$$\text{disc}_K(\alpha_1\beta_1, \dots, \alpha_n\beta_m) = \text{disc}_K(\alpha_1, \dots, \alpha_n)^m \cdot N_K^L(\text{disc}_L(\beta_1, \dots, \beta_m)).$$

PROOF. Let $\sigma_1, \dots, \sigma_n$ be the embeddings of L in a normal closure \overline{M} of $M : K$ which leave the elements of K fixed and τ_1, \dots, τ_m the embeddings of M in \overline{M} which leave the elements of L fixed. Extend the σ_i and τ_j to automorphisms in $\text{Gal}(\overline{M} : K)$. Then the $\sigma_i \tau_j$ are the mn embeddings of M in \overline{M} which leave the elements of K fixed. Put $B = (\tau_i(\beta_j))_{1 \leq i, j \leq m}$ and $A = (\sigma_i(\alpha_j))_{1 \leq i, j \leq n}$. Then $\text{disc}_L(\beta_1, \dots, \beta_m) = \det(B)^2$ and $\text{disc}_K(\alpha_1, \dots, \alpha_n) = \det(A)^2$. The $\alpha_i \beta_j$ form a K -basis of M and the discriminant of this basis is the square of the determinant of

$$\begin{pmatrix} \sigma_1(B) & 0 & \cdots & 0 \\ 0 & \sigma_2(B) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \sigma_n(B) \end{pmatrix} \begin{pmatrix} \sigma_1(\alpha_1)I_m & \sigma_1(\alpha_2)I_m & \cdots & \sigma_1(\alpha_n)I_m \\ \sigma_2(\alpha_1)I_m & \sigma_2(\alpha_2)I_m & \cdots & \sigma_2(\alpha_n)I_m \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1)I_m & \sigma_n(\alpha_2)I_m & \cdots & \sigma_n(\alpha_n)I_m \end{pmatrix}.$$

The entries in these matrices are $m \times m$ -matrices. □

1.6 The additive group of the ring of integers of a number field

In this section the discriminant will be used to show that the ring of integers in a number field is actually a lattice in the number field. This leads to the notion of discriminant of a number field.

1.34 Lemma. *Let R be an integral domain with field of fractions K and let $K' : K$ be a finite field extension. Then K' has a K -basis consisting of elements which are integral over R .*

PROOF. Let $\alpha \in K'^*$ and let $f(X) = X^d + a_1X^{d-1} + \cdots + a_d$ be the minimal polynomial of α over K . Let $r \in R$ be a common multiple of the denominators of a_1, \dots, a_d , that is $ra_i \in R$ for $i = 1, \dots, d$. Then

$$r^d f(X) = (rX)^d + ra_1(rX)^{d-1} + \cdots + r^{d-1}a_{d-1}rX + r^d a_d.$$

The element $r\alpha$ is integral over R since it is a zero of

$$X^d + ra_1X^{d-1} + \cdots + r^{d-1}a_{d-1}X + r^d a_d \in R[X].$$

So given a K -basis $(\alpha_1, \dots, \alpha_n)$ of K' , choose $r_1, \dots, r_n \in R$ such that $r_i \alpha_i$ is integral over R . Then $(r_1 \alpha_1, \dots, r_n \alpha_n)$ is a K -basis of K' as well and its elements are integral over R . □

1.35 Corollary. *Let K be a number field of degree n . Then K has a \mathbb{Q} -basis $(\alpha_1, \dots, \alpha_n)$ such that $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$.* □

1.36 Proposition. *Let R be an integrally closed domain with field of fractions K , $K' : K$ a finite separable field extension of degree n , R' the integral closure of R in K' and $(\alpha_1, \dots, \alpha_n)$ a K -basis of K' such that $\alpha_1, \dots, \alpha_n \in R'$. Let $(\beta_1, \dots, \beta_n)$ be the dual basis of $(\alpha_1, \dots, \alpha_n)$ with respect to the nondegenerate K -bilinear form $(\alpha, \beta) \mapsto \text{Tr}_K^{K'}(\alpha\beta)$. Then*

$$R\alpha_1 + \dots + R\alpha_n \subseteq R' \subseteq R\beta_1 + \dots + R\beta_n \subseteq \frac{1}{d}(R\alpha_1 + \dots + R\alpha_n),$$

where $d = \text{disc}(\alpha_1, \dots, \alpha_n)$.

PROOF. Let $\alpha \in R'$. Then $\alpha = \text{Tr}_K^{K'}(\alpha_1\alpha)\beta_1 + \dots + \text{Tr}_K^{K'}(\alpha_n\alpha)\beta_n$. Since R is integrally closed, $\alpha_i\alpha \in R'$ and $\text{Tr}_K^{K'}(\alpha_i\alpha) \in K$, it follows that $\text{Tr}_K^{K'}(\alpha_i\alpha) \in R$ and so $\alpha \in R\beta_1 + \dots + R\beta_n$.

For $M = (\text{Tr}_K^{K'}(\alpha_i\alpha_j))$ we have

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = M \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}$$

Multiplication by the adjoint of M yields

$$\text{adj}(M) \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \det(M) \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}.$$

Since $\text{adj}(M)$ has entries in R and $\det(M) = \text{disc}(\alpha_1, \dots, \alpha_n) = d$, we have $\beta_i \in \frac{1}{d}(R\alpha_1 + \dots + R\alpha_n)$ for $i = 1, \dots, n$. \square

In general the ring R' in the above proposition is not a free R -module of rank n . But if R is a principal ideal domain, it is. For this we need the following lemma.

1.37 Lemma. *Let R be a principal ideal domain, A a free R -module of rank n and B an R -submodule of A . Then B is a free R -module of rank $\leq n$.*

PROOF. We will use induction on n . For $n = 0$ it is trivially true and for $n = 1$ it is a reformulation of R being a principal ideal domain. Let $n > 1$ and a_1, \dots, a_n be an R -basis of A . Consider the projection

$$\pi: A \rightarrow R, \quad r_1a_1 + \dots + r_na_n \mapsto r_n.$$

We have a short exact sequence of R -modules

$$0 \rightarrow \text{Ker}(\pi) \cap B \rightarrow B \rightarrow \pi(B) \rightarrow 0$$

with $\pi(B)$ free of rank ≤ 1 (case $n = 1$) and $\text{Ker}(\pi) \cap B$ an R -submodule of a free R -module of rank $n - 1$. The sequence splits and from this the lemma follows. \square

1.38 Corollary. (Notation of Proposition 1.36). If R is a principal ideal domain, then there exists a K -basis $(\alpha_1, \dots, \alpha_n)$ of K' such that $R' = R\alpha_1 + \dots + R\alpha_n$.

PROOF. If R is a principal ideal domain, an R -submodule of a free R -module of rank n is a free R -module of rank $\leq n$. Because the ring R' is sandwiched between free R -modules of rank n , it is itself a free R -module of rank n . \square

For the case $R = \mathbb{Z}$ we have in particular:

1.39 Corollary. Let K be a number field. Then the ring \mathcal{O}_K is a number ring of K . \square

1.40 Lemma. Let A be a free abelian group of rank n and B a subgroup of A of the same rank, $(\alpha_1, \dots, \alpha_n)$ a basis of A and $(\beta_1, \dots, \beta_n)$ a basis of B . Then for the index of B in A we have

$$(A : B) = |\det(T)|,$$

where T is the transition matrix from $(\beta_1, \dots, \beta_n)$ to $(\alpha_1, \dots, \alpha_n)$.

PROOF. The matrix T has entries in \mathbb{Z} and $\det(T) \neq 0$. Since \mathbb{Z} is a Euclidean domain, the matrix T can be transformed by elementary operations to a diagonal matrix without changing the determinant. So we can assume that T is a diagonal matrix and for such a matrix the lemma clearly holds. \square

1.41 Proposition. Let $(\alpha_1, \dots, \alpha_n)$ and $(\beta_1, \dots, \beta_n)$ be \mathbb{Q} -bases of a number field K . Let the lattices Λ and Γ in K , generated by these \mathbb{Q} -bases respectively, satisfy $\Gamma \subseteq \Lambda$. Then

$$\text{disc}(\beta_1, \dots, \beta_n) = (\Lambda : \Gamma)^2 \cdot \text{disc}(\alpha_1, \dots, \alpha_n).$$

PROOF. This follows from Proposition 1.27 and Lemma 1.40. \square

1.42 Definition. Let K be a number field. A \mathbb{Q} -basis $(\alpha_1, \dots, \alpha_n)$ of K which satisfies $\mathbb{Z}\alpha_1 + \dots + \mathbb{Z}\alpha_n = \mathcal{O}_K$ is called an *integral basis* of K . The *discriminant* of K is defined as the discriminant of an integral basis of K . By Proposition 1.41 it is independent of the choice of the integral basis. Notation: $\text{disc}(K)$. Note that $\text{disc}(K) \in \mathbb{Q} \cap \mathcal{O} = \mathbb{Z}$.

Note that an integral basis of a number field K is not just a basis consisting of integers of K , but is a \mathbb{Z} -basis of \mathcal{O}_K .

Specializing the \mathbb{Q} -basis $(\alpha_1, \dots, \alpha_n)$ of Proposition 1.41 to the case of an integral basis yields:

1.43 Theorem. Let $(\beta_1, \dots, \beta_n)$ be a \mathbb{Q} -basis of a number field K with $\beta_1, \dots, \beta_n \in \mathcal{O}_K$ and let Γ be the lattice generated by this basis. Then

$$\text{disc}(\beta_1, \dots, \beta_n) = (\mathcal{O}_K : \Gamma)^2 \cdot \text{disc}(K).$$

1.6 The additive group of the ring of integers of a number field

In particular, if $K = \mathbb{Q}(\vartheta)$ with $\vartheta \in \mathcal{O}_K$, then

$$\text{disc}(f) = (\mathcal{O}_K : \mathbb{Z}[\vartheta])^2 \cdot \text{disc}(K),$$

where f is the minimal polynomial of ϑ over \mathbb{Q} . □

1.44 Example. Theorem 1.9 describes integral bases for quadratic number fields. Let m be a squarefree integer $\neq 1$. For $m \equiv 2, 3 \pmod{4}$ we have $\text{disc}(\mathbb{Q}(\sqrt{m})) = 4m$, whereas $\text{disc}(\mathbb{Q}(\sqrt{m})) = m$ for $m \equiv 1 \pmod{4}$.

The discriminant of a number field is an integer. The following two propositions give further restrictions.

1.45 Proposition (Stickelberger). *Let K be a number field. Then $\text{disc}(K) \equiv 0 \pmod{4}$ or $\text{disc}(K) \equiv 1 \pmod{4}$.*

PROOF. Let K be of degree n and let $\sigma_1, \dots, \sigma_n$ be the embeddings of K in the normal closure L of $K : \mathbb{Q}$. Let $(\alpha_1, \dots, \alpha_n)$ be an integral basis of K . By Proposition 1.28 the discriminant of K is the square of $\det(\sigma_i(\alpha_j))$. We have

$$\det(\sigma_i(\alpha_j)) = \sum_{\pi} \text{sgn}(\pi) \prod_{i=1}^n \sigma_{\pi(i)}(\alpha_i) = \sum_{\pi} \prod_{i=1}^n \sigma_{\pi(i)}(\alpha_i) - 2 \sum_{\pi \text{ odd}} \prod_{i=1}^n \sigma_{\pi(i)}(\alpha_i),$$

where the sums \sum_{π} are over all permutations π of $\{1, \dots, n\}$. Put

$$P = \sum_{\pi} \prod_{i=1}^n \sigma_{\pi(i)}(\alpha_i) \quad \text{and} \quad Q = \sum_{\pi \text{ odd}} \prod_{i=1}^n \sigma_{\pi(i)}(\alpha_i).$$

If $\sigma \in \text{Gal}(L : \mathbb{Q})$, then $\sigma_i \mapsto \sigma\sigma_i$ permutes the embeddings $\sigma_1, \dots, \sigma_n$ and so $\sigma(P) = P$. By the Main Theorem of Galois Theory it follows that $P \in \mathbb{Q}$. Since P is integral we have $P \in \mathbb{Z}$. Moreover,

$$\text{disc}(K) = (P - 2Q)^2 = P^2 + 4(Q^2 - PQ).$$

This implies that $Q^2 - PQ \in \mathbb{Q}$ and even $Q^2 - PQ \in \mathbb{Z}$, since $Q^2 - PQ \in \mathcal{O}$. Hence $\text{disc}(K) \equiv P^2 \pmod{4}$. □

1.46 Proposition. *Let K be a number field and let s be the number of pairs of complex embeddings of K . Then $\text{sgn}(\text{disc}(K)) = (-1)^s$.*

PROOF. In the notation used in the proof of the previous proposition: if σ is complex conjugation, then the permutation $\sigma_i \mapsto \sigma\sigma_i$ of the embeddings is a product of s disjoint transpositions. Therefore, $\det(\sigma\sigma_i(\alpha_j)) = (-1)^s \det(\sigma_i(\alpha_j))$. If s is even, then $\det(\sigma_i(\alpha_j))$ is real, and if s is odd, then $\det(\sigma_i(\alpha_j))$ is purely imaginary. □

For a given number field K it is usually not difficult to find a \mathbb{Q} -basis consisting of integers. By Theorem 1.43 the problem of finding an integral basis is then reduced to checking integrality of a finite number of elements of K :

1.47 Lemma. *Let K be a number field of degree n and let $(\alpha_1, \dots, \alpha_n)$ be a \mathbb{Q} -basis of K consisting of integers. If $m \in \mathbb{N}^*$ and $k_1, \dots, k_n \in \mathbb{Z}$ satisfy*

$$\frac{k_1\alpha_1 + \dots + k_n\alpha_n}{m} \in \mathcal{O}_K \quad \text{and} \quad \gcd(m, k_1, \dots, k_n) = 1,$$

then $m^2 \mid \text{disc}(\alpha_1, \dots, \alpha_n)$.

PROOF. If $k_i \neq 0$, then

$$\begin{aligned} \text{disc}(\alpha_1, \dots, \alpha_{i-1}, \frac{k_1\alpha_1 + \dots + k_n\alpha_n}{m}, \alpha_{i+1}, \dots, \alpha_n) \\ = \frac{1}{m^2} \text{disc}(\alpha_1, \dots, \alpha_{i-1}, k_i\alpha_i, \alpha_{i+1}, \dots, \alpha_n) = \frac{k_i^2}{m^2} \text{disc}(\alpha_1, \dots, \alpha_n). \end{aligned}$$

Hence $m^2 \mid k_i^2 \text{disc}(\alpha_1, \dots, \alpha_n)$ for $i = 1, \dots, m$. Since $\gcd(m, k_1, \dots, k_n) = 1$ it follows that $m^2 \mid \text{disc}(\alpha_1, \dots, \alpha_n)$. \square

The cyclotomic fields $\mathbb{Q}(\zeta_m)$ form an important class of number fields. The field $\mathbb{Q}(\zeta_m)$ is of degree $\varphi(m)$, the Euler totient of m . The minimal polynomial of ζ_m over \mathbb{Q} is the cyclotomic polynomial $\Phi_m(X)$, the polynomial with the $\varphi(m)$ primitive m -th roots of unity as zeros. We will show that $\mathbb{Z}[\zeta_m]$ is the ring of integers of $\mathbb{Q}(\zeta_m)$.

1.48 Lemma. *Let $m \in \mathbb{N}^*$. For the \mathbb{Q} -basis $(1, \zeta_m, \zeta_m^2, \dots, \zeta_m^{\varphi(m)-1})$ of $\mathbb{Q}(\zeta_m)$ we have*

$$\text{disc}(1, \zeta_m, \zeta_m^2, \dots, \zeta_m^{\varphi(m)-1}) \mid m^{\varphi(m)}.$$

PROOF. We have $X^m - 1 = \Phi_m(X) \cdot h(X)$ with $h(X) \in \mathbb{Z}[X]$ a monic polynomial. Take the derivative:

$$mX^{m-1} = \Phi_m(X) \cdot h'(X) + \Phi_m'(X) \cdot h(X).$$

Evaluate at ζ_m :

$$m\zeta_m^{m-1} = \Phi_m'(\zeta_m)h(\zeta_m)$$

and so

$$\zeta_m h(\zeta_m) \cdot \Phi_m'(\zeta_m) = m.$$

Take norms:

$$N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_m)}(h(\zeta_m)) \cdot N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_m)}(\Phi_m'(\zeta_m)) = m^{\varphi(m)}.$$

From $h(X) \in \mathbb{Z}[X]$ it follows that $h(\zeta_m)$ is an integer of $\mathbb{Q}(\zeta_m)$ and so

$$N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_m)}(h(\zeta_m)) \in \mathbb{Z}.$$

Now the lemma follows from Proposition 1.29. \square

First we consider cyclotomic fields $\mathbb{Q}(\zeta_m)$ where m is a prime power.

1.6 The additive group of the ring of integers of a number field

1.49 Proposition. *Let p be a prime number and $r \in \mathbb{N}^*$. Then $\mathbb{Z}[\zeta_{p^r}]$ is the ring of integers of the cyclotomic field $\mathbb{Q}(\zeta_{p^r})$.*

PROOF. Write $\zeta_{p^r} = \zeta$ and $\varphi(p^r) = n$. By Lemma 1.48 p is the only prime divisor of $\text{disc}(1, \zeta, \dots, \zeta^{n-1})$. Since $\mathbb{Z}[\zeta] = \mathbb{Z}[1 - \zeta]$, we have by Proposition 1.41 $\text{disc}(1, \zeta, \dots, \zeta^{n-1}) = \text{disc}(1, 1 - \zeta, \dots, (1 - \zeta)^{n-1})$. By Lemma 1.47 it suffices to show that there are no $a_0, \dots, a_{n-1} \in \mathbb{Z}$ such that $\gcd(p, a_0, \dots, a_{n-1}) = 1$ and

$$\frac{a_0 + a_1(1 - \zeta) + \dots + a_{n-1}(1 - \zeta)^{n-1}}{p} \in \mathcal{O}.$$

Suppose such a_0, \dots, a_{n-1} do exist. Let i be the least index for which $p \nmid a_i$. Then the element

$$\alpha = \frac{a_i(1 - \zeta)^i + \dots + a_{n-1}(1 - \zeta)^{n-1}}{p}$$

is integral. Since $\Phi_{p^r}(1) = p$ we have

$$\prod_{\substack{0 \leq k < p^r \\ p \nmid k}} (1 - \zeta^k) = p,$$

from which it follows that $\frac{p}{(1 - \zeta)^{i+1}}$ is integral:

$$\frac{p}{(1 - \zeta)^{i+1}} = (1 - \zeta)^{n-i-1} \frac{p}{(1 - \zeta)^n} = (1 - \zeta)^{n-i-1} \prod_{\substack{0 \leq k < p^r \\ p \nmid k}} \frac{1 - \zeta^k}{1 - \zeta}.$$

Multiply α by this element:

$$\frac{p}{(1 - \zeta)^{i+1}} \alpha = \frac{a_i}{1 - \zeta} + (\text{element of } \mathbb{Z}[\zeta]).$$

It follows that $\frac{a_i}{1 - \zeta}$ is integral. Therefore,

$$N_{\mathbb{Q}}^{\mathbb{Q}(\zeta)} \left(\frac{a_i}{1 - \zeta} \right) = \frac{a_i^n}{p} \in \mathbb{Z},$$

which contradicts $p \nmid a_i$. □

For the general case we will use the following theorem.

1.50 Theorem. *Let K_1 and K_2 be number fields, K_1 of degree n_1 and K_2 of degree n_2 . Let $d_1 = \text{disc}(K_1)$, $d_2 = \text{disc}(K_2)$ and $d = \gcd(d_1, d_2)$. If, moreover, $K_1 K_2$ is of degree $n_1 n_2$, then*

$$d \cdot \mathcal{O}_{K_1 K_2} \subseteq \mathcal{O}_{K_1} \mathcal{O}_{K_2}.$$

1 Integers in a Number Field

PROOF. Let $(\alpha_1, \dots, \alpha_{n_1})$ be an integral basis of K_1 . Then the condition on K_1K_2 implies that $(\alpha_1, \dots, \alpha_{n_1})$ is also a K_2 -basis of K_1K_2 consisting of integral elements. We have $\mathcal{O}_{K_2}\alpha_1 + \dots + \mathcal{O}_{K_2}\alpha_{n_1} \subseteq \mathcal{O}_{K_1K_2}$. Let $\lambda_1, \dots, \lambda_{n_1}$ be the \mathbb{Q} -basis of K_1 satisfying $\text{Tr}_{\mathbb{Q}}^{K_1}(\alpha_i\lambda_j) = \delta_{ij}$. There are n_1 embeddings of K_1K_2 in \mathbb{C} leaving elements of K_2 fixed. Their restrictions to K_1 are just the n_1 embeddings of K_1 in \mathbb{C} . So we have

$$\text{Tr}_{K_2}^{K_1K_2}(\alpha_i\lambda_j) = \sigma_1(\alpha_i\lambda_j) + \dots + \sigma_{n_1}(\alpha_i\lambda_j) = \text{Tr}_{\mathbb{Q}}^{K_1}(\alpha_i\lambda_j) = \delta_{ij}.$$

By Proposition 1.36 we have

$$\begin{aligned} \mathcal{O}_{K_1}\mathcal{O}_{K_2} &= \mathcal{O}_{K_2}\alpha_1 + \dots + \mathcal{O}_{K_2}\alpha_{n_1} \subseteq \mathcal{O}_{K_1K_2} \subseteq \frac{1}{d_1}(\mathcal{O}_{K_2}\alpha_1 + \dots + \mathcal{O}_{K_2}\alpha_{n_1}) \\ &= \frac{1}{d_1}\mathcal{O}_{K_1}\mathcal{O}_{K_2}. \end{aligned}$$

So $d_1 \cdot \mathcal{O}_{K_1K_2} \subseteq \mathcal{O}_{K_1}\mathcal{O}_{K_2}$ and similarly $d_2 \cdot \mathcal{O}_{K_1K_2} \subseteq \mathcal{O}_{K_1}\mathcal{O}_{K_2}$. Since $\gcd(d_1, d_2) = d$, there are $a_1, a_2 \in \mathbb{Z}$ such that $d = a_1d_1 + a_2d_2$ and this implies

$$d \cdot \mathcal{O}_{K_1K_2} \subseteq d_1 \cdot \mathcal{O}_{K_1K_2} + d_2 \cdot \mathcal{O}_{K_1K_2} \subseteq \mathcal{O}_{K_1}\mathcal{O}_{K_2}. \quad \square$$

1.51 Theorem. *For each $m \in \mathbb{N}^*$ the ring $\mathbb{Z}[\zeta_m]$ is the ring of integers of $\mathbb{Q}(\zeta_m)$.*

PROOF. By induction on the number of prime divisors of m . The case of one prime divisor is Proposition 1.49. If m has more than one prime divisor, write $m = m_1m_2$ with $\gcd(m_1, m_2) = 1$ and $m_1, m_2 > 1$. By assumption we have

$$\mathcal{O}_{\mathbb{Q}(\zeta_{m_1})} = \mathbb{Z}[\zeta_{m_1}] \quad \text{and} \quad \mathcal{O}_{\mathbb{Q}(\zeta_{m_2})} = \mathbb{Z}[\zeta_{m_2}].$$

Note that $\mathbb{Q}(\zeta_{m_1})\mathbb{Q}(\zeta_{m_2}) = \mathbb{Q}(\zeta_{m_1}, \zeta_{m_2}) = \mathbb{Q}(\zeta_m)$ and similarly $\mathbb{Z}[\zeta_{m_1}]\mathbb{Z}[\zeta_{m_2}] = \mathbb{Z}[\zeta_m]$. Also note that

$$[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \varphi(m) = \varphi(m_1)\varphi(m_2) = [\mathbb{Q}(\zeta_{m_1}) : \mathbb{Q}] \cdot [\mathbb{Q}(\zeta_{m_2}) : \mathbb{Q}].$$

From Theorem 1.50 and Lemma 1.47 follows that $\mathcal{O}_{\mathbb{Q}(\zeta_m)} = \mathbb{Z}[\zeta_m]$. \square

1.52 Corollary. *Let $m \in \mathbb{N}^*$ with $m > 2$ and $\vartheta_m = \zeta_m + \zeta_m^{-1}$. Then $\mathbb{Z}[\vartheta_m]$ is the ring of integers of the number field $\mathbb{Q}(\vartheta_m)$.*

PROOF. Put $n = \frac{\varphi(m)}{2}$. Then $[\mathbb{Q}(\vartheta_m) : \mathbb{Q}] = n$ and it is easily shown that

$$\begin{aligned} \mathbb{Q}(\vartheta_m) &= \mathbb{Q} + \mathbb{Q}\vartheta_m + \mathbb{Q}\vartheta_m^2 + \dots + \mathbb{Q}\vartheta_m^{n-1} \\ &= \mathbb{Q} + \mathbb{Q} \cdot (\zeta_m + \zeta_m^{-1}) + \mathbb{Q} \cdot (\zeta_m^2 + \zeta_m^{-2}) + \dots + \mathbb{Q} \cdot (\zeta_m^{n-1} + \zeta_m^{-(n-1)}) \end{aligned}$$

and similarly

$$\begin{aligned} \mathbb{Z}[\vartheta_m] &= \mathbb{Z} + \mathbb{Z}\vartheta_m + \mathbb{Z}\vartheta_m^2 + \dots + \mathbb{Z}\vartheta_m^{n-1} \\ &= \mathbb{Z} + \mathbb{Z} \cdot (\zeta_m + \zeta_m^{-1}) + \mathbb{Z} \cdot (\zeta_m^2 + \zeta_m^{-2}) + \dots + \mathbb{Z} \cdot (\zeta_m^{n-1} + \zeta_m^{-(n-1)}). \end{aligned}$$

1.6 The additive group of the ring of integers of a number field

The ring of integers of $\mathbb{Q}(\vartheta_m)$ is $\mathbb{Z}[\zeta_m] \cap \mathbb{Q}(\vartheta_m)$. Let $\alpha \in \mathbb{Z}[\zeta_m] \cap \mathbb{Q}(\vartheta_m)$, say

$$\alpha = a_0 + a_1(\zeta_m + \zeta_m^{-1}) + \cdots + a_{n-1}(\zeta_m^{n-1} + \zeta_m^{-(n-1)})$$

with $a_0, a_1, \dots, a_{n-1} \in \mathbb{Q}$. Then

$$\zeta_m^{n-1} \alpha = a_{n-1} + a_{n-2} \zeta_m + \cdots + a_1 \zeta_m^{n-2} + a_0 \zeta_m^{n-1} + a_1 \zeta_m^n + \cdots + a_{n-1} \zeta_m^{2n-2}$$

and since $\zeta_m^{n-1} \alpha \in \mathbb{Z}[\zeta_m]$ it follows that $a_0, \dots, a_{n-1} \in \mathbb{Z}$, that is $\alpha \in \mathbb{Z}[\vartheta_m]$. \square

The ring of integers of a number field K is an example of a number ring of K . It is maximal among the number rings of K , since by Proposition 1.12 the elements of a number ring are integral. We have seen examples of number rings which are principal ideal domains. These examples were rings of integers of number fields. It is easy to see that this is necessarily so. Let a number ring R of K be a principal ideal domain and let $\alpha \in \mathcal{O}_K$. We will show that $\alpha \in R$. The field K is the field of fractions of R , so there are $\beta, \gamma \in R$ such that $\alpha = \frac{\beta}{\gamma}$. Since R is a principal ideal domain we can assume that $\gcd(\beta, \gamma) = 1$. Since α is integral, it is a zero of a monic polynomial $f \in \mathbb{Z}[X]$, say $f(X) = X^n + a_1 X^{n-1} + \cdots + a_n$. Then $\beta^n + a_1 \beta^{n-1} \gamma + \cdots + a_n \gamma^n = 0$ and this implies that $\gamma \mid \beta^n$. So an irreducible divisor of γ is also a divisor of β . But $\gcd(\beta, \gamma) = 1$. This means that γ has no irreducible divisors, that is γ is a unit of R . It follows that $\alpha = \beta \gamma^{-1} \in R$.

1.53 Example. The simplest example of a ring of integers which is not a principal ideal domain is $\mathbb{Z}[\sqrt{-5}]$, the ring of integers of the imaginary quadratic number field $\mathbb{Q}(\sqrt{-5})$. In this ring we have: $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. The elements 2, 3, $1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ are irreducible: their norms are 4, 9, 6 and 6 respectively and in $\mathbb{Z}[\sqrt{-5}]$ there are no elements of norm 2 or 3. So 6 has two different factorizations as a product of irreducible elements. Hence $\mathbb{Z}[\sqrt{-5}]$ is not a principal ideal domain.

For future reference we compute the discriminants of $\mathbb{Q}(\zeta_m)$ and $\mathbb{Q}(\zeta_m + \zeta_m^{-1})$ for m a prime power.

1.54 Proposition. *Let p be a prime number, $r \in \mathbb{N}^*$ and $p^r > 2$. Then*

$$\text{disc}(\mathbb{Q}(\zeta_{p^r})) = \pm p^{p^{r-1}(pr-r-1)}.$$

The discriminant is negative when $p \equiv 3 \pmod{4}$ or $p^r = 4$ and positive otherwise.

PROOF. The cyclotomic polynomial $\Phi_{p^r}(X)$ is the minimal polynomial of ζ_{p^r} over \mathbb{Q} . Since

$$\Phi_{p^r}(X) = \frac{X^{p^r} - 1}{X^{p^{r-1}} - 1},$$

we have

$$\Phi'_{p^r}(X) = \frac{(X^{p^{r-1}} - 1) \cdot p^r X^{p^r-1} - (X^{p^r} - 1) \cdot p^{r-1} X^{p^{r-1}-1}}{(X^{p^{r-1}} - 1)^2}$$

and so

$$\Phi'_{p^r}(\zeta_{p^r}) = \frac{p^r \zeta_{p^r}^{-1}}{\zeta_p - 1}.$$

Put $n = \varphi(p^r) = p^{r-1}(p-1)$. Then by Proposition 1.29:

$$\begin{aligned} \text{disc}(\mathbb{Q}(\zeta_{p^r})) &= (-1)^{\frac{1}{2}n(n-1)} N_{\mathbb{Q}}^{\mathbb{Q}(\zeta_{p^r})} \left(\frac{p^r \zeta_{p^r}^{-1}}{\zeta_p - 1} \right) \\ &= (-1)^{\frac{1}{2}n(n-1)} \frac{p^{rn}}{p^{n/(p-1)}} = (-1)^{\frac{1}{2}n(n-1)} p^{p^{r-1}(pr-r-1)}. \end{aligned}$$

The number $\frac{1}{2}n(n-1)$ is odd if and only if $p \equiv 3 \pmod{4}$ or $p^r = 4$. □

1.55 Proposition. *Let p be a prime number, $r \in \mathbb{N}^*$, $p^r > 4$ and $\vartheta_{p^r} = \zeta_{p^r} + \zeta_{p^r}^{-1}$. Then*

$$\text{disc}(\mathbb{Q}(\vartheta_{p^r})) = \begin{cases} (-1)^{\frac{p-1}{2}} p^{\frac{1}{2}(p^{r-1}(pr-r-1)-1)} & \text{if } p \text{ is odd,} \\ 2^{2^{r-2}(r-1)-1} & \text{if } p = 2. \end{cases}$$

PROOF. Put $L = \mathbb{Q}(\zeta_{p^r})$ and $K = \mathbb{Q}(\vartheta_{p^r})$. By Theorem 1.51 and Corollary 1.52 $\mathcal{O}_L = \mathbb{Z}[\zeta_{p^r}]$ and $\mathcal{O}_K = \mathbb{Z}[\vartheta_{p^r}]$. So $\mathcal{O}_L = \mathbb{Z}[\zeta_{p^r}] = \mathbb{Z}[\vartheta_{p^r}][\zeta_{p^r}] = \mathcal{O}_K[\zeta_{p^r}]$ and by Proposition 1.33

$$\text{disc}(L) = \text{disc}(K)^2 \cdot N_{\mathbb{Q}}^K(\text{disc}_K(1, \zeta_{p^r})).$$

The minimal polynomial of ζ_{p^r} over K is $X^2 - \vartheta_{p^r}X + 1$. So

$$\text{disc}_K(1, \zeta_{p^r}) = -N_K^L(2\zeta_{p^r} - \vartheta_{p^r}) = -N_K^L(\zeta_{p^r} - \zeta_{p^r}^{-1})$$

and

$$|N_{\mathbb{Q}}^K(\text{disc}_K(1, \zeta_{p^r}))| = N_{\mathbb{Q}}^L(\zeta_{p^r} - \zeta_{p^r}^{-1}) = \begin{cases} N_{\mathbb{Q}}^L(\zeta_{p^r}^2 - 1) = p & \text{if } p \text{ is odd,} \\ N_{\mathbb{Q}}^L(\zeta_{2^{r-1}-1}) = 4 & \text{if } p = 2. \end{cases}$$

By Proposition 1.54

$$\text{disc}(K)^2 = \begin{cases} p^{p^{r-1}(pr-r-1)-1} & \text{if } p \text{ is odd,} \\ 2^{2^{r-1}(r-1)-2} & \text{if } p = 2. \end{cases}$$

The sign of $\text{disc}(K)$ follows from Proposition 1.46. □

1.7 Norm-Euclidean quadratic number fields

One way to prove that a ring is a principal ideal domain is by showing it is a Euclidean domain. In this section we consider only quadratic number fields. Let m be squarefree $\neq 1$. The restriction of the norm $N = N_{\mathbb{Q}}^{\mathbb{Q}(\sqrt{m})} : \mathbb{Q}(\sqrt{m}) \rightarrow \mathbb{Q}$ to

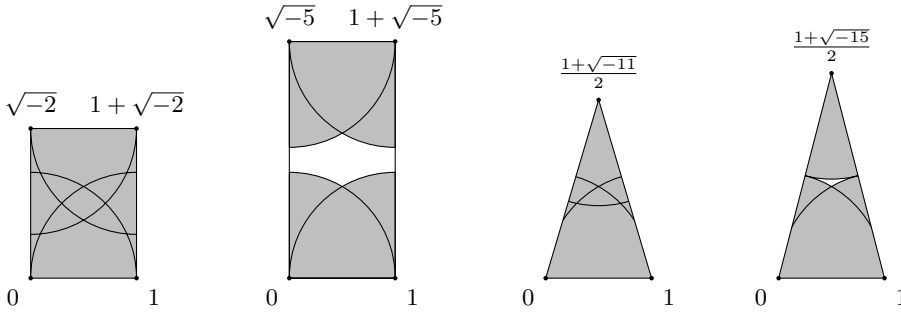


Figure 1.6: Points in \mathbb{C} (inside a rectangle or a triangle) with distance < 1 from $\mathbb{Z}[\omega_m]$ for $m = -2$, $m = -5$, $m = -11$ and $m = -15$

the ring of integers $\mathbb{Z}[\omega_m]$ takes values in \mathbb{Z} . For which m is the map $\alpha \mapsto |N(\alpha)|$ a Euclidean norm on $\mathbb{Z}[\omega_m]$? If it is, the number field $\mathbb{Q}(\sqrt{m})$ is called *norm-Euclidean*. We will see that for many m it is not.

We distinguish the imaginary and the real case.

Imaginary quadratic number fields

Let $\alpha, \beta \in \mathbb{Z}[\omega_m]$ with $\beta \neq 0$. Instead of $\alpha = \kappa\beta + \rho$, where $\kappa, \rho \in \mathbb{Z}[\omega_m]$, we can write $\frac{\alpha}{\beta} = \kappa + \frac{\rho}{\beta}$. The norm is Euclidean if elements $\frac{\rho}{\beta}$ are the sum of an integral element and an element of norm < 1 . The question becomes: for which m can \mathbb{C} be covered by open discs with radius 1 and center in $\mathbb{Z}[\omega_m]$?

Suppose $m \equiv 2, 3 \pmod{4}$. The distance of a complex number to $\mathbb{Z}[\omega_m]$ is at most $\sqrt{\frac{-m+1}{4}}$, the radius of the circumscribed circle of a rectangle with sides 1 and $\sqrt{-m}$. So the norm is a Euclidean norm if and only if $\frac{-m+1}{4} < 1$, that is $m > -3$. There are only two cases: $m = -1$ and $m = -2$.

Suppose $m \equiv 1 \pmod{4}$. The distance of a complex number to $\mathbb{Z}[\omega_m]$ is at most $\frac{-m+1}{4\sqrt{-m}}$, the radius of the circumscribed circle of a triangle with sides 1, $\sqrt{\frac{-m+1}{4}}$ and $\sqrt{\frac{-m+1}{4}}$. So the norm is a Euclidean norm if and only if $m > -7 - 4\sqrt{3}$, that is $m \geq -11$. There are three cases: $m = -3$, $m = -7$ and $m = -11$.

Thus we have found five norm-Euclidean imaginary quadratic number fields. These are in fact all imaginary quadratic number fields having a Euclidean ring of integers:

1.56 Theorem. For squarefree $m < 0$ we have:

$$\mathbb{Z}[\omega_m] \text{ is a Euclidean domain} \iff m = -1, -2, -3, -7 \text{ or } -11.$$

1 Integers in a Number Field

PROOF. We still have to prove the implication \Rightarrow . Suppose that for some $m \neq -1, -2, -3, -7, -11$ that there is a Euclidean norm $\psi: \mathbb{Z}[\omega_m] \setminus \{0\} \rightarrow \mathbb{N}$. We will derive a contradiction. Take in the set

$$\{ \beta \in \mathbb{Z}[\omega_m] \mid \beta \neq 0 \text{ and } \beta \notin \mathbb{Z}[\omega_m]^* \}$$

an element β with $\psi(\beta)$ minimal, i.e. $\beta \neq 0, 1, -1$ with $\psi(\beta)$ minimal. Note that $\mathbb{Z}[\omega_m]^* = \{1, -1\}$, since $m \neq -1, -3$. The residue class ring $\mathbb{Z}[\omega_m]/(\beta)$ consists of 2 or 3 elements:

Let $\alpha \in \mathbb{Z}[\omega_m]$. Then there are $\kappa, \rho \in \mathbb{Z}[\omega_m]$ with

$$\begin{cases} \alpha = \kappa\beta + \rho \\ \psi(\rho) < \psi(\beta) \quad \text{if } \rho \neq 0. \end{cases}$$

So $\rho = 0$ or $\rho \in \mathbb{Z}[\omega_m]^*$, that is $\rho \in \{0, 1, -1\}$, and this means that $\alpha \in (\beta)$ or $\alpha \in 1 + (\beta)$ or $\alpha \in -1 + (\beta)$. Because $\beta \notin \mathbb{Z}[\omega_m]^*$, the ring has 2 or 3 elements.

It follows that $N(\beta) = 2$ or $N(\beta) = 3$. However, as is easily verified, for $m \neq -1, -2, -3, -7, -11$ such a β does not exist. Contradiction. \square

Five of the imaginary quadratic number fields have a Euclidean ring of integers. These rings are principal ideal domains. But there are more: later we will see that also $\mathbb{Z}[\omega_{-19}]$, $\mathbb{Z}[\omega_{-43}]$, $\mathbb{Z}[\omega_{-67}]$ and $\mathbb{Z}[\omega_{-163}]$ are principal ideal domains.

Real quadratic number fields

Let $m \in \mathbb{Z}$ be squarefree and > 1 . The norm $N = N_{\mathbb{Q}(\sqrt{m})}^{\mathbb{Q}}: \mathbb{Q}(\sqrt{m}) \rightarrow \mathbb{Q}$ now also takes negative values, e.g. $N(\sqrt{m}) = -m$. Restriction to $\mathbb{Z}[\omega_m]$ yields a map $N: \mathbb{Z}[\omega_m] \rightarrow \mathbb{Z}$. The question is: for which m is the map $\mathbb{Z}[\omega_m] \rightarrow \mathbb{N}$, $\alpha \mapsto |N(\alpha)|$ a Euclidean norm on $\mathbb{Z}[\omega_m]$? For which m are there for each $\alpha, \beta \in \mathbb{Z}[\omega_m]$ with $\beta \neq 0$ numbers $\kappa, \rho \in \mathbb{Z}[\omega_m]$ such that

$$\alpha = \kappa\beta + \rho \quad \text{and} \quad |N(\rho)| < |N(\beta)|?$$

Via the embedding in $\mathbb{R} \times \mathbb{R}$ the ring $\mathbb{Z}[\omega_m]$ maps onto a lattice in $\mathbb{R} \times \mathbb{R}$. The points γ of $\mathbb{R} \times \mathbb{R}$ with $|N(\gamma)| < 1$ lie ‘inside’ the hyperbolas with equations $xy = \pm 1$. For which m is the plane covered by all translations of this domain over the vectors of the lattice? The following square, which is contained in this domain is easier to handle

$$\{ (x, y) \mid |x| + |y| < 2 \},$$

see Figure 1.7. Using this square instead already yields a number of Euclidean domains. Translation of the square over $(1, 1)$ does overlap with the original square.

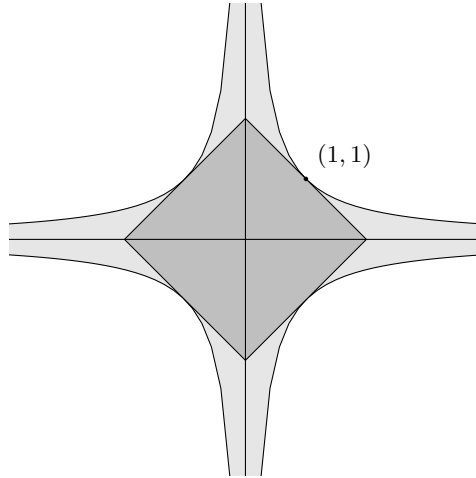


Figure 1.7: The domains $|xy| < 1$ and $|x| + |y| < 2$ inside $\mathbb{R} \times \mathbb{R}$

They also have to overlap under translation over $(\sqrt{m}, -\sqrt{m})$ for $m \equiv 2, 3 \pmod{4}$, respectively over $(\frac{1+\sqrt{m}}{2}, \frac{1-\sqrt{m}}{2})$ for $m \equiv 1 \pmod{4}$. The first is the case if $m < 4$ and the second if $m < 16$. See Figure 1.8. So we have:

1.57 Theorem. *The map $\mathbb{Z}[\omega_m] \rightarrow \mathbb{N}$, $\alpha \mapsto |N(\alpha)|$ is a Euclidean norm on $\mathbb{Z}[\omega_m]$ for $m = 2$, $m = 3$, $m = 5$ and $m = 13$. \square*

Here is a complete list of values of m for which $\mathbb{Z}[\omega_m] \rightarrow \mathbb{N}$, $\alpha \mapsto |N(\alpha)|$ is a Euclidean norm: $-11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$.

There are four negative m for which $\mathbb{Z}[\omega_m]$ is a non-Euclidean principal ideal domain. For positive m there are possibly infinitely many principal ideal domains; for $1 < m < 100$ the values of m for which $\mathbb{Q}(\sqrt{m})$ is not norm-Euclidean and $\mathbb{Z}[\omega_m]$ is a principal ideal domain are: $14, 22, 23, 31, 38, 43, 46, 47, 53, 59, 61, 62, 67, 69, 71, 77, 83, 86, 89, 93$ and 97 .

EXERCISES

1. Show that there is a one-to-one correspondence between quadratic number fields and squarefree integers $\neq 1$, where such an integer m corresponds to the field $\mathbb{Q}(\sqrt{m})$.
2. Show that $\mathbb{Z}[\sqrt{-6}]$, $\mathbb{Z}[\sqrt{-13}]$, $\mathbb{Z}[\frac{1+\sqrt{-15}}{2}]$ and $\mathbb{Z}[\sqrt{10}]$ are no principal ideal domains.

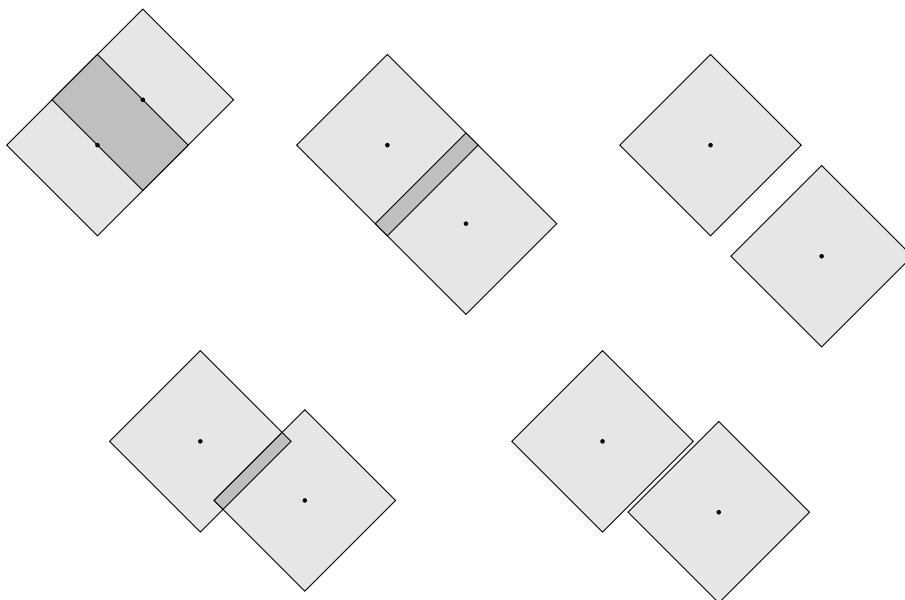


Figure 1.8: Overlap of squares in $\mathbb{R} \times \mathbb{R}$ under translation over respectively $(1, 1)$, $(\sqrt{3}, -\sqrt{3})$, $(\sqrt{6}, -\sqrt{6})$, $(\frac{1+\sqrt{13}}{2}, \frac{1-\sqrt{13}}{2})$ and $(\frac{1+\sqrt{17}}{2}, \frac{1-\sqrt{17}}{2})$

3. Let $K = \mathbb{Q}(\sqrt{m})$ with m a squarefree integer > 1 . Let's assume that $\mathcal{O}_K^* \neq \{1, -1\}$. Then, as explained in Example 1.24, K contains a fundamental unit.
 - (i) Suppose $m \equiv 2, 3 \pmod{4}$. Let $\nu_1, \nu_2 \in \mathcal{O}_K^*$ such that $\nu_2, \nu_1 > 1$. Then $\nu_1 = x_1 + y_1\sqrt{m}$, $\nu_2 = x_2 + y_2\sqrt{m}$ and $\nu_1\nu_2 = x_3 + y_3\sqrt{m}$ with $x_i, y_i \in \mathbb{N}^*$ for $i = 1, 2, 3$. Show that $y_3 > y_1, y_2$.
 - (ii) For $m \equiv 2, 3 \pmod{4}$ there exists a least $y \in \mathbb{N}^*$ such that $my^2 \pm 1$ is a square, say x^2 , in \mathbb{N}^* . Show that $x + y\sqrt{m}$ is the fundamental unit of K .
 - (iii) Suppose $m \equiv 1 \pmod{4}$ and $m \neq 5$. Let $\nu_1, \nu_2 \in \mathcal{O}_K^*$ such that $\nu_2, \nu_1 > 1$. Then $\nu_1 = \frac{1}{2}x_1 + \frac{1}{2}y_1\sqrt{m}$, $\nu_2 = \frac{1}{2}x_2 + \frac{1}{2}y_2\sqrt{m}$ and $\nu_1\nu_2 = \frac{1}{2}x_3 + \frac{1}{2}y_3\sqrt{m}$ with $x_i, y_i \in \mathbb{N}^*$ for $i = 1, 2, 3$. Show that $y_3 > y_1, y_2$.
 - (iv) For $m \equiv 1 \pmod{4}$ there exists a least $y \in \mathbb{N}^*$ such that $my^2 \pm 4$ is a square in \mathbb{N}^* , say x^2 . Show that $\frac{1}{2}x + \frac{1}{2}y\sqrt{m}$ is the fundamental unit of K if $m \neq 5$.
 - (v) Compute the fundamental units for $m = 11, 13, 14, 15, 17$. (This way of computing fundamental units is slow. For $m = 19$ the least y is 39 and for $m = 94$ it is 221064. A fast algorithm based on continued fractions is described in section 4.8.)
4. Show that for extensions $L : K$ of finite fields the group homomorphism $N_K^L : L^* \rightarrow K^*$ is surjective.

5. Let p be an odd prime. Show that $\mathbb{Q}(\zeta_p)$ contains a unique quadratic number field. Which one?
6. (i) Let $\alpha \in \mathbb{R}$ satisfy $\alpha^3 = \alpha + 1$. Show that $\mathbb{Z}[\alpha]$ is the ring of integers of $\mathbb{Q}(\alpha)$.
(ii) Let $\alpha \in \mathbb{R}$ satisfy $\alpha^3 = \alpha + 2$. Show that $\mathbb{Z}[\alpha]$ is the ring of integers of $\mathbb{Q}(\alpha)$.
7. Determine an integral basis of $\mathbb{Q}(\sqrt{-2 + \sqrt{2}})$.
8. Let $m \in \mathbb{Z}$ be not a cube in \mathbb{Z} . We determine an integral basis of the *pure cubic* number field $K = \mathbb{Q}(\sqrt[3]{m})$.
(i) Show that there are $h, k \in \mathbb{Z}$ such that $K = \mathbb{Q}(\sqrt[3]{h k^2})$, $\gcd(h, k) = 1$, h and k squarefree, $h k \neq 1$, $h \equiv 0, 1 \pmod{3}$ and $k \equiv 1 \pmod{3}$.
Put $\alpha = \sqrt[3]{h k^2}$ and $\beta = \sqrt[3]{h^2 k}$.
(ii) Let $\gamma = a + b\alpha + c\beta$, where $a, b, c \in \mathbb{Q}$. Verify:

$$\Delta_\gamma = X^3 - 3aX^2 + 3(a^2 - h k b c)X - (a^3 - 3h k a b c + h k^2 b^3 + h^2 k c^3).$$

(iii) Let p be a prime divisor of h or k . Let $\gamma = a + b\alpha + c\beta$ with $a, b, c \in \mathbb{Z}$. Show that $\frac{\gamma}{p} \notin \mathcal{O}$ if $\gcd(p, a, b, c) = 1$.
(iv) Suppose $h \equiv k \equiv 1 \pmod{3}$. Let γ be as in (iii). Show that if $\frac{\gamma}{3} \in \mathcal{O}$, then $a^2 \equiv b c \pmod{3}$ and $a + b + c \equiv 0 \pmod{3}$. Show that this implies that $a \equiv b \equiv c \pmod{3}$.
(v) Suppose $h \equiv k \equiv 1 \pmod{3}$ and let $\gamma = 1 + \alpha + \beta$. Show that

$$\frac{\gamma}{3} \in \mathcal{O} \iff 1 - 3hk + h k^2 + h^2 k \equiv 0 \pmod{27} \iff h \equiv k \pmod{9}.$$

(vi) Conclude that $(1, \alpha, \beta)$ is an integral basis of K if $h \not\equiv k \pmod{9}$ and that $(1, \alpha, \frac{1+\alpha+\beta}{3})$ is an integral basis if $h \equiv k \pmod{9}$.
(vii) Determine integral bases of $\mathbb{Q}(\sqrt[3]{m})$ for $m = 2, 3, 5, 6, 7, 12, 17, 18, 19, 20, 44$.
9. Let $m, n \in \mathbb{Z}$ be different and squarefree $\neq 1$. We determine an integral basis of the biquadratic field $K = \mathbb{Q}(\sqrt{m}, \sqrt{n})$. Put $k = \frac{mn}{\gcd(m, n)^2}$.
(i) Prove that $2\mathcal{O}_K \subseteq \mathbb{Z} + \mathbb{Z}\omega_m + \mathbb{Z}\omega_n + \mathbb{Z}\omega_k$. (Notation: see comment after Theorem 1.9. Hint: use the traces from K to quadratic subfields.)
(ii) Let $\alpha \in K$. Prove that $\alpha \in \mathcal{O}_K$ if and only if $N_{\mathbb{Q}(\sqrt{m})}^K(\alpha), \text{Tr}_{\mathbb{Q}(\sqrt{m})}^K(\alpha) \in \mathcal{O}$.
(iii) Show that there are essentially the following three cases:
(I) $m \equiv 3 \pmod{4}$ and $n, k \equiv 2 \pmod{4}$;
(II) $m \equiv 1 \pmod{4}$ and $n \equiv k \not\equiv 1 \pmod{4}$;
(III) $m \equiv n \equiv k \equiv 1 \pmod{4}$.
(iv) Show that an integral basis of K is for the above three cases as follows:
(I) $(1, \sqrt{m}, \sqrt{n}, \frac{\sqrt{n+\sqrt{k}}}{2})$;
(II) $(1, \frac{1+\sqrt{m}}{2}, \sqrt{n}, \frac{\sqrt{n+\sqrt{k}}}{2})$;
(III) $(1, \frac{1+\sqrt{m}}{2}, \frac{1+\sqrt{n}}{2}, \frac{1+\sqrt{m}}{2} \cdot \frac{1+\sqrt{k}}{2})$.

1 Integers in a Number Field

- (v) Prove that $\text{disc}(K) = \text{disc}(\mathbb{Q}(\sqrt{m})) \cdot \text{disc}(\mathbb{Q}(\sqrt{n})) \cdot \text{disc}(\mathbb{Q}(\sqrt{k}))$.
- (vi) Show that $(\mathcal{O}_K : \mathbb{Z} + \mathbb{Z}\omega_m + \mathbb{Z}\omega_n + \mathbb{Z}\omega_k) = 2$.
10. Diophantine equations of type $y^2 = x^3 + k$, where $k \in \mathbb{Z}$ and $k \neq 0$, are called *Mordell equations*. In this exercise we solve the equation for $k = -1$. Let $x, y \in \mathbb{Z}$ satisfy $y^2 + 1 = x^3$.
- (i) Show that x is odd and that y is even.
- (ii) Prove that $y + i$ is a cube in $\mathbb{Z}[i]$.
- (iii) Solve the Diophantine equation.
11. The Mordell equation for $k = -4$. Let $x, y \in \mathbb{Z}$ satisfy $y^2 + 4 = x^3$.
- (i) Show that $y + 2i$ is a cube in $\mathbb{Z}[i]$.
- (ii) Solve the equation.
12. Sometimes a Mordell equation can be solved using ordinary integers, for example for $k = 7$. Let $x, y \in \mathbb{Z}$ satisfy $y^2 = x^3 + 7$.
- (i) Show that x is odd and that y is even.
- (ii) Prove that $x^3 + 8$ has a prime divisor $\equiv 3 \pmod{4}$.
- (iii) Derive a contradiction.
13. Let K and L be number fields such that $[KL : \mathbb{Q}] = [K : \mathbb{Q}][L : \mathbb{Q}]$ and moreover $\text{gcd}(\text{disc}(K), \text{disc}(L)) = 1$. Prove that

$$\text{disc}(KL) = \text{disc}(K)^{[L:\mathbb{Q}]} \text{disc}(L)^{[K:\mathbb{Q}]}$$

14. Let $m, n \in \mathbb{N}^*$ be relatively prime. Show that

$$\text{disc}(\mathbb{Q}(\zeta_{mn})) = \text{disc}(\mathbb{Q}(\zeta_m))^{\varphi(n)} \text{disc}(\mathbb{Q}(\zeta_n))^{\varphi(m)}.$$

2 Dedekind Domains

Principal ideal domains are unique factorization domains: in a principal ideal domain there is unique factorization of nonzero elements as products of irreducible elements. Some rings of integers of number fields are principal ideal domains, but many are not. E.g. the ring of integers of $\mathbb{Q}(\sqrt{-5})$ is not a principal ideal domain, see Example 1.53. The notion of Dedekind domain is more general than that of principal ideal domain. In Dedekind domains there is a unique factorization not of elements, but of nonzero ideals, namely as a product of prime ideals. In chapter 3 it will be shown that rings of integers of number fields are Dedekind domains. In this chapter Dedekind domains are treated in general. In section 2.4 it is shown that the isomorphism classes of nonzero ideals of a Dedekind domain form a group, the ideal class group. This group is trivial if and only if the Dedekind domain is a principal ideal domain.

2.1 Definition

The notion of product of ideals is essential for our approach to Dedekind domains.

2.1 Definition. Let \mathfrak{a} and \mathfrak{b} be ideals of a commutative ring R . Their *product* is the ideal

$$\mathfrak{a}\mathfrak{b} = (ab \mid a \in \mathfrak{a} \text{ and } b \in \mathfrak{b}),$$

the ideal of R generated by all products ab with $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$.

The ideals of a commutative ring R form under multiplication an abelian monoid, in particular the multiplication is associative:

$$(\mathfrak{a}\mathfrak{b})\mathfrak{c} = \mathfrak{a}(\mathfrak{b}\mathfrak{c}) (= \mathfrak{a}\mathfrak{b}\mathfrak{c} = (abc \mid a \in \mathfrak{a}, b \in \mathfrak{b} \text{ and } c \in \mathfrak{c})).$$

The unity element is the ring R itself. For principal ideals we have $(a)(b) = (ab)$.

The *sum* $\mathfrak{a} + \mathfrak{b}$ of the ideals \mathfrak{a} and \mathfrak{b} consists of all $a + b$ with $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$. The union of systems of generators of the ideals \mathfrak{a} and \mathfrak{b} is a system of generators of $\mathfrak{a} + \mathfrak{b}$. Under addition the ideals form an abelian monoid as well. The ideal (0) is the zero element. The multiplication is distributive over the addition:

$$\mathfrak{a}(\mathfrak{b} + \mathfrak{c}) = \mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{c}.$$

2.2 Definition. Let \mathfrak{a} and \mathfrak{b} be ideals of an integral domain R . Then the ideal \mathfrak{a} is said to *divide* the ideal \mathfrak{b} (notation: $\mathfrak{a} \mid \mathfrak{b}$) if there exists an ideal \mathfrak{c} of R such that $\mathfrak{a}\mathfrak{c} = \mathfrak{b}$.

Note that for principal ideals we have:

$$(a) \mid (b) \iff a \mid b \iff b \in (a) \iff (a) \supseteq (b).$$

2.3 Definition. An integral domain R is called a *Dedekind domain* if R is not a field and for all ideals $\mathfrak{a}, \mathfrak{b}$ of R we have

$$\mathfrak{a} \mid \mathfrak{b} \iff \mathfrak{a} \supseteq \mathfrak{b}.$$

Note that “ \implies ” holds in general. If \mathfrak{a} is a principal ideal, then the converse is true as well: assume $\mathfrak{a} = (a)$ with $a \neq 0$ (otherwise it is trivially true) and $\mathfrak{a} \supseteq \mathfrak{b}$; then \mathfrak{b} consists of multiples of a and the ideal

$$\frac{1}{a}\mathfrak{b} = \left\{ \frac{b}{a} \mid b \in \mathfrak{b} \right\}$$

satisfies

$$\mathfrak{a} \cdot \frac{1}{a}\mathfrak{b} = \mathfrak{b}.$$

The collection of nonzero ideals of a Dedekind domain is a monoid with cancellation:

2.4 Proposition (Cancellation). *Let R be a Dedekind domain. Let $\mathfrak{a}, \mathfrak{c}$ and \mathfrak{c}' be ideals of R , where $\mathfrak{a} \neq 0$. Then*

$$\mathfrak{a}\mathfrak{c} \subseteq \mathfrak{a}\mathfrak{c}' \implies \mathfrak{c} \subseteq \mathfrak{c}'$$

and consequently

$$\mathfrak{a}\mathfrak{c} = \mathfrak{a}\mathfrak{c}' \implies \mathfrak{c} = \mathfrak{c}'.$$

PROOF. Since $\mathfrak{a} \neq (0)$, there is an $a \in \mathfrak{a}$ with $a \neq 0$. Because R is a Dedekind domain, there is an ideal \mathfrak{a}' such that $(a) = \mathfrak{a}\mathfrak{a}'$. We have $(a)\mathfrak{c} = \mathfrak{a}\mathfrak{a}'\mathfrak{c} \subseteq \mathfrak{a}'\mathfrak{a}\mathfrak{c}' = (a)\mathfrak{c}'$. Since R is an integral domain, it follows that $\mathfrak{c} \subseteq \mathfrak{c}'$. \square

In section 2.5 a characterization of Dedekind domains is given, which is based on three properties of Dedekind domains, the Propositions 2.6, 2.8 and 2.9. In Proposition 2.6 the following alternative for the definition of prime ideal will be used.

2.5 Lemma. *Let R be a commutative ring. Let \mathfrak{a} and \mathfrak{b} be ideals of R and let \mathfrak{p} be a prime ideal of R . Then*

$$\mathfrak{p} \supseteq \mathfrak{a}\mathfrak{b} \implies \mathfrak{p} \supseteq \mathfrak{a} \quad \text{or} \quad \mathfrak{p} \supseteq \mathfrak{b}.$$

PROOF. Suppose $\mathfrak{p} \supseteq \mathfrak{a}\mathfrak{b}$. If $\mathfrak{p} \not\supseteq \mathfrak{a}$, then there exists an $a \in \mathfrak{a} \setminus \mathfrak{p}$. Then $ab \in \mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$ for all $b \in \mathfrak{b}$. So $b \in \mathfrak{p}$ for all $b \in \mathfrak{b}$, since \mathfrak{p} is prime. Hence $\mathfrak{p} \supseteq \mathfrak{b}$. \square

2.6 Proposition. *Prime ideals $\neq (0)$ of a Dedekind domain are maximal ideals.*

PROOF. Let R be a Dedekind domain and $\mathfrak{p} \neq (0)$ a prime ideal of R . Let \mathfrak{a} be an ideal of R with $\mathfrak{p} \subseteq \mathfrak{a}$. Because R is a Dedekind domain, there is an ideal \mathfrak{b} of R such that $\mathfrak{a}\mathfrak{b} = \mathfrak{p}$. By Lemma 2.5 we have $\mathfrak{p} \supseteq \mathfrak{a}$ or $\mathfrak{p} \supseteq \mathfrak{b}$. In the first case we have $\mathfrak{p} = \mathfrak{a}$. In the second $\mathfrak{p} = \mathfrak{b}$ and by Proposition 2.4 we have $\mathfrak{a} = R$. So \mathfrak{p} is maximal. \square

2.7 Notation. For R a commutative ring, we denote the set of maximal ideals of R by $\text{Max}(R)$, and the collection of prime ideals of R by $\text{Spec}(R)$.

On $\text{Spec}(R)$ the so-called *Zariski topology* can be defined: the closed sets are the intersections of the sets

$$V(r) = \{ \mathfrak{p} \in \text{Spec}(R) \mid r \in \mathfrak{p} \},$$

where $r \in R$. The set of prime ideals of R equipped with the Zariski topology is called the *spectrum* of R . For R a Dedekind domain we have $\text{Max}(R) = \text{Spec}(R) \setminus \{(0)\}$ (Proposition 2.6). The *Krull dimension* of a commutative ring R is by definition the maximal length n of a chain

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n$$

of prime ideals of R . By Proposition 2.6 the Krull dimension of a Dedekind domain equals 1. Note that we excluded fields in the definition. Fields have Krull dimension 0. If there is an infinite chain of prime ideals, the Krull dimension is said to be infinite.

Ideals of a Dedekind domain are finitely generated: Dedekind domains are *Noetherian*. Equivalently, infinite ascending chains of ideals stabilize, or nonempty collections of ideals have a maximal element (an ideal in the collection not contained in any other ideal of the collection). The proof of these generalities is in many algebra textbooks. Here the proof of these equivalences is left as an exercise (exercise 2).

2.8 Proposition. *Dedekind domains are Noetherian.*

PROOF. Let $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \cdots$ be a chain of ideals of a Dedekind domain R . Then $\mathfrak{b} = \bigcup_i \mathfrak{a}_i$ is an ideal of R . We can assume that that $\mathfrak{b} \neq 0$. Since R is a Dedekind domain, there are a $b \in \mathfrak{b} \setminus \{0\}$ and an ideal \mathfrak{b}' of R such that $\mathfrak{b}\mathfrak{b}' = (b)$. Then $(b) = \bigcup_i \mathfrak{a}_i \mathfrak{b}'$. There is an $N \in \mathbb{N}^*$ such that $\mathfrak{a}_N \mathfrak{b}' = (b)$. Then $\mathfrak{a}_n \mathfrak{b}' = (b)$ for all $n \geq N$ and so by cancellation $\mathfrak{a}_n = \mathfrak{a}_N$ for all $n \geq N$. \square

The far most important property of Dedekind domains is the unique factorization of ideals: Theorem 2.11 in the next section. The definition of Dedekind domain (Definition 2.3) as presented here is quite close to this factorization property. In chapter 3 we will prove that the ring of integers of a number field is a Dedekind domain. This will not be done directly from the definition, but by proving the

three properties which will characterize Dedekind domains. The third of these is the following.

2.9 Proposition. *Dedekind domains are integrally closed.*

PROOF. Let R be a Dedekind domain with field of fractions K and let $a \in K$ be a zero of a monic $f \in R[X]$. We will prove that $a \in R$. Put $f(X) = X^n + b_1X^{n-1} + b_2X^{n-2} + \cdots + b_n$ and $a = \frac{a_1}{a_2}$ with $a_1, a_2 \in R$. Then

$$a_1^n + b_1a_1^{n-1}a_2 + b_2a_1^{n-2}a_2^2 + \cdots + b_na_2^n = a_2^n f(a) = 0$$

and so

$$a_1^n \in (a_1^{n-1}a_2, \dots, a_1a_2^{n-1}, a_2^n).$$

Put $\mathfrak{a} = (a_1^{n-1}, a_1^{n-2}a_2, \dots, a_1a_2^{n-2}, a_2^{n-1})$. Then

$$a_1\mathfrak{a} = (a_1^n, a_1^{n-1}a_2, \dots, a_1^2a_2^{n-2}, a_1a_2^{n-1}) \subseteq (a_1^{n-1}a_2, \dots, a_1^2a_2^{n-2}, a_1a_2^{n-1}, a_2^n) = a_2\mathfrak{a}.$$

Since R is a Dedekind domain it follows that $(a_1) \subseteq (a_2)$, that is $\frac{a_1}{a_2} \in R$. \square

2.2 Factorization of ideals

In a principal ideal domain we have unique factorization of nonzero elements. For a Dedekind domain we have unique factorization of nonzero ideals.

2.10 Notation. Let R be an integral domain. The set of nonzero ideals of R is denoted by $\mathbb{I}^+(R)$. Under the product of ideals it is an abelian monoid.

2.11 Theorem. *Let R be a Dedekind domain and $\mathfrak{a} \in \mathbb{I}^+(R)$. Then there are prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ such that $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_n$. This factorization is unique up to order. (We allow that $n = 0$: an empty product equals R .)*

PROOF. First we prove that every ideal $\mathfrak{a} \neq (0)$ is a product of prime ideals. If $\mathfrak{a} \neq R$, then there is a maximal ideal $\mathfrak{p}_1 \supseteq \mathfrak{a}$. Then, since R is a Dedekind domain, $\mathfrak{a} = \mathfrak{p}_1\mathfrak{a}_1$, where \mathfrak{a}_1 is a nonzero ideal. If $\mathfrak{a}_1 \neq R$, then continue with \mathfrak{a}_1 : there is a maximal ideal $\mathfrak{p}_2 \supseteq \mathfrak{a}_1$ such that $\mathfrak{a}_1 = \mathfrak{p}_2\mathfrak{a}_2$, etc. Since R is Noetherian, we thus obtain a strictly ascending chain $\mathfrak{a} = \mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots \subset \mathfrak{a}_n = R$ such that $\mathfrak{a}_{j-1} = \mathfrak{p}_j\mathfrak{a}_j$ with \mathfrak{p}_j a prime ideal for $j = 1, \dots, n$. Then $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_n$.

For the uniqueness of the factorization we use Lemma 2.5. Suppose that $\mathfrak{p}_1 \cdots \mathfrak{p}_n = \mathfrak{q}_1 \cdots \mathfrak{q}_m$ ($\mathfrak{p}_i, \mathfrak{q}_j$ being prime ideals $\neq (0)$ of R). Then $\mathfrak{p}_1 \mid \mathfrak{q}_1 \cdots \mathfrak{q}_m$ and so $\mathfrak{q}_1 \cdots \mathfrak{q}_m \subseteq \mathfrak{p}_1$. So there is a $\mathfrak{q}_i \subseteq \mathfrak{p}_1$. We may assume: $\mathfrak{q}_1 \subseteq \mathfrak{p}_1$. Since R is a Dedekind domain, the nonzero prime ideal \mathfrak{q}_1 is maximal, so $\mathfrak{q}_1 = \mathfrak{p}_1$. By cancellation: $\mathfrak{p}_2 \cdots \mathfrak{p}_n = \mathfrak{q}_2 \cdots \mathfrak{q}_m$. Proceed by induction. \square

2.12 Example. In Example 1.53 we saw that in the ring $\mathbb{Z}[\sqrt{-5}]$ there is no unique factorization of elements: the element 6 can be factored as a product of irreducible elements in two ways: $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. In $\mathbb{Z}[\sqrt{-5}]$ we have ideals

$$\mathfrak{p}_2 = (2, 1 + \sqrt{-5}), \quad \mathfrak{p}_3 = (3, 1 + \sqrt{-5}) \quad \text{and} \quad \mathfrak{p}'_3 = (3, 1 - \sqrt{-5}).$$

It is easily verified that the lattices $\mathbb{Z}2 + \mathbb{Z}(1 + \sqrt{-5})$, $\mathbb{Z}3 + \mathbb{Z}(1 + \sqrt{-5})$ and $\mathbb{Z}3 + \mathbb{Z}(1 - \sqrt{-5})$ are actually ideals of $\mathbb{Z}[\sqrt{-5}]$. From this it follows that they are the ideals \mathfrak{p}_2 , \mathfrak{p}_3 and \mathfrak{p}'_3 respectively. Because their indices in $\mathbb{Z}[\sqrt{-5}]$ are 2 or 3, these ideals are maximal ideals. It is easily verified that

$$(2) = \mathfrak{p}_2^2, \quad (3) = \mathfrak{p}_3\mathfrak{p}'_3, \quad (1 + \sqrt{-5}) = \mathfrak{p}_2\mathfrak{p}_3 \quad \text{and} \quad (1 - \sqrt{-5}) = \mathfrak{p}_2\mathfrak{p}'_3.$$

So the irreducible elements do not generate prime ideals. The two factorizations of the element 6 both lead to the same factorization of the ideal (6):

$$(6) = \mathfrak{p}_2^2\mathfrak{p}_3\mathfrak{p}'_3.$$

In the next chapter we show that rings of integers of number fields are Dedekind domains. In particular $\mathbb{Z}[\sqrt{-5}]$ is a Dedekind domain. For this example many verifications were needed. Later, having many structure theorems for rings of integers at our disposal, almost all of these computations become unnecessary.

2.13 Definition and notation. Let \mathfrak{p} be a prime ideal $\neq (0)$ of a Dedekind domain R and let \mathfrak{a} be an ideal $\neq (0)$ of R . The number of factors \mathfrak{p} in the factorization of \mathfrak{a} as a product of prime ideals is called the \mathfrak{p} -valuation of \mathfrak{a} and is denoted by $v_{\mathfrak{p}}(\mathfrak{a})$. So $v_{\mathfrak{p}}(\mathfrak{a}) \in \mathbb{N}$ and this number is given by

$$\mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})} \mid \mathfrak{a} \quad \text{and} \quad \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})+1} \nmid \mathfrak{a}.$$

(Let's agree that $\mathfrak{p}^0 = R$.) Thus we have a monoid homomorphism

$$v_{\mathfrak{p}}: \mathbb{I}^+(R) \rightarrow \mathbb{N}, \quad \mathfrak{a} \mapsto v_{\mathfrak{p}}(\mathfrak{a})$$

from the multiplicative monoid $\mathbb{I}^+(R)$ to the additive monoid \mathbb{N} .

For $a \in R \setminus \{0\}$ we have $aR \in \mathbb{I}^+(R)$ and we define

$$v_{\mathfrak{p}}(a) = v_{\mathfrak{p}}(aR).$$

Note that

$$v_{\mathfrak{p}}(\mathfrak{a}) = 0 \iff \mathfrak{p} \nmid \mathfrak{a}.$$

For each ideal $\mathfrak{a} \neq (0)$ we have

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})},$$

2 Dedekind Domains

where the product is over all $\mathfrak{p} \in \text{Max}(R)$. This formula makes sense: $v_{\mathfrak{p}}(\mathfrak{a}) \neq 0$ only for finitely many \mathfrak{p} and we can interpret the formula as the product over all \mathfrak{p} with $v_{\mathfrak{p}}(\mathfrak{a}) \neq 0$.

The unique factorization property implies that the map

$$(v_{\mathfrak{p}})_{\mathfrak{p}}: \mathbb{I}^+(R) \longrightarrow \bigoplus_{\mathfrak{p} \in \text{Max}(R)} \mathbb{N}, \quad \mathfrak{a} \mapsto (v_{\mathfrak{p}}(\mathfrak{a}))_{\mathfrak{p}} \quad (2.1)$$

is an isomorphism of abelian monoids: the product of $\mathfrak{a}, \mathfrak{b} \in \mathbb{I}^+(R)$ is given by

$$v_{\mathfrak{p}}(\mathfrak{a}\mathfrak{b}) = v_{\mathfrak{p}}(\mathfrak{a}) + v_{\mathfrak{p}}(\mathfrak{b}) \quad \text{for all } \mathfrak{p} \in \text{Max}(R).$$

To put it differently: for a Dedekind domain R the monoid $\mathbb{I}^+(R)$ is a free abelian monoid on the set $\text{Max}(R)$. The set $\mathbb{I}^+(R)$ is ordered by the relation \supseteq , which for Dedekind domains is the same as $|$. Under the isomorphism (2.1) $\mathfrak{a} | \mathfrak{b}$ translates into

$$v_{\mathfrak{p}}(\mathfrak{a}) \leq v_{\mathfrak{p}}(\mathfrak{b}) \quad \text{for all } \mathfrak{p} \in \text{Max}(R).$$

In the next proposition we consider two other operations: addition $((\mathfrak{a}, \mathfrak{b}) \mapsto \mathfrak{a} + \mathfrak{b})$ and intersection $((\mathfrak{a}, \mathfrak{b}) \mapsto \mathfrak{a} \cap \mathfrak{b})$.

2.14 Proposition. *Let \mathfrak{p} be a maximal ideal of a Dedekind domain R and let $\mathfrak{a}, \mathfrak{b} \in \mathbb{I}^+(R)$. Then:*

$$v_{\mathfrak{p}}(\mathfrak{a} + \mathfrak{b}) = \min(v_{\mathfrak{p}}(\mathfrak{a}), v_{\mathfrak{p}}(\mathfrak{b})) \quad \text{and} \quad v_{\mathfrak{p}}(\mathfrak{a} \cap \mathfrak{b}) = \max(v_{\mathfrak{p}}(\mathfrak{a}), v_{\mathfrak{p}}(\mathfrak{b})).$$

PROOF. Note that $\mathfrak{a} + \mathfrak{b}$ is the supremum of \mathfrak{a} and \mathfrak{b} in the ordering of $\mathbb{I}^+(R)$, whereas $\mathfrak{a} \cap \mathfrak{b}$ is the infimum. \square

In $\mathbb{I}^+(R)$ we clearly have the notion of greatest common divisor and least common multiple and the proposition tells us that $\text{gcd}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} + \mathfrak{b}$ and $\text{lcm}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} \cap \mathfrak{b}$. For elements a, b in a principal ideal domain we have:

$$\begin{aligned} (a)(b) &= (ab), \\ (a) + (b) &= (\text{gcd}(a, b)), \\ (a) \cap (b) &= (\text{lcm}(a, b)). \end{aligned}$$

The gcd and lcm of elements are defined up to units of the domain.

2.15 Definition. Nonzero ideals \mathfrak{a} and \mathfrak{b} of a Dedekind domain R are called *relatively prime* if they are comaximal, that is if $\mathfrak{a} + \mathfrak{b} = R$.

So ideals \mathfrak{a} and \mathfrak{b} of a Dedekind domain R are comaximal if and only if no $\mathfrak{p} \in \text{Max}(R)$ is a common divisor of \mathfrak{a} and \mathfrak{b} . In general, comaximality of ideals of a commutative ring has an important implication for the residue class rings:

2.16 Chinese Remainder Theorem. *Let R be a commutative ring and let \mathfrak{a} and \mathfrak{b} be comaximal ideals of R . Then the ring homomorphism $R \rightarrow R \times R$, $x \mapsto (x, x)$ induces an isomorphism*

$$R/\mathfrak{a}\mathfrak{b} \xrightarrow{\sim} R/\mathfrak{a} \times R/\mathfrak{b}.$$

PROOF. The kernel of the homomorphism

$$R \longrightarrow R/\mathfrak{a} \times R/\mathfrak{b}, \quad x \mapsto (\bar{x}, \bar{x})$$

is the ideal $\mathfrak{a}\mathfrak{b}$. By comaximality there are $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$ such that $a+b=1$. So for each $x \in \mathfrak{a}\mathfrak{b}$ one has $x = xa + xb \in \mathfrak{a}\mathfrak{b}$. Since trivially $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a}\mathfrak{b}$, it follows that $\mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{b}$. Surjectivity of the homomorphism follows from $ya + xb \equiv xb \equiv x \pmod{\mathfrak{a}}$ and $ya + xb \equiv ya \equiv y \pmod{\mathfrak{b}}$. \square

Unique factorization of ideals in Dedekind domains has implications for the structure of their residue class rings.

2.17 Proposition. *Let R be a Dedekind domain, \mathfrak{a} an ideal $\neq (0)$ of R and let \mathfrak{p} be a prime ideal $\neq (0)$ of R . Then the kernel of the surjective ring homomorphism*

$$\varphi: R/\mathfrak{p}\mathfrak{a} \rightarrow R/\mathfrak{a}, \quad x + \mathfrak{p}\mathfrak{a} \mapsto x + \mathfrak{a},$$

is an R -module isomorphic to R/\mathfrak{p} .

PROOF. Clearly $\text{Ker}(\varphi) = \mathfrak{a}/\mathfrak{p}\mathfrak{a}$. From $\mathfrak{p}\mathfrak{a} \subseteq \mathfrak{a}$ and the unique factorization follows that $\mathfrak{p}\mathfrak{a} \subset \mathfrak{a}$. Choose $a \in \mathfrak{a} \setminus \mathfrak{p}\mathfrak{a}$. Then there is an ideal \mathfrak{b} such that $\mathfrak{a}\mathfrak{b} = aR$. We have $\mathfrak{p} \nmid \mathfrak{b}$, since otherwise $\mathfrak{p}\mathfrak{a} \mid \mathfrak{a}\mathfrak{b}$ and so $a \in \mathfrak{p}\mathfrak{a}$. Note that $\mathfrak{a}\mathfrak{b} \cap \mathfrak{p}\mathfrak{a} = \mathfrak{a}\mathfrak{b}\mathfrak{p}$ and $\mathfrak{a}\mathfrak{b} + \mathfrak{p}\mathfrak{a} = \mathfrak{a}$. The inclusion $aR \subseteq \mathfrak{a}$ induces an R -module homomorphism

$$\psi: aR/\mathfrak{a}\mathfrak{p} \rightarrow \mathfrak{a}/\mathfrak{p}\mathfrak{a}.$$

We prove that ψ is an isomorphism:

$$\text{Ker}(\psi) = (aR \cap \mathfrak{p}\mathfrak{a})/\mathfrak{a}\mathfrak{p} = (\mathfrak{a}\mathfrak{b} \cap \mathfrak{p}\mathfrak{a})/\mathfrak{a}\mathfrak{p} = \mathfrak{a}\mathfrak{b}\mathfrak{p}/\mathfrak{a}\mathfrak{p} = \mathfrak{a}\mathfrak{p}/\mathfrak{a}\mathfrak{p} = 0.$$

$$\text{Im}(\psi) = (aR + \mathfrak{p}\mathfrak{a})/\mathfrak{p}\mathfrak{a} = (\mathfrak{a}\mathfrak{b} + \mathfrak{p}\mathfrak{a})/\mathfrak{p}\mathfrak{a} = \mathfrak{a}/\mathfrak{p}\mathfrak{a}.$$

Clearly the R -module isomorphism $R \rightarrow aR$, $r \mapsto ar$ induces an isomorphism $R/\mathfrak{p} \xrightarrow{\sim} aR/\mathfrak{a}\mathfrak{p}$. Hence,

$$R/\mathfrak{p} \cong aR/\mathfrak{a}\mathfrak{p} \cong \mathfrak{a}/\mathfrak{p}\mathfrak{a} = \text{Ker}(\varphi). \quad \square$$

In terms of exact sequences: there is a short exact sequence

$$0 \longrightarrow R/\mathfrak{p} \longrightarrow R/\mathfrak{p}\mathfrak{a} \longrightarrow R/\mathfrak{a} \longrightarrow 0$$

of R -modules. Note that if $\mathfrak{p} \nmid \mathfrak{a}$, then by the Chinese Remainder Theorem we have an isomorphism $R/\mathfrak{p}\mathfrak{a} \xrightarrow{\sim} R/\mathfrak{p} \times R/\mathfrak{a}$. In this case the short exact sequence splits and the proposition follows in a direct manner. So the more interesting aspect of the proposition is that it holds if $\mathfrak{p} \mid \mathfrak{a}$ as well.

Ideals of a Dedekind domain may not be principal, but since the domain is Noetherian, they are finitely generated. In fact at most two elements are needed for the generation of an ideal. This will follow from:

2.18 Lemma. *Let R be a Dedekind domain, P a finite collection of maximal ideals of R and $\mathfrak{p} \in P$. Then there exists an $x \in R$ satisfying $v_{\mathfrak{p}}(x) = 1$ and $v_{\mathfrak{q}}(x) = 0$ for all $\mathfrak{q} \in P \setminus \{\mathfrak{p}\}$.*

PROOF. Choose a $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$. Such an element exists because $\mathfrak{p} \neq \mathfrak{p}^2$ by the cancellation property. By the Chinese Remainder Theorem there exists an $x \in R$ such that

$$x \equiv \begin{cases} \pi \pmod{\mathfrak{p}^2}, \\ 1 \pmod{\mathfrak{q}} \end{cases} \text{ for each } \mathfrak{q} \in P \setminus \{\mathfrak{p}\}.$$

Then $x \in \mathfrak{p}$, $x \notin \mathfrak{p}^2$ and $x \notin \mathfrak{q}$ for all $\mathfrak{q} \in P$ with $\mathfrak{q} \neq \mathfrak{p}$. □

2.19 Proposition. *Let R be a Dedekind domain and let \mathfrak{a} and \mathfrak{b} be nonzero ideals of R such that $\mathfrak{a} \subseteq \mathfrak{b}$. Then there exists an $x \in \mathfrak{b}$ such that $\mathfrak{b} = \mathfrak{a} + xR$.*

PROOF. Let P be the collection of prime divisors of \mathfrak{a} . By Lemma 2.18 we can choose for each $\mathfrak{p} \in P$ an $x_{\mathfrak{p}} \in R$ such that $v_{\mathfrak{p}}(x_{\mathfrak{p}}) = 1$ and $v_{\mathfrak{q}}(x_{\mathfrak{p}}) = 0$ for all $\mathfrak{q} \in P \setminus \{\mathfrak{p}\}$. Take

$$x = \prod_{\mathfrak{p} \in P} x_{\mathfrak{p}}^{v_{\mathfrak{p}}(\mathfrak{b})}.$$

Then $v_{\mathfrak{p}}(x) = v_{\mathfrak{p}}(\mathfrak{b})$ for all $\mathfrak{p} \mid \mathfrak{a}$. By Proposition 2.14 we have $\mathfrak{a} + xR = \mathfrak{b}$. □

2.20 Corollary. *Let \mathfrak{a} be an ideal of a Dedekind domain R . Then there are $a, b \in R$ such that $\mathfrak{a} = (a, b)$.*

PROOF. We may assume that $\mathfrak{a} \neq 0$. Take $a \in \mathfrak{a}$ with $a \neq 0$. By Lemma 2.19 there is a $b \in R$ such that $\mathfrak{a} = aR + bR = (a, b)$. □

Commutative rings with only finitely many maximal ideals are called *semi-local*.

2.21 Proposition. *Semi-local Dedekind domains are principal ideal domains.*

PROOF. Let R be a Dedekind domain with $\text{Max}(R)$ finite. It suffices to prove that maximal ideals of R are principal. Let \mathfrak{p} be a maximal ideal of R . By Lemma 2.18 there is an $x \in R$ such that $v_{\mathfrak{p}}(x) = 1$ and $v_{\mathfrak{q}}(x) = 0$ for all maximal ideals $\mathfrak{q} \neq \mathfrak{p}$. It follows that $\mathfrak{p} = xR$. □

2.3 The ideal class group of a Dedekind domain

2.22 Definition. Let R be an integral domain and $\mathfrak{a}, \mathfrak{b} \in \mathbb{I}^+(R)$. Then \mathfrak{a} and \mathfrak{b} are called *equivalent* if there exist nonzero $x, y \in R$ such that $x\mathfrak{a} = y\mathfrak{b}$. Notation: $\mathfrak{a} \sim \mathfrak{b}$.

Note that $x\mathfrak{a} \in \mathbb{I}^+(R)$. It can be seen as the product of the principal ideal (x) and the ideal \mathfrak{a} .

2.23 Lemma. *Equivalence of nonzero ideals of an integral domain R is an equivalence relation in $\mathbb{I}^+(R)$.*

PROOF. Obviously the relation is reflexive and symmetric. For transitivity it is needed that the ring has no zero divisors. \square

For Dedekind domains we have the following property, which—as we will see—has many consequences.

2.24 Lemma. *Let R be a Dedekind domain and $\mathfrak{a} \in \mathbb{I}^+(R)$. Then there is a $\mathfrak{b} \in \mathbb{I}^+(R)$ such that $\mathfrak{a}\mathfrak{b}$ is a principal ideal.*

PROOF. Choose $a \in \mathfrak{a}$ with $a \neq 0$. Then $\mathfrak{a} \supseteq (a)$ and hence $\mathfrak{a} \mid (a)$, that is $(a) = \mathfrak{a}\mathfrak{b}$ for a $\mathfrak{b} \in \mathbb{I}^+(R)$. \square

2.25 Proposition. *Let R be a Dedekind domain. Multiplication in $\mathbb{I}^+(R)$ induces a group structure on the set $\mathbb{I}^+(R)/\sim$ of equivalence classes.*

PROOF. Clearly, if $\mathfrak{a}, \mathfrak{a}', \mathfrak{b}, \mathfrak{b}' \in \mathbb{I}^+(R)$ satisfy $\mathfrak{a}' \sim \mathfrak{a}$ and $\mathfrak{b}' \sim \mathfrak{b}$, then $\mathfrak{a}'\mathfrak{b}' \sim \mathfrak{a}\mathfrak{b}$. Let's denote the class of \mathfrak{a} by $[\mathfrak{a}]$. It follows that $\mathbb{I}^+(R)/\sim$ is an abelian monoid under the operation $[\mathfrak{a}] \cdot [\mathfrak{b}] = [\mathfrak{a}\mathfrak{b}]$. The unit element is $[(1)]$, which is the class of principal ideals. By Lemma 2.24 for each $\mathfrak{a} \in \mathbb{I}^+(R)$ there is a $\mathfrak{b} \in \mathbb{I}^+(R)$ such that $[\mathfrak{a}] \cdot [\mathfrak{b}] = [\mathfrak{a}\mathfrak{b}] = [(a)] = [(1)]$, so the class $[\mathfrak{b}]$ is the inverse of $[\mathfrak{a}]$. \square

2.26 Definition and notation. Let R be a Dedekind domain. The equivalence classes in $\mathbb{I}^+(R)$ are called *ideal classes* and the group $\mathbb{I}^+(R)/\sim$ is called the *ideal class group* of R . Notation: $\mathcal{C}\ell(R)$. The class of an $\mathfrak{a} \in \mathbb{I}^+(R)$ is denoted by $[\mathfrak{a}]$.

As remarked in the proof of Proposition 2.25 the unity element of the ideal class group of a Dedekind domain consists of all principal ideals of that domain. So in a sense the ideal class group tells us how much a Dedekind domain deviates from a principal ideal domain:

2.27 Proposition. *Let R be a Dedekind domain. Then R is a principal ideal domain if and only if the group $\mathcal{C}\ell(R)$ is trivial.* \square

By Proposition 2.21 only Dedekind domains with infinitely many maximal ideals can have a nontrivial ideal class group. In chapter 1 examples were given of rings of integers of number fields which are not principal ideal domains. In the next chapter it will be shown that rings of integers of number fields are Dedekind domains. So each ring of integers which is not a principal ideal domain, is a Dedekind domain with a nontrivial ideal class group.

Representing ideals of ideal classes of a Dedekind domain can be chosen to be comaximal with a given nonzero ideal:

2.28 Proposition. *Let R be a Dedekind domain and let \mathfrak{a} and \mathfrak{b} be nonzero ideals of R . Then there is an ideal \mathfrak{c} of R such that $\mathfrak{c} \sim \mathfrak{a}$ and $\mathfrak{b} + \mathfrak{c} = R$.*

PROOF. Take $a \in \mathfrak{a}$ with $a \neq 0$. Then $aR = \mathfrak{a}\mathfrak{a}'$ for an ideal \mathfrak{a}' of R . From Lemma 2.19 it follows that there is an $x \in R$ such that $\mathfrak{a}' = \mathfrak{a}'\mathfrak{b} + xR$. Then $aR = \mathfrak{a}\mathfrak{a}' = \mathfrak{a}\mathfrak{a}'\mathfrak{b} + xa = a\mathfrak{b} + xR$. So take $\mathfrak{c} = \frac{x}{a}\mathfrak{a}$. \square

2.4 Fractional ideals

Ideals in a commutative ring R are R -submodules of the R -module R . For an integral domain R we consider a larger collection of R -modules isomorphic to ideals of R .

2.29 Definition. Let R be an integral domain and K its field of fractions. A nonzero R -submodule \mathfrak{a} of K is called a *fractional ideal* of R if there is an $x \in K^*$ such that $x\mathfrak{a} \subseteq R$. The set of fractional ideals of R is denoted by $\mathbb{I}(R)$. Fractional ideals Ra with $a \in K^*$ are called *principal* fractional ideals. The set of principal fractional ideals of R is denoted by $\mathbb{P}(R)$.

For Noetherian integral domains we have an alternative characterization:

2.30 Lemma. *Let R be a Noetherian integral domain with field of fractions K and let \mathfrak{a} be a nonzero R -submodule of K . Then:*

$$\mathfrak{a} \text{ is a fractional ideal of } R \iff \mathfrak{a} \text{ is a finitely generated } R\text{-module.}$$

PROOF. Fractional ideals of R are isomorphic to ideals of R and these are by definition finitely generated. On the other hand, if an R -submodule of K is finitely generated, then there is a nonzero $x \in R$ such that $x\mathfrak{a} \subseteq R$: for x one can take the product of the denominators of the fractions generating \mathfrak{a} . \square

Fractional ideals are R -submodules of K and as such they can be added: $\mathfrak{a} + \mathfrak{b} = \{a + b \mid a \in \mathfrak{a}, b \in \mathfrak{b}\}$. Using the multiplication in the field of fractions there also is a multiplication of fractional ideals as there is one for ideals of R :

2.31 Definition. Let R be a Noetherian integral domain with field of fractions K and let \mathfrak{a} and \mathfrak{b} be fractional ideals of R . The *product* $\mathfrak{a}\mathfrak{b}$ of \mathfrak{a} and \mathfrak{b} is the R -submodule of K generated by all ab with $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$.

Note that if \mathfrak{a} and \mathfrak{b} are fractional ideals, say $x\mathfrak{a} \subseteq R$ and $y\mathfrak{b} \subseteq R$, where x and y are nonzero elements of R . Then $xy\mathfrak{a}\mathfrak{b} \subseteq R$. Hence $\mathfrak{a}\mathfrak{b}$ is indeed a fractional ideal.

2.32 Lemma. *Let R be a Noetherian integral domain. Then the set $\mathbb{I}(R)$ is an abelian monoid under the multiplication of fractional ideals. The ring R is the unit element of the monoid. Moreover, the multiplication is distributive over the addition.*

PROOF. The proof is straightforward. \square

2.33 Definition. Let R be a Noetherian integral domain. A fractional ideal of R is called *invertible* if it is an invertible element of the monoid $\mathbb{I}(R)$. If $\mathfrak{a} \in \mathbb{I}(R)$ is invertible, then \mathfrak{a}^{-1} is also denoted by $\frac{1}{\mathfrak{a}}$ or $\frac{R}{\mathfrak{a}}$. More generally, a product $\mathfrak{a}^{-1}\mathfrak{b}$ is also denoted by $\frac{\mathfrak{b}}{\mathfrak{a}}$.

2.34 Lemma. Let R be a Noetherian integral domain and $\mathfrak{a}, \mathfrak{b} \in \mathbb{I}(R)$ invertible. Then:

$$\mathfrak{a} \supseteq \mathfrak{b} \iff \mathfrak{a}^{-1} \subseteq \mathfrak{b}^{-1}.$$

PROOF. If $\mathfrak{a} \supseteq \mathfrak{b}$, then $\mathfrak{a}^{-1} = \mathfrak{a}^{-1}\mathfrak{b}\mathfrak{b}^{-1} \subseteq \mathfrak{a}^{-1}\mathfrak{a}\mathfrak{b}^{-1} = \mathfrak{b}^{-1}$. \square

2.35 Theorem. Let R be a Noetherian integral domain. Then R is a Dedekind domain if and only if the monoid $\mathbb{I}(R)$ is a group.

PROOF. Let R be a Dedekind domain and $\mathfrak{a} \in \mathbb{I}(R)$. There is a nonzero $x \in R$ such that $x\mathfrak{a} \subseteq R$. Let y be a nonzero element of the ideal $x\mathfrak{a}$. Then $yR \subseteq x\mathfrak{a}$. Since R is a Dedekind domain, there is an ideal \mathfrak{b} of R such that $x\mathfrak{a} \cdot \mathfrak{b} = yR$. It follows that the fractional ideal $\frac{x}{y}\mathfrak{b}$ is the inverse of \mathfrak{a} . So all fractional ideals of R are invertible, that is $\mathbb{I}(R)$ is a group. Conversely, suppose $\mathbb{I}(R)$ is a group and let $\mathfrak{a}, \mathfrak{b} \in \mathbb{I}^+(R)$ satisfy $\mathfrak{a} \supseteq \mathfrak{b}$. Then $\mathfrak{b} = \mathfrak{a}(\mathfrak{b}\mathfrak{a}^{-1})$ and by Lemma 2.34 $\mathfrak{b}\mathfrak{a}^{-1} \subseteq \mathfrak{b}\mathfrak{b}^{-1} = R$. Hence $\mathfrak{a} \mid \mathfrak{b}$. \square

2.36 Theorem. Let R be a Dedekind domain. Then $\mathbb{I}(R)$ is a free abelian group with the set $\text{Max}(R)$ as a basis.

PROOF. The monoid $\mathbb{I}^+(R)$ is freely generated by the maximal ideals of R . This implies that the group $\mathbb{I}(R)$ is freely generated as an abelian group by the maximal ideals. \square

We can now extend the definition of $v_{\mathfrak{p}}$ for nonzero ideals in a Dedekind domain to the group $\mathbb{I}(R)$:

2.37 Definition. Let R be a Dedekind domain. The maps $v_{\mathfrak{p}}: \mathbb{I}(R) \rightarrow \mathbb{Z}$ are the coordinate maps corresponding to the basis of maximal ideals \mathfrak{p} of R . The map $v_{\mathfrak{p}}$ is called the *\mathfrak{p} -adic valuation* of $\mathbb{I}(R)$. For $a \in K^*$ we put $v_{\mathfrak{p}}(a) = v_{\mathfrak{p}}(Ra)$. Thus we also have a group homomorphism $v_{\mathfrak{p}}: K^* \rightarrow \mathbb{Z}$, the *\mathfrak{p} -adic valuation* on K .

So for a Dedekind domain R we have a group isomorphism

$$\mathbb{I}(R) \xrightarrow{\sim} \bigoplus_{\mathfrak{p} \in \text{Max}(R)} \mathbb{Z}, \quad \mathfrak{a} \mapsto (v_{\mathfrak{p}}(\mathfrak{a}))_{\mathfrak{p}}.$$

The abelian group $\bigoplus_{\mathfrak{p}} \mathbb{Z}$ is the group completion of the abelian monoid $\bigoplus_{\mathfrak{p}} \mathbb{N}$ and the group $\mathbb{I}(R)$ of fractional ideals is the group completion of the monoid $\mathbb{I}^+(R)$ of nonzero ideals.

2.38 Lemma. Let R be a Dedekind domain. Then $\mathbb{P}(R)$ is a subgroup of $\mathbb{I}(R)$.

PROOF. For nonzero a, b in the field of fractions of R we have $Ra \cdot Rb = Rab$ and in particular $Ra \cdot Ra^{-1} = R$. \square

2.39 Proposition. *Let R be a Dedekind domain. Then the inclusion $\mathbb{I}^+(R) \rightarrow \mathbb{I}(R)$ induces an isomorphism $\mathcal{C}(R) \xrightarrow{\sim} \mathbb{I}(R)/\mathbb{P}(R)$.*

PROOF. The map $\mathbb{I}^+(R) \rightarrow \mathbb{I}(R)/\mathbb{P}(R)$ is surjective. Ideals $\mathfrak{a}, \mathfrak{b} \in \mathbb{I}^+(R)$ are congruent modulo $\mathbb{P}(R)$ if and only if there is an $a \in K^*$ such that $\mathfrak{a} = a\mathfrak{b}$. Put $a = \frac{y}{x}$ with $x, y \in R \setminus \{0\}$. Then $x\mathfrak{a} = y\mathfrak{b}$, that is $\mathfrak{a} \sim \mathfrak{b}$. \square

So for a Dedekind domain R with field of fractions K we have an exact sequence

$$1 \longrightarrow R^* \longrightarrow K^* \longrightarrow \mathbb{I}(R) \longrightarrow \mathcal{C}(R) \longrightarrow 1.$$

The map $K^* \rightarrow \mathbb{I}(R)$ sends a to Ra . The fractional ideal Ra is the unit element R of the group $\mathbb{I}(R)$ if and only if $a \in R^*$. Alternatively, we have an exact sequence

$$1 \longrightarrow R^* \longrightarrow K^* \xrightarrow{(v_{\mathfrak{p}})_{\mathfrak{p}}} \bigoplus_{\mathfrak{p}} \mathbb{Z} \longrightarrow \mathcal{C}(R) \longrightarrow 1. \quad (2.2)$$

For each \mathfrak{p} the map $\mathbb{Z} \rightarrow \mathcal{C}(R)$ sends 1 to $[\mathfrak{p}]$.

2.5 Characterization of Dedekind domains

We have seen in section 2.1 that Dedekind domains are integrally closed Noetherian domains in which nonzero prime ideals are maximal. In this section we prove the converse. This converse (Theorem 2.43) is the main tool for identifying Dedekind domains in many cases. A direct consequence is that the integral closure of a Dedekind domain in a finite separable extension of its field of fractions is a Dedekind domain as well (Theorem 2.45). This applies directly to the rings of integers of a number field (Theorem 2.46), being the integral closure of \mathbb{Z} in the number field.

2.40 Lemma. *Let R be an integrally closed integral domain with field of fractions K and let $a \in K^*$. Then $a \in R$ if and only if there is a finitely generated nonzero submodule A of K such $aA \subseteq A$.*

PROOF. This follows from Proposition 1.12. \square

2.41 Lemma. *In a Noetherian ring every nonzero ideal contains a product of nonzero prime ideals.*

PROOF. Let R be a Noetherian ring and suppose that there exists an ideal $\mathfrak{a} \neq (0)$ of R that does not contain a product of prime ideals $\neq (0)$. Then the collection Φ of such ideals is nonempty. Since R is Noetherian, the collection Φ has a maximal element, say \mathfrak{m} . Then \mathfrak{m} clearly is not a prime ideal, so there are $a, b \in R$ with $a, b \notin \mathfrak{m}$ and $ab \in \mathfrak{m}$. We have $\mathfrak{m} \subset \mathfrak{m} + (a)$ and $\mathfrak{m} \subset \mathfrak{m} + (b)$. Since \mathfrak{m} is maximal in

Φ , the ideals $\mathfrak{m} + (a)$ and $\mathfrak{m} + (b)$ both contain a product of nonzero prime ideals. But then $(\mathfrak{m} + (a))(\mathfrak{m} + (b))$ contains such a product as well. However,

$$(\mathfrak{m} + (a))(\mathfrak{m} + (b)) = \mathfrak{m}^2 + a\mathfrak{m} + b\mathfrak{m} + (ab) \subseteq \mathfrak{m},$$

in contradiction with $\mathfrak{m} \in \Phi$. □

2.42 Lemma. *Let R be a Noetherian domain with the property that nonzero prime ideals of R are maximal. Let \mathfrak{a} be an ideal of R with $(0) \neq \mathfrak{a} \neq R$. Then there exists an element $c \in K$, the field of fractions of R , such that $c \notin R$ and $c\mathfrak{a} \subseteq R$.*

PROOF. Let $a \in \mathfrak{a}$ with $a \neq 0$. By Lemma 2.41 there are prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ of R such that $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq (a)$ and such that r is minimal. Let \mathfrak{p} be a maximal ideal such that $\mathfrak{p} \supseteq \mathfrak{a}$. Then $\mathfrak{p} \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r$ and so $\mathfrak{p} \supseteq \mathfrak{p}_i$ for some i , because maximal ideals are prime. Say $\mathfrak{p} \supseteq \mathfrak{p}_1$. Since nonzero prime ideals are maximal, we have $\mathfrak{p} = \mathfrak{p}_1$. The number r is minimal, so there exists a $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r$ with $b \notin (a)$. Then

$$b\mathfrak{a} \subseteq b\mathfrak{p} \subseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq (a)$$

and so $\frac{b}{a}\mathfrak{a} \subseteq R$, whereas $\frac{b}{a} \notin R$. So take $c = \frac{b}{a}$. □

2.43 Theorem. *An integral domain R is a Dedekind domain if and only if*

- a) R is Noetherian,
- b) nonzero prime ideals of R are maximal ideals,
- c) R is integrally closed.

PROOF. We have already seen that a Dedekind domain satisfies a), b) and c): Propositions 2.8, 2.6 and 2.9. Now let R be an integral domain satisfying a), b) and c), and let K be its field of fractions. Let Φ be the collection of ideals \mathfrak{b} of R which contain an ideal \mathfrak{a} , whereas $\mathfrak{b} \nmid \mathfrak{a}$. We will prove that Φ is empty. Suppose $\Phi \neq \emptyset$. Since R is Noetherian, Φ has a maximal element \mathfrak{b} and let \mathfrak{a} be an ideal of R such that $\mathfrak{a} \subseteq \mathfrak{b}$ and $\mathfrak{b} \nmid \mathfrak{a}$. By Lemma 2.42 there are nonzero $a, b \in R$ such that $\frac{b}{a} \in K \setminus R$ and $\frac{b}{a}\mathfrak{b} \subseteq R$. Put $\mathfrak{b}' = \frac{1}{a}(a, b)\mathfrak{b}$. Then $\mathfrak{b}' = \mathfrak{b} + \frac{b}{a}\mathfrak{b} \subseteq R$, so the fractional ideal \mathfrak{b}' is actually an ideal of R . We have $\mathfrak{b}' \supset \mathfrak{b}$, since otherwise $\mathfrak{b}' = \mathfrak{b}' + \frac{b}{a}\mathfrak{b}'$, that is $\frac{b}{a}\mathfrak{b}' \subseteq \mathfrak{b}'$ and because R is Noetherian this would imply by Lemma 2.40 that $\frac{b}{a} \in R$. So we have $\mathfrak{b}' \notin \Phi$ and $\mathfrak{a} \subseteq \mathfrak{b}'$. Hence, there exists an ideal \mathfrak{c}' of R such that $\mathfrak{a} = \mathfrak{b}'\mathfrak{c}'$. Take $\mathfrak{c} = \frac{1}{a}(a, b)\mathfrak{c}'$. Then $\mathfrak{b}\mathfrak{c} = \frac{1}{a}(a, b)\mathfrak{b}\mathfrak{c}' = \mathfrak{b}'\mathfrak{c}' = \mathfrak{a}$ and this contradicts $\mathfrak{b} \in \Phi$ if \mathfrak{c} is an ideal of R , that is if $\mathfrak{c} \subseteq R$. For all $c \in \mathfrak{c}$ we have $c\mathfrak{b} \subseteq \mathfrak{a} \subseteq \mathfrak{b}$ and so again by Lemma 2.40 indeed $c \in R$. □

The integral closure of a Dedekind domain in a finite separable extension of its field of fractions is again a Dedekind domain. For a proof we will use this characterization of Dedekind domains. The following well-known lemma will be used.

2.44 Lemma. *Let R be a Noetherian ring, A a free R -module of finite rank and B an R -submodule of A . Then B is a finitely generated R -module.*

PROOF. Let n denote the rank of A . For $n = 0$ it is trivially true. We proceed by induction on n . Let $n \geq 1$. We may assume that $A = R^n$. Let $p: R^n \rightarrow R^{n-1}$ be the projection $(r_1, \dots, r_{n-1}, r_n) \mapsto (r_1, \dots, r_{n-1})$. For an R -submodule B of R^n we have $B/(\text{Ker}(p) \cap B) \cong p(B)$. The R -module $p(B)$ is finitely generated by induction hypothesis since it is a submodule of R^{n-1} . The R -module $\text{Ker}(p)$ is free of rank 1, so $B \cap \text{Ker}(p)$ is finitely generated because the ring is Noetherian. Clearly B is generated by generators of $B \cap \text{Ker}(p)$ together with lifts of generators of $p(B)$. \square

2.45 Theorem. *Let R be a Dedekind domain with field of fractions K and let $K' : K$ be a finite separable field extension. Then the integral closure R' of R in K' is a Dedekind domain.*

PROOF. We apply Theorem 2.43:

- a) By Proposition 1.36 R' is an R -submodule of a free R -module of finite rank and so is each ideal of R' . Since R is Noetherian, it follows from Lemma 2.44 that each ideal of R' is finitely generated as R -module and, therefore, also as R' -module.
- b) Let \mathfrak{q} be a nonzero prime ideal of R' . Then $\mathfrak{p} = \mathfrak{q} \cap R$ is a nonzero prime ideal of R . Since R is a Dedekind domain, \mathfrak{p} is a maximal ideal. The ring R'/\mathfrak{q} is both an integral domain and a finite-dimensional R/\mathfrak{p} -vector space. It follows that R'/\mathfrak{q} is a field. So \mathfrak{q} is maximal.
- c) The ring R' is integrally closed by Corollary 1.13. \square

In particular:

2.46 Theorem. *The ring of integers of a number field is a Dedekind domain.*

PROOF. Let K be a number field. Then \mathcal{O}_K is the integral closure of the principal ideal domain \mathbb{Z} in K . \square

In the next chapter we continue the study of number fields. Here we only give an example of a Dedekind domain with a nontrivial ideal class group. Another example is given in the exercises.

2.47 Example. The ring $\mathbb{Z}[\sqrt{-5}]$ is the ring of integers of the number field $\mathbb{Q}(\sqrt{-5})$. By Theorem 2.46 it is a Dedekind domain. It is not a principal ideal domain (Example 1.53). The ideal $\mathfrak{p}_2 = (2, 1 + \sqrt{-5})$ is not principal, see Example 2.12, so \mathfrak{p}_2 represents a nontrivial element of $\mathcal{C}(\mathbb{Z}[\sqrt{-5}])$. Since $\mathfrak{p}_2^2 = (2)$, we have $[\mathfrak{p}_2]^2 = [(2)] = 1$. So the element $[\mathfrak{p}_2]$ of the ideal class group is of order 2. For $\mathfrak{p}_3 = (3, 1 + \sqrt{-5})$ we have $\mathfrak{p}_2\mathfrak{p}_3 = (1 + \sqrt{-5})$ and so $[\mathfrak{p}_2] = [\mathfrak{p}_3]$. In the next chapter it will be shown that the ideal class group of $\mathbb{Z}[\sqrt{-5}]$ is a group of order 2 (Example 3.27).

EXERCISES

1. (i) Let \mathfrak{a} , \mathfrak{b} and \mathfrak{c} be ideals of a Dedekind domain R . Show that $\mathfrak{a}(\mathfrak{b} \cap \mathfrak{c}) = \mathfrak{a}\mathfrak{b} \cap \mathfrak{a}\mathfrak{c}$.
 (ii) Give an example of an integral domain R and ideals \mathfrak{a} , \mathfrak{b} and \mathfrak{c} of R such that $\mathfrak{a}(\mathfrak{b} \cap \mathfrak{c}) \neq \mathfrak{a}\mathfrak{b} \cap \mathfrak{a}\mathfrak{c}$.
2. A commutative ring is called Noetherian if its ideals are finitely generated. Let R be a commutative ring. Show the equivalence of:
 - (i) R is Noetherian.
 - (ii) Each nonempty collection Φ of ideals of R ordered by inclusion contains a maximal element.
 - (iii) Each ascending chain $\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \cdots \subseteq \mathfrak{a}_n \subseteq \cdots$ of ideals of R stabilizes, i.e. there is an $N \in \mathbb{N}$ such that $\mathfrak{a}_n = \mathfrak{a}_N$ for all $n \geq N$.
3. Let \mathfrak{a} be a nonzero ideal of the ring of integers of a quadratic number field. Show that there exist $a \in \mathbb{N}^*$ and $\alpha \in \mathfrak{a}$ such that $\mathfrak{a} = \mathbb{Z}a + \mathbb{Z}\alpha$.
4. Let \mathfrak{a} be a nonzero ideal of the ring of integers of a quadratic number field. Show that $\mathfrak{a}\mathfrak{a}' = (n)$ for some $n \in \mathbb{N}^*$. (Use exercise 3; \mathfrak{a}' is the conjugate ideal of \mathfrak{a} , that is $\mathfrak{a}' = \sigma(\mathfrak{a})$, where σ is the nontrivial automorphism of the number field.)
5. The ring of integers of a quadratic number field is a Dedekind domain. Show this by applying the result in exercise 4.
6. Let $m \in \mathbb{Z}$ be squarefree $\neq 1$ and congruent to 1 modulo 4. Show that $\mathbb{Z}[\sqrt{m}]$ is not a Dedekind domain.
7. Let $m \in \mathbb{Z}$ be squarefree, negative and congruent to 2 modulo 4. Let $\mathfrak{p} = (2, \sqrt{m})$.
 - (i) Show that \mathfrak{p} is a prime ideal of $\mathbb{Z}[\sqrt{m}]$.
 - (ii) Prove that $[\mathfrak{p}] \in \mathcal{C}(\mathbb{Z}[\sqrt{m}])$ is of order 2.
8. The field $K = \mathbb{R}(X)$ is the field of fractions of the polynomial ring $R = \mathbb{R}[X]$. Let $L = K(y)$ such that $y^2 = 1 - X^2$.
 - (i) Show that $[L : K] = 2$ and that $R[y]$ is the integral closure of R in L .
 - (ii) Show that the ideal $(X, 1 - y)$ of $R[y]$ represents an ideal class of order 2 in the ideal class group of the Dedekind domain $R[y]$. (In exercise 6 of chapter 10 it is asked to compute the ideal class group.)

3 Rings of Integers of Number Fields

In the previous chapter it was shown that rings of integers of number fields are Dedekind domains (Theorem 2.46). In section 3.3 it will be shown that their ideal class groups are finite. The argument used for this result enables us to compute ideal class groups in simple cases. In chapter 5 a more powerful method of computation is described and moreover in chapter 4 algorithms are given for the quadratic case.

In chapter 1 we noted (on page 25) that a number ring which is a principal ideal domain, necessarily is the ring of integers. In fact, the ring of integers of a number field is the unique number ring of that field which is a Dedekind domain:

3.1 Proposition. *Let K be a number field and let a number ring R of K be a Dedekind domain. Then $R = \mathcal{O}_K$.*

PROOF. Since R is finitely generated as an abelian group, we have by Proposition 1.12 that $R \subseteq \mathcal{O}_K$. The field K is the field of fractions of R . Since R is a Dedekind domain, it is integrally closed and so its integral closure in K is R itself. Because $\mathbb{Z} \subseteq R$, their integral closures in K satisfy $\mathcal{O}_K \subseteq R$. \square

The group of fractional ideals of a Dedekind domain is a free abelian group with the set of nonzero prime ideals as basis. In section 3.1 it is shown that prime ideals divide (the ideals generated by) prime numbers. A method is given for the computation of the factorization of ideals generated by prime numbers, which works up to a finite number of prime numbers. The last section is about ramifying prime numbers: prime numbers divisible by a prime ideal with multiplicity greater than 1.

3.1 Prime ideals

Let K be a number field. Since its ring of integers \mathcal{O}_K is a Dedekind domain, we have in this ring unique factorization of nonzero ideals as products of maximal ideals. What are the maximal ideals? Let \mathfrak{p} be a maximal ideal of \mathcal{O}_K . Then $\mathfrak{p} \cap \mathbb{Z}$ is a nonzero prime ideal of \mathbb{Z} , say $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, for a prime number p . The ideal $p\mathcal{O}_K$ is contained in \mathfrak{p} and, since \mathcal{O}_K is a Dedekind domain, we have $\mathfrak{p} \mid p\mathcal{O}_K$. Hence \mathfrak{p} is a factor in the factorization of the ideal $p\mathcal{O}_K$.

3.2 Definition. Let \mathfrak{p} be a maximal ideal of the ring of integers of a number field K . The prime number p that generates $\mathfrak{p} \cap \mathbb{Z}$ is said to be *under* \mathfrak{p} . The prime ideal \mathfrak{p} is said to be *above* p .

3.3 Definition. Let K be a number field, $\mathfrak{p} \in \text{Max}(\mathcal{O}_K)$ and p the prime number under \mathfrak{p} . Then $v_{\mathfrak{p}}(p) = v_{\mathfrak{p}}(p\mathcal{O}_K) \in \mathbb{N}^*$ is called the *ramification index* of \mathfrak{p} . Notation: $e(\mathfrak{p}) = v_{\mathfrak{p}}(p)$. The degree of the field extension $\mathcal{O}_K/\mathfrak{p} : \mathbb{F}_p$ is called the *residue class degree* of \mathfrak{p} . Notation: $f(\mathfrak{p}) = [\mathcal{O}_K/\mathfrak{p} : \mathbb{F}_p]$.

So we have

$$p\mathcal{O}_K = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(p)} = \prod_{\mathfrak{p}|p\mathcal{O}_K} \mathfrak{p}^{e(\mathfrak{p})}.$$

Often we will write the factorization as $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, where the \mathfrak{p}_i are the r prime ideals above p and e_i is the ramification index of \mathfrak{p}_i . Accordingly, the residue class degree of \mathfrak{p}_i is then denoted by f_i .

For a given number field the ramification indices and residue class degrees of the prime ideals above a prime number satisfy a relation:

3.4 Theorem. *Let K be a number field of degree n and let*

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$$

be the factorization of $p\mathcal{O}_K$ in \mathcal{O}_K . Then

$$e_1 f_1 + \cdots + e_r f_r = n,$$

where f_i is the residue class degree of \mathfrak{p}_i .

PROOF. Since \mathcal{O}_K is a free abelian group of rank n , the ring $\mathcal{O}_K/p\mathcal{O}_K$ is an \mathbb{F}_p -vector space of dimension n . For each ideal $\mathfrak{a} | p\mathcal{O}_K$ the ring $\mathcal{O}_K/\mathfrak{a}$ is a homomorphic image of $\mathcal{O}_K/p\mathcal{O}_K$ and, therefore, an \mathbb{F}_p -vector space as well. Repeated application of Proposition 2.17 yields that $\mathcal{O}_K/p\mathcal{O}_K$ is an \mathbb{F}_p -vector space of dimension $e_1 f_1 + \cdots + e_r f_r$. \square

3.5 Definition. Let K be a number field of degree n and p a prime number. For the factorization of $p\mathcal{O}_K$ there are three special cases:

p totally ramifies in K : there is only one prime ideal \mathfrak{p} above p and its ramification index is n : the factorization is $p\mathcal{O}_K = \mathfrak{p}^n$.

p remains prime in K : the ideal $p\mathcal{O}_K$ is a prime ideal; then the ideal $p\mathcal{O}_K$ is the only prime ideal above p and its residue class degree is n .

p splits completely in K : there are n prime ideals above p ; then each of them having ramification index 1 and residue class degree 1.

The three cases described in this definition are in a sense the three extreme cases. For a quadratic number field they are obviously the only possible cases, see also Theorem 3.7. In section 3.4 we will see that it are precisely the prime divisors of the discriminant of the number field that ramify. So only finitely many primes ramify. In chapter 5 it is shown that at least one prime number ramifies (Theorem 5.25). Total ramification of a prime, however, does not need to occur. On the other hand infinitely many primes split completely (exercise 16 of chapter 7). It depends on the number field whether there are primes that remain prime. If there is such a prime number, there are infinitely many of them.

In many cases it is not hard to factorize (the ideal generated by) a prime number in the ring of integers of a number field. The main tool for computations is given by the following theorem.

3.6 Theorem (Kummer-Dedekind). *Let K be a number field and $\vartheta \in \mathcal{O}_K$ a primitive element of $K : \mathbb{Q}$. Let $f \in \mathbb{Z}[X]$ be the minimal polynomial of ϑ over \mathbb{Q} . Assume the prime number p satisfies $p \nmid (\mathcal{O}_K : \mathbb{Z}[\vartheta])$. Let*

$$\bar{f} = \bar{g}_1^{e_1} \cdots \bar{g}_r^{e_r}$$

be the factorization of the polynomial $\bar{f} \in \mathbb{F}_p[X]$ as a product of irreducible polynomials, where the $g_i \in \mathbb{Z}[X]$ are taken to be monic. Then

$$p\mathcal{O}_K = (p, g_1(\vartheta))^{e_1} \cdots (p, g_r(\vartheta))^{e_r}$$

is the factorization of $p\mathcal{O}_K$ as a product of prime ideals.

PROOF. The ring homomorphism $\mathbb{Z}[X] \rightarrow \mathbb{F}_p[X]$ induces a ring isomorphism $\mathbb{Z}[X]/(p, g_i) \xrightarrow{\sim} \mathbb{F}_p[X]/(\bar{g}_i)$ and the ring homomorphism $\mathbb{Z}[X] \rightarrow \mathbb{Z}[\vartheta]$ induces an isomorphism $\mathbb{Z}[X]/(p, g_i) \xrightarrow{\sim} \mathbb{Z}[\vartheta]/(p, g_i(\vartheta))$. Since $\mathbb{F}_p[X]/(\bar{g}_i)$ is a field, the ideal $(p, g_i(\vartheta))$ of $\mathbb{Z}[\vartheta]$ is maximal. The inclusion $\mathbb{Z}[\vartheta] \rightarrow \mathcal{O}_K$ induces a ring homomorphism

$$\psi: \mathbb{Z}[\vartheta]/(p, g_i(\vartheta)) \rightarrow \mathcal{O}_K/(p, g_i(\vartheta)).$$

We will show that that the condition on the prime number p implies that it is an isomorphism.

Surjectivity: Let $\alpha \in \mathcal{O}_K$ and put $k = (\mathcal{O}_K : \mathbb{Z}[\vartheta])$. Since $p \nmid k$ there are $x, y \in \mathbb{Z}$ such that $xk + yp = 1$. Then $\alpha = xk\alpha + yp\alpha \in \mathbb{Z}[\vartheta] + p\mathcal{O}_K$ and so $\psi(\overline{xk\alpha}) = \overline{xk\alpha} = \bar{\alpha}$.

Injectivity: $\mathbb{Z}[\vartheta]/(p, g_i(\vartheta))$ is a field, so it suffices to show that $\psi(1) \neq 0$. Suppose $\psi(1) = 0$. Then $1 \in p\mathcal{O}_K + g_i(\vartheta)\mathcal{O}_K$ and so $k \in pk\mathcal{O}_K + g_i(\vartheta)k\mathcal{O}_K \subseteq p\mathbb{Z}[\vartheta] + g_i(\vartheta)\mathbb{Z}[\vartheta]$, which means that $\bar{k} = 0$ in the field $\mathbb{Z}[\vartheta]/(p, g_i(\vartheta))$. This field is of characteristic p . Contradiction with $p \nmid k$.

3 Rings of Integers of Number Fields

So the ideals $(p, g_i(\vartheta))$ of \mathcal{O}_K are maximal ideals of residue class degree $\deg(g_i)$. Next we show that they are different. Let $i \neq j$. Then \bar{g}_i and \bar{g}_j are different irreducible polynomials in $\mathbb{F}_p[X]$. So there are $u, v \in \mathbb{Z}[X]$ such that $\bar{u} \cdot \bar{g}_i + \bar{v} \cdot \bar{g}_j = 1$, that is $ug_i + vg_j \in 1 + p\mathbb{Z}[X]$. It follows that $u(\vartheta)g_i(\vartheta) + v(\vartheta)g_j(\vartheta) \in 1 + p\mathbb{Z}[\vartheta]$. Therefore, $1 \in (p, g_i(\vartheta), g_j(\vartheta)) = (p, g_i(\vartheta)) + (p, g_j(\vartheta))$. So the maximal ideals are comaximal and in particular they are different. Finally we have

$$(p, g_1(\vartheta))^{e_1} \cdots (p, g_r(\vartheta))^{e_r} \subseteq (p, g_1(\vartheta)^{e_1} \cdots g_r(\vartheta)^{e_r}) = (p, f(\vartheta)) = (p)$$

and since the residue class degree of $(p, g_i(\vartheta))$ equals $\deg(g_i)$, it follows from Theorem 3.4 that we have equality here. \square

A straightforward application of this theorem yields the splitting of primes in a quadratic number field. Let m be a squarefree integer $\neq 1$. We will compute the factorization of prime numbers in the quadratic number field $K = \mathbb{Q}(\sqrt{m})$. The ring of integers of K is $\mathbb{Z}[\omega_m]$. Since the index of $\mathbb{Z}[\sqrt{m}]$ in $\mathbb{Z}[\omega_m]$ equals 1 or 2, we can apply Theorem 3.6 for the factorization of prime numbers using the primitive element \sqrt{m} if the prime number is odd or if the index equals 1.

Let p be a prime number. The polynomial $X^2 - m$ is the minimal polynomial of \sqrt{m} over \mathbb{Q} . The polynomial $X^2 - \bar{m} \in \mathbb{F}_p[X]$ is reducible if and only if \bar{m} is a square in \mathbb{F}_p . We have the following cases for the factorization of (p) in $\mathbb{Z}[\omega_m]$ for p odd or $m \equiv 2, 3 \pmod{4}$:

1. $p \nmid m$ and $\bar{m} \in \mathbb{F}_p^*$ is not a square. Then (p) is a maximal ideal. In this case p remains prime.
2. $p \nmid m$ and $\bar{m} \in \mathbb{F}_p^*$ is a square, say $\bar{m} = \bar{n}^2$ with $n \in \mathbb{Z}$. Then $(p) = \mathfrak{p}\mathfrak{p}'$, where $\mathfrak{p} = (p, n - \sqrt{m})$ and $\mathfrak{p}' = (p, n + \sqrt{m})$. In this case p splits completely, unless $p = 2$ and $m \equiv 2 \pmod{4}$, in which case p ramifies.
3. $p \mid m$. Then $(p) = \mathfrak{p}^2$, where $\mathfrak{p} = (p, \sqrt{m})$. In this case p ramifies.

For the factorization of (2) in $\mathbb{Q}(\sqrt{m})$ with $m \equiv 1 \pmod{4}$ we can use the minimal polynomial of $\frac{1+\sqrt{m}}{2}$. This is the polynomial $f(X) = X^2 - X + \frac{1-m}{4}$. There are two cases:

1. $m \equiv 1 \pmod{8}$. Then $\bar{f}(X) = X^2 - X \in \mathbb{F}_2[X]$ and so $(2) = \mathfrak{p}\mathfrak{p}'$, where $\mathfrak{p} = (2, \frac{1+\sqrt{m}}{2})$ and $\mathfrak{p}' = (2, \frac{1-\sqrt{m}}{2})$. In this case 2 splits completely.
2. $m \equiv 5 \pmod{8}$. Then $\bar{f}(X) = X^2 + X + 1 \in \mathbb{F}_2[X]$, an irreducible polynomial. In this case 2 remains prime.

Now we have a complete picture of the splitting behavior of primes in a quadratic number field:

3.7 Theorem. *Let $m \in \mathbb{Z}$ be squarefree $\neq 1$ and let p be an odd prime. The factorization of the ideal (p) in the ring of integers of the quadratic number field $\mathbb{Q}(\sqrt{m})$ is as follows.*

- a) If $p \nmid m$ and \bar{m} is not a square in \mathbb{F}_p , then p remains prime.
- b) If $p \nmid m$ and $m \equiv n^2 \pmod{p}$, then p splits completely:
 $(p) = (p, n - \sqrt{m})(p, n + \sqrt{m})$.
- c) If $p \mid m$, then p ramifies: $(p) = (p, \sqrt{m})^2$.

For the prime 2 we have:

- d) If $m \equiv 2 \pmod{4}$, then 2 ramifies: $(2) = (2, \sqrt{m})^2$.
- e) If $m \equiv 3 \pmod{4}$, then 2 ramifies: $(2) = (2, 1 + \sqrt{m})^2$.
- f) If $m \equiv 1 \pmod{8}$, then 2 splits completely: $(2) = (2, \frac{1-\sqrt{m}}{2})(2, \frac{1+\sqrt{m}}{2})$.
- g) If $m \equiv 5 \pmod{8}$, then 2 remains prime. □

Note that this computation shows that a prime p ramifies in a quadratic number field if and only if it is a divisor of the discriminant of that field. In section 3.4 we will see that this holds for any number field (Theorem 3.30). The splitting of an odd prime number p in a quadratic number field $\mathbb{Q}(\sqrt{m})$ is determined by the residue class of m modulo p . The following terminology is often used.

3.8 Definition. Let p be a prime number and $a \in \mathbb{Z}$ such that $p \nmid a$. If \bar{a} is a square in \mathbb{F}_p^* , the integer a is called a *quadratic residue* modulo p . Otherwise it is called a *quadratic nonresidue* modulo p .

By squaring 1 up to $\frac{p-1}{2}$ and taking the residues of these outcomes by division by p one obtains all quadratic residues modulo p . Figure 3.1 is a graphic representation of the quadratic residues modulo the first twelve odd prime numbers. Because -1 is a quadratic residue modulo a prime $\equiv 1 \pmod{4}$, for these primes the distribution of the quadratic residues is symmetric with respect to the midpoint of the interval. For primes $\equiv 3 \pmod{4}$ quadratic residues map to quadratic nonresidues under reflection in the midpoint.

Problem. For the first twelve odd primes p the following holds

- for primes $p \equiv 1 \pmod{4}$ there are more quadratic residues in the first (and fourth) quarter of the interval $[0, p]$ than in the second (and third) quarter;
- for primes $p \equiv 3 \pmod{4}$ there are more quadratic residues in the first half of the interval $[0, p]$ than in the second half.

Is this generally true for all odd primes?

This is solved in chapter 9 using complex analytic methods. It is generally true and surprisingly that the difference in these numbers depends on the orders of the ideal class groups of $\mathbb{Q}(\sqrt{-p})$.

3 Rings of Integers of Number Fields

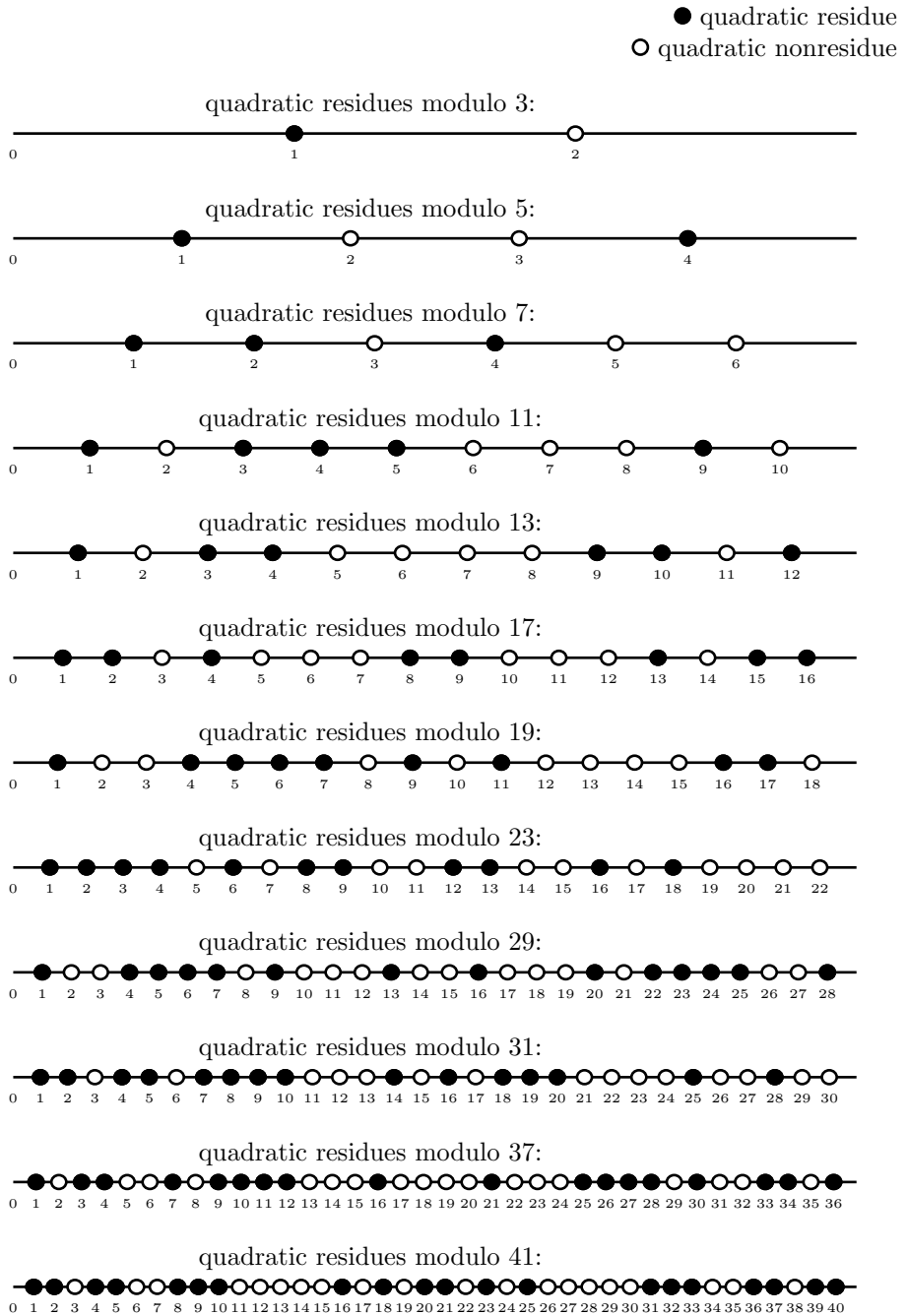


Figure 3.1: Quadratic residues modulo the first twelve odd primes

3.9 Example. $\mathbb{Z}[\sqrt[3]{5}]$ is the ring of integers of $\mathbb{Q}(\sqrt[3]{5})$, see exercise 8 of chapter 1. We factorize 2, 3, 5 and 7 in $\mathbb{Q}(\sqrt[3]{5})$ by factorizing $X^3 - 5$ over $\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_5$ and \mathbb{F}_7 respectively, where $\alpha = \sqrt[3]{5}$:

$$\begin{aligned}(2) &= (2, 1 + \alpha)(2, 1 + \alpha + \alpha^2), \\(3) &= (3, 1 + \alpha)^3, \\(5) &= (5, \alpha)^3, \\(7) &\text{ is a prime ideal.}\end{aligned}$$

So: 7 remains prime, 3 and 5 totally ramify and 2 splits as a product of two prime ideals having different residue class degrees.

3.10 Example. Let $\alpha \in \mathbb{R}$ satisfy $\alpha^3 = \alpha + 1$. The ring of integers of $\mathbb{Q}(\alpha)$ is $\mathbb{Z}[\alpha]$ (exercise 6 of chapter 1). Over \mathbb{F}_{23} we have

$$X^3 - X - 1 = (X - \overline{10})^2(X - \overline{3}).$$

So the factorization of 23 in $\mathbb{Q}(\alpha)$ is

$$(23) = (23, \alpha - 10)^2(23, \alpha - 3).$$

Note that the two prime ideals above 23 have different ramification indices.

These examples show that residue class degrees and ramification indices of prime ideals above the same prime number may differ. For Galois extensions this does not happen. It is a consequence of:

3.11 Theorem. *Let $K : \mathbb{Q}$ be a Galois extension and p a prime number. Then $\text{Gal}(K : \mathbb{Q})$ operates transitively on the set of prime ideals of K above p .*

PROOF. Put $G = \text{Gal}(K : \mathbb{Q})$ and $X = \{\mathfrak{p} \in \text{Max}(\mathcal{O}_K) \mid \mathfrak{p} \cap \mathbb{Q} = p\mathbb{Z}\}$. Suppose the action of G on X is not transitive: there are $\mathfrak{p}_1, \mathfrak{p}_2 \in X$ such that $\sigma(\mathfrak{p}_1) \neq \mathfrak{p}_2$ for all $\sigma \in G$. Then by the Chinese Remainder Theorem there is an $\alpha \in \mathcal{O}_K$ such that

$$\alpha \equiv \begin{cases} 0 & \text{modulo } \mathfrak{p}_2, \\ 1 & \text{modulo } \sigma(\mathfrak{p}_1) \text{ for all } \sigma \in G. \end{cases}$$

So $\sigma^{-1}(\alpha) \equiv 1 \pmod{\mathfrak{p}_1}$ for all $\sigma \in G$. It follows that $N_{\mathbb{Q}}^K(\alpha) = \prod_{\sigma \in G} \sigma(\alpha) \notin \mathfrak{p}_1 \cap \mathbb{Q} = p\mathbb{Z}$. But since $\alpha \in \mathfrak{p}_2$, we have $N_{\mathbb{Q}}^K(\alpha) = \alpha \cdot \prod_{\sigma \neq 1} \sigma(\alpha) \in \mathfrak{p}_2 \cap \mathbb{Q} = p\mathbb{Z}$. Contradiction. \square

3.12 Corollary. *Let $K : \mathbb{Q}$ be a Galois extension, p a prime number and $\mathfrak{p}_1, \mathfrak{p}_2 \in \text{Max}(\mathcal{O}_K)$ above p . Then $e(\mathfrak{p}_1) = e(\mathfrak{p}_2)$ and $f(\mathfrak{p}_1) = f(\mathfrak{p}_2)$.*

PROOF. There is a $\sigma \in \text{Gal}(K : \mathbb{Q})$ such that $\sigma(\mathfrak{p}_1) = \mathfrak{p}_2$. This automorphism σ induces an automorphism of \mathcal{O}_K , which in turn induces an isomorphism $\mathcal{O}_K/\mathfrak{p}_1 \xrightarrow{\sim} \mathcal{O}_K/\mathfrak{p}_2$. Hence $f(\mathfrak{p}_1) = f(\mathfrak{p}_2)$. For the ramification indices we have

$$e(\mathfrak{p}_1) = v_{\mathfrak{p}_1}(p\mathcal{O}_K) = v_{\sigma(\mathfrak{p}_1)}(\sigma(p\mathcal{O}_K)) = v_{\mathfrak{p}_2}(p\mathcal{O}_K) = e(\mathfrak{p}_2). \quad \square$$

3.13 Terminology and notation. Let $K : \mathbb{Q}$ be a Galois extension and p a prime number. The number $e(\mathfrak{p})$, where \mathfrak{p} is any prime ideal of \mathcal{O}_K above p , is called the *ramification index of p in K* and is denoted by $e_p^{(K)}$. Similarly we have the residue class degree $f_p^{(K)}$ of p in K .

For $K : \mathbb{Q}$ a Galois extension and p a prime number the formula in Theorem 3.4 simplifies to $n = ref$, where e is the ramification index of p in K , f the residue class degree of p in K and r the number of prime ideals of \mathcal{O}_K above p .

Let's compute the splitting behavior of a prime p in a cyclotomic field $\mathbb{Q}(\zeta_m)$. The minimum polynomial of ζ_m over \mathbb{Q} is the m -th cyclotomic polynomial

$$\Phi_m(X) = \prod_{\substack{\zeta \in \mu(\mathbb{C}) \\ o(\zeta)=m}} (X - \zeta) = \prod_{\substack{0 \leq k < m \\ \gcd(k,m)=1}} (X - \zeta_m^k).$$

Since $\mathbb{Z}[\zeta_m]$ is the ring of integers, the splitting of p can be computed by factorizing the m -th cyclotomic polynomial over \mathbb{F}_p . First we consider the case $p \nmid m$.

3.14 Proposition. *Let $m \in \mathbb{N}^*$ and p a prime number with $p \nmid m$. Then p does not ramify in $\mathbb{Q}(\zeta_m)$ and the residue class degree of p in $\mathbb{Q}(\zeta_m)$ is equal to the order of \bar{p} in the group $(\mathbb{Z}/m)^*$.*

PROOF. Let f be the order of $\bar{p} \in (\mathbb{Z}/m)^*$. For $\mathfrak{p} \in \text{Max}(\mathbb{Z}[\zeta_m])$ above p , the extension $\mathbb{Z}[\zeta_m]/\mathfrak{p} : \mathbb{F}_p$ is the m -th cyclotomic extension of \mathbb{F}_p . It is a Galois extension and its Galois group is generated by the Frobenius automorphism $x \mapsto x^p$. This automorphism is of order f . So the polynomial $\bar{\Phi}_m \in \mathbb{F}_p[X]$ is a product of $\varphi(m)/f$ irreducible polynomials, each of degree f . It follows that $p\mathbb{Z}[\zeta_m]$ is a product of $\varphi(m)/f$ prime ideals of residue class degree f . \square

For the general case we will use the following lemma.

3.15 Lemma. *Let $m, n \in \mathbb{N}^*$ and p a prime number. Then*

- (i) $\Phi_{mn}(X) \mid \Phi_n(X^m)$,
- (ii) $\Phi_n(X^p) = \begin{cases} \Phi_{pn}(X) & \text{if } p \mid n, \\ \Phi_n(X)\Phi_{pn}(X) & \text{if } p \nmid n. \end{cases}$

PROOF.

- (i) $\Phi_{mn}(X)$ is the minimal polynomial of ζ_{mn} and this root of unity is a zero of $\Phi_n(X^m)$.
- (ii) In both cases the right hand side divides the left hand side. For $p \mid n$ this follows from (i). For $p \nmid n$ use that Φ_n and Φ_{pn} are different irreducible monic polynomials which both divide $\Phi_n(X^p)$. Equality follows by comparing degrees. \square

3.16 Theorem. Let $m \in \mathbb{N}^*$, p a prime number, $r = v_p(m)$, $m = p^r m_0$ and $K = \mathbb{Q}(\zeta_m)$. Then

$$e_p^{(K)} = \varphi(p^r) \quad \text{and} \quad f_p^{(K)} = \text{the order of } \bar{p} \in (\mathbb{Z}/m_0)^*.$$

PROOF. The case $r = 0$ is dealt with in Proposition 3.14, so we assume that $r > 0$. By Lemma 3.15

$$\Phi_{p^r m_0}(X) = \Phi_{p^{r-1} m_0}(X^p) = \cdots = \Phi_{p m_0}(X^{p^{r-1}}) = \frac{\Phi_{m_0}(X^{p^r})}{\Phi_{m_0}(X^{p^{r-1}})}.$$

Hence in $\mathbb{F}_p[X]$:

$$\overline{\Phi_m}(X) \cdot \overline{\Phi_{m_0}}(X^{p^{r-1}}) = \overline{\Phi_{m_0}}(X^{p^r})$$

and so

$$\overline{\Phi_m}(X) = \frac{\overline{\Phi_{m_0}}(X^{p^r})}{\overline{\Phi_{m_0}}(X^{p^{r-1}})} = \frac{\overline{\Phi_{m_0}}(X)^{p^r}}{\overline{\Phi_{m_0}}(X)^{p^{r-1}}} = \overline{\Phi_{m_0}}(X)^{p^{r-1}(p-1)}.$$

The theorem follows from the splitting behavior of $\overline{\Phi_m}$ for the case $p \nmid m$. \square

3.2 The norm of an ideal

The rings of integers of number fields are lattices, and so are the nonzero ideals, more precisely:

3.17 Lemma. Let K be a number field and \mathfrak{a} a nonzero ideal of \mathcal{O}_K . Then \mathfrak{a} is a lattice in K and the residue class ring $\mathcal{O}_K/\mathfrak{a}$ is finite.

PROOF. Let $a \in \mathfrak{a}$ with $a \neq 0$. Then $a\mathcal{O}_K$ is a lattice in K : if $\alpha_1, \dots, \alpha_n$ is an integral basis of K , then $a\alpha_1, \dots, a\alpha_n$ is a \mathbb{Z} -basis of $a\mathcal{O}_K$. The ideal \mathfrak{a} is sandwiched between $a\mathcal{O}_K$ and \mathcal{O}_K : $a\mathcal{O}_K \subseteq \mathfrak{a} \subseteq \mathcal{O}_K$. We can take a to be an element of $\mathfrak{a} \cap \mathbb{N}^*$. Then, if $n = [K : \mathbb{Q}]$, the index of $a\mathcal{O}_K$ in \mathcal{O}_K is equal to a^n . The index of \mathfrak{a} in \mathcal{O}_K is a divisor of this number. \square

Since nonzero ideals are of finite index in the ring of integers, we can make the following definition.

3.18 Definition. Let K be a number field and let \mathfrak{a} be a nonzero ideal of \mathcal{O}_K . The number of elements of the residue class ring $\mathcal{O}_K/\mathfrak{a}$ is called the *norm* of the ideal \mathfrak{a} . Notation: $N(\mathfrak{a}) = \#(\mathcal{O}_K/\mathfrak{a})$.

The norm is multiplicative in the following sense;

3.19 Proposition. Let K be a number field and \mathfrak{a} and \mathfrak{b} nonzero ideals of \mathcal{O}_K . Then $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$.

3 Rings of Integers of Number Fields

PROOF. This follows from Proposition 2.17 by induction on the number of prime ideal factors in the factorization of \mathfrak{a} . \square

Note that for a prime ideal \mathfrak{p} of \mathcal{O}_K above p we have $N(\mathfrak{p}) = \#(\mathcal{O}_K/\mathfrak{p}) = p^{f(\mathfrak{p})}$. Applying the above proposition to $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ yields

$$p^n = N(\mathfrak{p}_1)^{e_1} \cdots N(\mathfrak{p}_r)^{e_r} = p^{e_1 f_1} \cdots p^{e_r f_r} = p^{e_1 f_1 + \cdots + e_r f_r}.$$

Thus we have in this way another proof of Theorem 3.4, a proof that uses the finiteness of residue class rings of rings of integers of number fields.

The norm of an element is related to the norm of the ideal it generates:

3.20 Proposition. *Let K be a number field and α a nonzero element of \mathcal{O}_K . Then $N(\alpha\mathcal{O}_K) = |N_{\mathbb{Q}}^K(\alpha)|$.*

PROOF. Let $(\alpha_1, \dots, \alpha_n)$ be an integral basis of K and M the matrix of the \mathbb{Q} -linear transformation $x \mapsto \alpha x$ with respect to the basis $(\alpha_1, \dots, \alpha_n)$. Then by definition $N_{\mathbb{Q}}^K(\alpha) = \det(M)$. The matrix M is the transition matrix from the basis $(\alpha\alpha_1, \dots, \alpha\alpha_n)$ to the basis $(\alpha_1, \dots, \alpha_n)$. Then by Lemma 1.40

$$(\mathcal{O}_K : \alpha\mathcal{O}_K) = |\det(M)| = |N_{\mathbb{Q}}^K(\alpha)|. \quad \square$$

For Galois extensions $K : \mathbb{Q}$ we have:

3.21 Proposition. *Let $K : \mathbb{Q}$ be a Galois extension and \mathfrak{a} a nonzero ideal of \mathcal{O}_K . Then*

$$N(\mathfrak{a})\mathcal{O}_K = \prod_{\sigma \in \text{Gal}(L:K)} \sigma(\mathfrak{a}).$$

PROOF. It suffices to prove that $N(\mathfrak{p})\mathcal{O}_K = \prod_{\sigma} \sigma(\mathfrak{p})$ for prime ideals \mathfrak{p} . Let \mathfrak{p} be a prime ideal of \mathcal{O}_K above a prime number p . Put $e = e_p^{(K)}$ and $f = f_p^{(K)}$. Then by Corollary 3.12

$$\prod_{\sigma} \sigma(\mathfrak{p}) = \left(\prod_{\mathfrak{q}|p\mathcal{O}_K} \mathfrak{q} \right)^{ef} = \left(\prod_{\mathfrak{q}|p\mathcal{O}_K} \mathfrak{q}^e \right)^f = (p\mathcal{O}_K)^f = p^f \mathcal{O}_K = N(\mathfrak{p})\mathcal{O}_K,$$

where \mathfrak{q} varies over the prime ideals of \mathcal{O}_K above p . \square

In particular:

3.22 Corollary. *Let K be a quadratic number field, \mathfrak{a} a nonzero ideal of \mathcal{O}_K and \mathfrak{a}' its conjugate. Then $[\mathfrak{a}'] = [\mathfrak{a}]^{-1}$.*

PROOF. By Proposition 3.21 $\mathfrak{a}\mathfrak{a}' = N(\mathfrak{a})\mathcal{O}_K$ and so $[\mathfrak{a}] \cdot [\mathfrak{a}'] = 1$. \square

3.3 The ideal class group of a number field

In this section it is shown that the ideal class group of the ring of integers of a number field is finite.

The ring \mathcal{O}_K of integers of a number field K is determined by the field K . Because of this circumstance, objects related to \mathcal{O}_K are often attributed to K instead of \mathcal{O}_K and as a consequence notations are adapted accordingly.

3.23 Terminology and notations. The ideal class group of the ring of integers of a number field K is also called the ideal class group of K . Notation: $\mathcal{C}(K)$. Similarly, the groups of fractional ideals and of principal fractional ideals are denoted by $\mathbb{I}(K)$ and $\mathbb{P}(K)$ respectively. Moreover, the monoid of nonzero ideals of \mathcal{O}_K is denoted by $\mathbb{I}^+(K)$.

The finiteness of the ideal class group of a number field is based on the following proposition.

3.24 Proposition. *Let K be a number field. Then there is a $\lambda \in \mathbb{R}$ such that for every nonzero ideal \mathfrak{a} of \mathcal{O}_K there is a nonzero $\alpha \in \mathfrak{a}$ with $|\mathbb{N}_{\mathbb{Q}}^K(\alpha)| \leq \lambda \mathbb{N}(\mathfrak{a})$.*

PROOF. Let $(\alpha_1, \dots, \alpha_n)$ be an integral basis of K and $\sigma_1, \dots, \sigma_n$ the embeddings of K in \mathbb{C} and let $m \in \mathbb{N}^*$ be such that $m^n \leq \mathbb{N}(\mathfrak{a}) < (m+1)^n$. Consider the following subset of \mathcal{O}_K :

$$\left\{ \sum_{j=1}^n m_j \alpha_j \mid m_j \in \mathbb{N} \text{ and } m_j \leq m \right\}.$$

This set has $(m+1)^n$ elements. Since $\mathcal{O}_K/\mathfrak{a}$ has less elements, there must exist two of these elements which are congruent modulo \mathfrak{a} . Their difference is an element $\alpha = \sum_{j=1}^n m_j \alpha_j$ in \mathfrak{a} with $|m_j| \leq m$. We have

$$\begin{aligned} |\mathbb{N}_{\mathbb{Q}}^K(\alpha)| &= \prod_{i=1}^n |\sigma_i(\alpha)| \leq \prod_{i=1}^n \sum_{j=1}^n |m_j| \cdot |\sigma_i(\alpha_j)| \leq \prod_{i=1}^n m \sum_{j=1}^n |\sigma_i(\alpha_j)| \\ &= m^n \prod_{i=1}^n \sum_{j=1}^n |\sigma_i(\alpha_j)| \leq \mathbb{N}(\mathfrak{a}) \prod_{i=1}^n \sum_{j=1}^n |\sigma_i(\alpha_j)|. \end{aligned}$$

So we can take

$$\lambda = \prod_{i=1}^n \sum_{j=1}^n |\sigma_i(\alpha_j)| \quad \square$$

For a nonzero $\alpha \in \mathfrak{a}$ we have $\mathfrak{a} \supseteq \alpha \mathcal{O}_K$ and since \mathcal{O}_K is a Dedekind domain $\mathfrak{a} \mid \alpha \mathcal{O}_K$. By multiplicativity of the norm it follows that $|\mathbb{N}_{\mathbb{Q}}^K(\alpha)|$ is a multiple of $\mathbb{N}(\mathfrak{a})$. So the λ in the proposition can be taken to be in \mathbb{N}^* and, therefore, there is a least such λ . The ring \mathcal{O}_K is a principal ideal domain if and only if this least λ equals 1.

3.25 Corollary. *Let K and λ be as in the proposition. Then every ideal class of \mathcal{O}_K contains a nonzero ideal \mathfrak{b} satisfying $N(\mathfrak{b}) \leq \lambda$.*

PROOF. Let C be an ideal class of \mathcal{O}_K and $\mathfrak{a} \in C^{-1}$. By Proposition 3.24 there is a nonzero $\alpha \in \mathfrak{a}$ such that $|N_{\mathbb{Q}}^K(\alpha)| \leq \lambda N(\mathfrak{a})$. We have $\alpha \mathcal{O}_K = \mathfrak{a}\mathfrak{b}$ for an ideal $\mathfrak{b} \in C$. From $|N_{\mathbb{Q}}^K(\alpha)| = N(\mathfrak{a})N(\mathfrak{b})$ follows that $N(\mathfrak{b}) \leq \lambda$. \square

3.26 Theorem. *The ideal class group of a number field is finite.*

PROOF. Let K be a number field and λ be as in Proposition 3.24. By Corollary 3.25 the ideal classes of \mathcal{O}_K are represented by ideals \mathfrak{a} with $N(\mathfrak{a}) \leq \lambda$. Since there are only finitely many prime numbers $\leq \lambda$, the number of prime ideals \mathfrak{p} of \mathcal{O}_K with $N(\mathfrak{p}) \leq \lambda$ is finite as well. Ideals \mathfrak{a} with $N(\mathfrak{a}) \leq \lambda$ are products of these prime ideals. It follows that there are only finitely many of such ideals. \square

3.27 Example. For $d \in \mathbb{Z}$ squarefree with $d \equiv 2, 3 \pmod{4}$ the ring of integers of $\mathbb{Q}(\sqrt{d})$ is $\mathbb{Z}[\sqrt{d}]$. An integral basis is $(1, \sqrt{d})$. For this basis the number λ in the proof of Theorem 3.24 equals $(1 + |\sqrt{d}|)^2$. For $d = -5$ we have $\lambda = (1 + \sqrt{5})^2 < 11$. In Example 2.12 it is shown that $\mathbb{Z}[\sqrt{-5}]$ is not a principal ideal domain. The ideal $\mathfrak{p}_2 = (2, 1 + \sqrt{-5})$ represents an ideal class of order 2 (Example 2.47). Ideals of norm less than 11 are products of prime ideals of norm < 11 and these are above prime numbers < 11 . Since $(2) = \mathfrak{p}_2^2$, the ideal \mathfrak{p}_2 is the only prime ideal of norm 2. From $(3) = \mathfrak{p}_3\mathfrak{p}'_3$ follows that \mathfrak{p}_3 and \mathfrak{p}'_3 are the prime ideals of norm 3. The ideal $\mathfrak{p}_5 = (\sqrt{-5})$ is the unique prime ideal of norm 5: we have $(5) = \mathfrak{p}_5^2$. The element $3 + \sqrt{-5}$ has norm 14, so $(3 + \sqrt{-5}) = \mathfrak{p}_2\mathfrak{p}_7$ for some prime ideal \mathfrak{p}_7 of norm 7. In fact $(7) = \mathfrak{p}_7\mathfrak{p}'_7 = (7, 3 + \sqrt{-5})(7, 3 - \sqrt{-5})$. The ideals of $\mathbb{Z}[\sqrt{-5}]$ of norm ≤ 10 are: (1) , \mathfrak{p}_2 , \mathfrak{p}_3 , \mathfrak{p}'_3 , $\mathfrak{p}_2^2 = (2)$, $\mathfrak{p}_5 = (\sqrt{-5})$, $\mathfrak{p}_2\mathfrak{p}_3 = (1 + \sqrt{-5})$, $\mathfrak{p}_2\mathfrak{p}'_3 = (1 - \sqrt{-5})$, \mathfrak{p}_7 , \mathfrak{p}'_7 , $\mathfrak{p}_2^3 = 2\mathfrak{p}_2$, \mathfrak{p}_3^2 , $\mathfrak{p}_3\mathfrak{p}'_3 = (3)$ and $\mathfrak{p}_2\mathfrak{p}_5$. The ideal class group is generated by the classes represented by the prime ideals among these. From $\mathfrak{p}_3\mathfrak{p}'_3 = (3)$ it follows that $[\mathfrak{p}'_3] = [\mathfrak{p}_3]^{-1}$ and similarly for the other prime ideals. So the group is generated by $[\mathfrak{p}_2]$, $[\mathfrak{p}_3]$ and $[\mathfrak{p}_7]$ ($[\mathfrak{p}_5] = 1$). Since $\mathfrak{p}_2\mathfrak{p}_3$ and $\mathfrak{p}_2\mathfrak{p}_7$ are principal ideals the group is generated by $[\mathfrak{p}_2]$ alone and by Example 2.47 it is a group of order 2. The algorithm in chapter 4 will simplify the computation considerably. Apart from this, in chapter 5 we will see on general grounds that we could have taken $\lambda = 2$. Then \mathfrak{p}_2 is the only prime ideal to consider.

3.4 Ramification

3.28 Definition. Let K be a number field. A $\mathfrak{p} \in \text{Max}(\mathcal{O}_K)$ with ramification index $e(\mathfrak{p}) > 1$ is called *ramified*. We also say that in that case the prime p under \mathfrak{p} *ramifies* in K .

In this section it is shown that for a given number field it are just the prime divisors of its discriminant which ramify. We will use the following lemma.

3.29 Lemma. *Let K be a number field, p a prime number and $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$ such that $(\overline{\alpha_1}, \dots, \overline{\alpha_n})$ is an \mathbb{F}_p -basis of $\mathcal{O}_K/p\mathcal{O}_K$. Then $p \mid \text{disc}(K)$ if and only if $p \mid \text{disc}(\alpha_1, \dots, \alpha_n)$.*

PROOF. Clearly $(\alpha_1, \dots, \alpha_n)$ is a \mathbb{Q} -basis of K . Let $(\beta_1, \dots, \beta_n)$ be an integral basis of K . Then $\text{disc}(\alpha_1, \dots, \alpha_n) = \det(T)^2 \text{disc}(K)$, where T is the transition matrix from $(\beta_1, \dots, \beta_n)$ to $(\alpha_1, \dots, \alpha_n)$. Since both $(\overline{\alpha_1}, \dots, \overline{\alpha_n})$ and $(\overline{\beta_1}, \dots, \overline{\beta_n})$ are \mathbb{F}_p -bases of $\mathcal{O}_K/p\mathcal{O}_K$, the transition matrix \overline{T} is invertible. Hence $\det(\overline{T}) \neq 0$, that is $p \nmid \det(T)$. So $p \mid \text{disc}(\alpha_1, \dots, \alpha_n)$ if and only if $p \mid \text{disc}(K)$. \square

3.30 Theorem. *Let K be a number field and p a prime number. Then p ramifies in K if and only if $p \mid \text{disc}(K)$.*

PROOF. Suppose that p does not ramify in K , say $p\mathcal{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ with $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ the different maximal ideals of \mathcal{O}_K above p . Put $f_i = f(\mathfrak{p}_i)$ for $i = 1, \dots, r$. Choose for each i an \mathbb{F}_p -basis $(\overline{\beta_{i1}}, \dots, \overline{\beta_{if_i}})$ of $\mathcal{O}_K/p\mathcal{O}_K$, where $\beta_{ij} \in \mathcal{O}_K$ for all ij . The Chinese Remainder Theorem implies that there are $\alpha_{ij} \in \mathcal{O}_K$ such that

$$\alpha_{ij} \equiv \begin{cases} \beta_{ij} \pmod{\mathfrak{p}_i}, \\ 0 \pmod{\mathfrak{p}_k} \quad \text{for all } k \neq i. \end{cases}$$

Then

$$(\alpha_{11}, \dots, \alpha_{1f_1}, \alpha_{21}, \dots, \alpha_{2f_2}, \dots, \dots, \alpha_{r1}, \dots, \alpha_{rf_r})$$

is modulo $p\mathcal{O}_K$ an \mathbb{F}_p -basis of $\mathcal{O}_K/p\mathcal{O}_K$, and, therefore, also a \mathbb{Q} -basis of K . By Lemma 3.29 it suffices to prove that $p \nmid \text{disc}(\alpha_{11}, \dots, \alpha_{rf_r})$. For $i \neq k$ we have $\alpha_{ij}\alpha_{kl} \in p\mathcal{O}_K$, and so $\text{Tr}_{\mathbb{Q}}^K(\alpha_{ij}\alpha_{kl}) \in p\mathcal{O}_K$. The matrix $A = (\text{Tr}_{\mathbb{Q}}^K(\alpha_{ij}\alpha_{kl}))$ has the following shape:

$$A = \begin{pmatrix} \boxed{A_1} & & & & \\ & \boxed{A_2} & & & \\ & & \ddots & & \\ * & & & \ddots & \\ & & & & \boxed{A_r} \end{pmatrix},$$

where the A_i are the $f_i \times f_i$ -matrices $(\text{Tr}_{\mathbb{Q}}^K(\alpha_{ij}\alpha_{il}))$ and in the matrix outside these square matrices along the diagonal all entries are in $p\mathbb{Z}$. It suffices to prove that $p \nmid \det(A_i)$ for $i = 1, \dots, r$, because $\det(A) \equiv \det(A_1) \cdot \det(A_2) \cdots \det(A_r) \pmod{p}$. Since the $\alpha_{i1}, \dots, \alpha_{if_i}$ form modulo \mathfrak{p}_i a basis of $\mathcal{O}_K/\mathfrak{p}_i$, we have in \mathbb{F}_p :

$$\overline{\text{Tr}_{\mathbb{Q}}^K(\alpha_{ij}\alpha_{ik})} = \overline{\text{Tr}(M_{\alpha_{ij}\alpha_{ik}})} = \text{Tr}(M_{\overline{\alpha_{ij}\alpha_{ik}}}).$$

So $\overline{\det(A_i)}$ is the discriminant of the \mathbb{F}_p -basis of $\mathcal{O}_K/\mathfrak{p}_i$. By Corollary 1.30 it follows that $\overline{\det(A_i)} \neq 0$, that is $p \nmid \det(A_i)$.

For the converse suppose that p ramifies in K . Then there is a $\mathfrak{p} \in \text{Max}(\mathcal{O}_K)$ above p such that $p\mathcal{O}_K = \mathfrak{p}\mathfrak{a}$, where \mathfrak{a} is an ideal of \mathcal{O}_K with $\mathfrak{p} \mid \mathfrak{a}$. Choose an $\alpha \in \mathfrak{a} \setminus p\mathcal{O}_K$. Then $\alpha^2 \in p\mathcal{O}_K$. The ring $\mathcal{O}_K/p\mathcal{O}_K$ is an \mathbb{F}_p -vector space of dimension $n = [K : \mathbb{Q}]$. The image $\bar{\alpha}$ of α in $\mathcal{O}_K/p\mathcal{O}_K$ is not 0, so there are $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$ such that $(\bar{\alpha}_1, \dots, \bar{\alpha}_n)$ is a basis of the \mathbb{F}_p -vector space $\mathcal{O}_K/p\mathcal{O}_K$ and $\alpha_1 = \alpha$. The discriminant of $(\alpha_1, \dots, \alpha_n)$ is the determinant of the matrix $(\text{Tr}_{\mathbb{Q}}^K(\alpha_i\alpha_j))$. We show that the entries in the first row of this matrix are all multiples of p . The $1j$ -entry equals $\text{Tr}_{\mathbb{Q}}^K(\alpha\alpha_j)$. Modulo \mathfrak{p} this is $\text{Tr}(M_{\overline{\alpha\alpha_j}})$, the trace of the \mathbb{F}_p -linear transformation $x \mapsto \overline{\alpha\alpha_j}x$ of $\mathcal{O}_K/p\mathcal{O}_K$. Since $(\alpha\alpha_j)^2 \in p\mathcal{O}_K$, the square of this linear transformation is the 0-map. It follows that $\text{Tr}(M_{\overline{\alpha\alpha_j}}) = 0$, that is $p \mid \text{Tr}_{\mathbb{Q}}^K(\alpha\alpha_j)$. Therefore, $\text{disc}(\alpha_1, \dots, \alpha_n) = \det(\text{Tr}(\alpha_i\alpha_j)) \in p\mathbb{Z}$. \square

3.31 Example. Let α satisfy $\alpha^3 = \alpha + 1$. The discriminant of $\mathbb{Q}(\alpha)$ is -23 and its ring of integers is $\mathbb{Z}[\alpha]$. In Example 3.10 we saw that 23 ramifies in $\mathbb{Q}(\alpha)$. Since 23 is the only prime divisor of the discriminant, it is the only ramifying prime.

3.32 Example. Let p be a prime number and $r \in \mathbb{N}^*$ and, moreover, $r \geq 2$ if $p = 2$. The discriminant of the cyclotomic field $\mathbb{Q}(\zeta_{p^r})$ is a divisor of a power of p . (Lemma 1.48). We have for ideals in the ring of integers $(p) = (1 - \zeta_{p^r})^{\varphi(p^r)}$. The prime p totally ramifies in $\mathbb{Q}(\zeta_{p^r})$. Since $\varphi(p^r) > 1$ the field is not \mathbb{Q} , so p ramifies. By Theorem 3.30 it is the only ramifying prime.

EXERCISES

1. Let R be a number ring. Show that nonzero prime ideals of R are maximal.
2. Let $m \in \mathbb{Z}$ be squarefree and $\neq 1$. Prove that $\mathbb{Z}[\sqrt{m}]$ is a Dedekind domain if and only if $m \equiv 2, 3 \pmod{4}$.
3. Prove the following for ideals in $\mathbb{Z}[\sqrt{3}]$:

$$(33, 7 - 3\sqrt{3}) = (4 + 3\sqrt{3}),$$

$$(13, 7 + 5\sqrt{3}) = (4 + \sqrt{3}),$$

$$(1 + \sqrt{3}) = (1 - \sqrt{3}),$$

$$(4 + \sqrt{3}) \neq (4 - \sqrt{3}).$$

4. Compute the norm of the following ideals of $\mathbb{Z}[\sqrt{7}]$:

$$\begin{array}{ccccccc} (\sqrt{7}), & (8 + 3\sqrt{7}), & (1 + \sqrt{7}), & & (3 + \sqrt{7}), \\ (2 + \sqrt{7}), & (1 + \sqrt{7}, 3 + \sqrt{7}), & (1 + \sqrt{7}) \cap (3 + \sqrt{7}). & & \end{array}$$

5. Let $\omega = \sqrt{-14}$. Factorize the following ideals of $\mathbb{Z}[\sqrt{-14}]$ as a product of maximal ideals:

$$\begin{array}{cccc} (11 - \omega), & (2 - \omega), & (22 - 22\omega), & (13 - 2\omega), \\ (1 - \omega), & (13 - 2\omega)(1 - \omega), & (11 - \omega, 2 - \omega), & (11 - \omega, 1 - \omega), \\ (13 - 2\omega, 1 - \omega), & (11 - \omega) \cap (1 - \omega). & & \end{array}$$

6. Compute all nonzero ideals \mathfrak{a} of $\mathbb{Z}[\sqrt{10}]$ with $N(\mathfrak{a}) \leq 17$.

7. Prove that $\mathbb{Z}[\frac{1}{2} + \frac{1}{2}\sqrt{-19}]$ is a principal ideal domain.

8. Prove that $\mathbb{Z}[\sqrt{6}]$ is a principal ideal domain. (It is even Euclidean.)

9. Prove that the ideal class group of $\mathbb{Q}(\sqrt{-6})$ is of order 2.

10. Show that the ring of integers of $\mathbb{Q}(\sqrt{m})$ is not a principal ideal domain for m squarefree < 0 , $m \not\equiv 5 \pmod{8}$ and $m \neq -1, -2, -7$.

11. We will show that the Mordell equation for $k = -5$ has no solutions. (See exercise 10 of chapter 1.) Let $x, y \in \mathbb{Z}$ satisfy $y^2 + 5 = x^3$.

(i) Show that x is odd and that y is even.

(ii) Prove that the ideal $(y + \sqrt{-5})$ of $\mathbb{Z}[\sqrt{-5}]$ is the cube of an ideal.

(iii) Show that $y + \sqrt{-5}$ is a cube in $\mathbb{Z}[\sqrt{-5}]$ and this leads to a contradiction.

(iv) Also the identity $(y^2 + 4) = (x - 1)(x^2 + x + 1)$ for $x, y \in \mathbb{Z}$ leads to a contradiction. How? (Hint: show that $x^2 + x + 1 \equiv 3 \pmod{4}$.)

12. Let K be a number field of degree n and let $(\alpha_1, \dots, \alpha_n)$ be a \mathbb{Q} -basis of K with $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$. Put $d = \text{disc}(\alpha_1, \dots, \alpha_n)$. Show that a prime divisor p of d with $v_p(d)$ odd ramifies in K .

13. (i) Show that for $K = \mathbb{Q}(\sqrt{-23})$ we can take $\lambda = 11$ in Proposition 3.24.

(ii) Compute the prime ideal factorizations of the ideals (p) of $\mathbb{Z}[\omega_{-23}]$ for the prime numbers $p \leq 11$.

(iii) Compute the prime ideal factorization of the ideals (ω_{-23}) and $(1 + \omega_{-23})$ of $\mathbb{Z}[\omega_{-23}]$.

(iv) Compute the ideal class group of $\mathbb{Q}(\sqrt{-23})$.

14. Let $\alpha \in \mathbb{R}$ satisfy $\alpha^3 = \alpha + 2$. The ring $\mathbb{Z}[\alpha]$ is the ring of integers of $\mathbb{Q}(\alpha)$ (exercise 6(ii) of chapter 1).

(i) Compute all prime ideals \mathfrak{p} of $\mathbb{Z}[\alpha]$ of norm ≤ 10 .

(ii) What is the number of nonzero ideals \mathfrak{a} of $\mathbb{Z}[\alpha]$ of norm ≤ 10 ?

(iii) Show that the nonzero ideals of $\mathbb{Z}[\alpha]$ of norm ≤ 10 are principal.

(iv) Which prime numbers ramify in $\mathbb{Q}(\alpha)$? Compute their factorization in $\mathbb{Z}[\alpha]$.

15. Let K be a number field of degree n and suppose that p is a prime number less than n which splits completely in K . Show that there is no $\alpha \in \mathcal{O}_K$ such that $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

3 Rings of Integers of Number Fields

16. Let K be the unique cubic subfield of $\mathbb{Q}(\zeta_{31})$. Prove that there is no $\alpha \in \mathcal{O}_K$ such that $\mathcal{O}_K = \mathbb{Z}[\alpha]$.
17. (i) Show that the ideals (2), (3) and (7) of $\mathbb{Z}[\zeta_5]$ are prime.
(ii) Show that 5 totally ramifies in $\mathbb{Z}[\zeta_5]$ and that the prime ideal of $\mathbb{Z}[\zeta_5]$ above 5 is principal.
(iii) Show that 11 splits completely in $\mathbb{Z}[\zeta_5]$ and that $(2 + \zeta_5)$ is a prime ideal of $\mathbb{Z}[\zeta_5]$ above 11.
(iv) Show that $1 + \zeta_5$, $1 + \zeta_5 + \zeta_5^2$ and $1 + \zeta_5 + \zeta_5^2 + \zeta_5^3$ are units of $\mathbb{Z}[\zeta_5]$.
18. Let $\alpha \in \mathbb{C}$ be an algebraic integer with minimal polynomial $f \in \mathbb{Z}[X]$. Let p be a prime number with $p \nmid \text{disc}(f)$. Show that $p \nmid (\mathcal{O}_K : \mathbb{Z}[\alpha])$.
19. Let $\alpha \in \mathbb{C}$ be an algebraic integer with minimal polynomial $f \in \mathbb{Z}[X]$. Let $k \in \mathbb{Z}$ and p a prime number such that $p \mid f(k)$ and $p^2 \nmid f(k)$. Prove that the ideal $(p, \alpha - k)$ of \mathcal{O}_K is a prime ideal of norm p .
20. Let p be a prime number. Let's call a polynomial

$$f = X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n \in \mathbb{Z}[X]$$

an Eisenstein p -polynomial if $p \mid a_1, \dots, a_n$ and $p^2 \nmid a_n$. Let K be a number field of degree n .

- (i) Suppose that p totally ramifies in K , say $(p) = \mathfrak{p}^n$ in \mathcal{O}_K . Let $\alpha \in \mathfrak{p} \setminus \mathfrak{p}^2$. Show that the minimal polynomial of α over \mathbb{Q} is an Eisenstein p -polynomial.
- (ii) Let $K = \mathbb{Q}(\alpha)$ with $\alpha \in \mathcal{O}_K$. Suppose that the minimal polynomial of α over \mathbb{Q} is an Eisenstein p -polynomial. Prove that p totally ramifies in K .
- (iii) Suppose that p totally ramifies in K . Prove that there is an $\alpha \in \mathcal{O}_K$ such that $p \nmid (\mathcal{O}_K : \mathbb{Z}[\alpha])$.
21. Let p be a prime number, r a positive integer and $\vartheta = \zeta_{p^r} + \zeta_{p^r}^{-1}$. Show that p totally ramifies in $\mathbb{Q}(\vartheta)$. Show that the unique prime ideal of $\mathbb{Z}[\vartheta]$ above p is principal.

4 Quadratic Number Fields

Fractional ideals of quadratic number fields are lattices of rank 2. They are equivalent to lattices having 1 as a first basis element. Such fractional ideals are determined by the second basis element. Thus equivalence of ideals is translated into equivalence in the set of these second elements. This is the basis for algorithms for ideal class groups of quadratic number fields. In the imaginary case the action of $\mathrm{SL}_2(\mathbb{Z})$ on the upper half of the complex plane is used, whereas in the real case use is made of continued fractions. Continued fractions are also used to show the existence of a fundamental unit for real quadratic number fields. Moreover, they provide an easy computation of the fundamental unit (section 4.8).

In the last section the 2-rank of the ideal class group is determined. Especially in the real case this is—though not difficult—quite elaborate because of the many case distinctions that have to be made. Later, when the main theorems of class field theory are available, it will be an easy application (Application 15.68).

Throughout this chapter m is a squarefree integer $\neq 1$.

The discriminant of the quadratic number field $\mathbb{Q}(\sqrt{m})$ is denoted by D_m (so $D_m = m$ if $m \equiv 1 \pmod{4}$ and $D_m = 4m$ otherwise). In the first section it is shown that the splitting behavior of prime numbers in $\mathbb{Q}(\sqrt{m})$ is determined by their residue class modulo $|D_m|$. It is an application of the well-known Quadratic Reciprocity Law.

4.1 The Quadratic Reciprocity Law

An interesting question is

Which primes remain prime in a given quadratic number field?

In the previous chapter we saw that an odd prime p remains prime in $\mathbb{Q}(\sqrt{m})$ if and only if \bar{m} is not a square in \mathbb{F}_p . So the question

In which quadratic number fields does a given prime remain prime?

is relatively easy: only a finite number of cases need to be considered. At first sight the first question is difficult. However, the *Quadratic Reciprocity Law* makes it accessible. The notation introduced in the following definition will be used in its formulation.

4.1 Definition. Let p be an odd prime and $a \in \mathbb{Z}$. We define:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a, \\ 1 & \text{if } p \nmid a \text{ and } a \text{ is quadratic residue modulo } p, \\ -1 & \text{if } p \nmid a \text{ and } a \text{ is a quadratic nonresidue modulo } p. \end{cases}$$

$\left(\frac{a}{p}\right)$ is called a *Legendre symbol*.

For a fixed odd prime p the Legendre symbol can be seen as a map

$$\mathbb{Z} \rightarrow \{0, 1, -1\}, a \mapsto \left(\frac{a}{p}\right)$$

and since $\left(\frac{a}{p}\right)$ depends only on the residue class of a modulo p , it determines a map

$$\mathbb{F}_p \rightarrow \{0, 1, -1\}, \bar{a} \mapsto \left(\frac{a}{p}\right).$$

The group \mathbb{F}_p^* is cyclic of even order, so the squares in this group form a subgroup of index 2. The image of the group homomorphism $\mathbb{F}_p^* \rightarrow \mathbb{F}_p^*$, $\bar{a} \mapsto \bar{a}^{\frac{p-1}{2}}$ is $\{\bar{1}, -\bar{1}\}$ and the unique subgroup of index 2 is its kernel. From this follows:

4.2 Proposition (Euler's criterion). Let $a \in \mathbb{Z}$ and p an odd prime. Then

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}. \quad \square$$

Easy consequences of this criterion are:

4.3 Corollary. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ for all odd primes p and all $a, b \in \mathbb{Z}$. □

4.4 Corollary. Let p be an odd prime number. Then $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$. □

The first proofs of the Quadratic Reciprocity Law were given by Gauß. Here we give a proof of the Quadratic Reciprocity Law using finite fields as described in [22]. Another proof, using the theory of splitting of primes in abelian number fields, will be given in chapter 7. First we compute the Legendre symbol $\left(\frac{2}{p}\right)$.

4.5 Proposition. Let p be an odd prime. Then $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

PROOF. Let L be the splitting field of $X^8 - 1$ over \mathbb{F}_p . Then $L = \mathbb{F}_p(\zeta)$, where ζ is a primitive 8-th root of unity. The element $\eta = \zeta + \zeta^{-1} \in L$ satisfies

$$\eta^2 = (\zeta + \zeta^{-1})^2 = \zeta^2 + \zeta^{-2} + \bar{2} = \zeta^{-2}(\zeta^4 + \bar{1}) + \bar{2} = \bar{2}.$$

So $\bar{2}$ is a square in \mathbb{F}_p if and only if $\eta \in \mathbb{F}_p$ and this in turn is equivalent to $\eta^p = \eta$. From $\eta^p = \zeta^p + \zeta^{-p}$ it follows easily that $\eta^p = \eta$ if and only if $p \equiv \pm 1 \pmod{8}$. \square

The sign of $(-1)^{\frac{p^2-1}{8}}$ depends only on p modulo 8. We could also write

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 7 \pmod{8}, \\ -1 & \text{if } p \equiv 3, 5 \pmod{8}. \end{cases}$$

Prime numbers are positive by definition. Another choice for a system of representatives of the irreducible integers modulo association is obtained by requiring the odd ones to be congruent to 1 modulo 4. For p an odd prime, p^* is the prime associated to p which is congruent to 1 modulo 4. This notation is used in the proof of the Quadratic Reciprocity Law below.

4.6 Notation. For odd $n \in \mathbb{Z}$ we write $n^* = (-1)^{\frac{n-1}{2}} n$.

4.7 Theorem (Quadratic Reciprocity Law). *Let p and q be different odd primes. Then*

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

PROOF. Let L be the splitting field of $f = X^q - 1 \in \mathbb{F}_p[X]$ over \mathbb{F}_p . Then $L = \mathbb{F}_p(\zeta)$, where ζ is a primitive q -th root of unity. The discriminant of f is easily computed:

$$\text{disc}(f) = (-1)^{\frac{q-1}{2}} \prod_{k=0}^{q-1} f'(\zeta^k) = (-1)^{\frac{q-1}{2}} \prod_{k=0}^{q-1} q\zeta^{q-1} = (-1)^{\frac{q-1}{2}} q^q = q^* q^{q-1} \in \mathbb{F}_p.$$

The Galois group $\text{Gal}_{\mathbb{F}_p}(f)$ of the polynomial f is the group of permutations of the set $\{1, \zeta, \dots, \zeta^{q-1}\}$ induced by the automorphisms in $\text{Gal}(L : \mathbb{F}_p)$. The group $\text{Gal}(L : \mathbb{F}_p)$ is generated by the automorphism given by $\zeta \mapsto \zeta^p$. So $\text{Gal}_{\mathbb{F}_p}(f)$ is the cyclic group generated by the permutation $\sigma : \zeta^j \mapsto \zeta^{jp}$ of $\{1, \zeta, \dots, \zeta^{q-1}\}$. It is a product of $\frac{q-1}{n}$ disjoint cycles of length n , where n is the order of p in \mathbb{F}_q^* . We have

$$\begin{aligned} \left(\frac{q^*}{p}\right) = 1 &\iff \text{disc}(f) \text{ is a square modulo } p \\ &\iff \text{Gal}_{\mathbb{F}_p}(f) \text{ consists of even permutations} \\ &\iff \sigma \text{ is an even permutation} \\ &\iff \frac{q-1}{n} \text{ is even} \iff n \mid \frac{q-1}{2} \iff \left(\frac{p}{q}\right) = 1. \end{aligned}$$

4 Quadratic Number Fields

So we have

$$\left(\frac{p}{q}\right)\left(\frac{q^*}{p}\right) = 1$$

and since

$$\left(\frac{q^*}{p}\right) = \left(\frac{(-1)^{\frac{q-1}{2}}}{p}\right) = \left(\frac{-1}{p}\right)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left(\frac{q}{p}\right),$$

the Quadratic Reciprocity Law follows. \square

4.8 Application. Corollary 4.4 and Proposition 4.5 are called the *Subsidiary Laws* for Quadratic Reciprocity. The Quadratic Reciprocity Law and its Subsidiary Laws enable us to compute Legendre symbols; for example

$$\left(\frac{59}{97}\right) = -\left(\frac{97}{59}\right) = -\left(\frac{38}{59}\right) = -\left(\frac{2}{59}\right)\left(\frac{19}{59}\right) = \left(\frac{19}{59}\right) = -\left(\frac{59}{19}\right) = -\left(\frac{2}{19}\right) = 1.$$

Since in the computation numbers have to be factorized, for large numbers this is an obstacle. See, however, the end of this section, especially Application 4.15.

4.9 Examples. For odd primes p we know that p remains prime in a quadratic number field $\mathbb{Q}(\sqrt{m})$ if and only if $\left(\frac{m}{p}\right) = -1$. So Corollary 4.4 implies

$$p \text{ remains prime in } \mathbb{Q}(i) \iff p \equiv 3 \pmod{4}$$

and by Proposition 4.5 we have

$$p \text{ remains prime in } \mathbb{Q}(\sqrt{2}) \iff p \equiv 3, 5 \pmod{8}$$

and

$$p \text{ remains prime in } \mathbb{Q}(\sqrt{-2}) \iff p \equiv 5, 7 \pmod{8}.$$

From

$$\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{3}} \left(\frac{p}{3}\right)$$

follows that

$$p \text{ remains prime in } \mathbb{Q}(\sqrt{3}) \iff p \equiv 3, 7 \pmod{12}$$

and

$$p \text{ remains prime in } \mathbb{Q}(\sqrt{-3}) \iff p \equiv 2 \pmod{3}.$$

For the quadratic number fields K in the examples we see that there is an $N \in \mathbb{N}^*$ such that the splitting behavior in K of a prime only depends on its residue class modulo N . This is a consequence of the Quadratic Reciprocity Law and we will see that this holds for quadratic number fields in general. The following lemma will be used:

4.10 Lemma. Let $n \in \mathbb{Z}$ with $n \neq 0$. Then n has a unique factorization

$$n = up_1^{*k_1} \cdots p_r^{*k_r},$$

where p_1, \dots, p_r are different odd primes, $k_1, \dots, k_r \in \mathbb{N}^*$ and $u \in \{\pm 2^k \mid k \in \mathbb{N}\}$.

PROOF. This is just the unique factorization in the principal ideal domain \mathbb{Z} with another choice for the irreducible elements. \square

4.11 Proposition. For each odd prime p the Legendre symbol $\left(\frac{m}{p}\right)$ only depends on the residue class of p modulo $|D_m|$.

PROOF. Use the factorization of the squarefree m as in the above lemma:

$$m = up_1^* \cdots p_r^*.$$

Then $u \in \{1, -1, 2, -2\}$ and by quadratic reciprocity we have

$$\left(\frac{m}{p}\right) = \left(\frac{u}{p}\right) \left(\frac{p_1^*}{p}\right) \cdots \left(\frac{p_r^*}{p}\right) = \left(\frac{u}{p}\right) \left(\frac{p}{p_1}\right) \cdots \left(\frac{p}{p_r}\right).$$

From this the proposition follows. Note that $u = 1$ if $m \equiv 1 \pmod{4}$, $u = \pm 2$ if $m \equiv 2 \pmod{4}$, and $u = -1$ if $m \equiv 3 \pmod{4}$. \square

So for the splitting behavior of primes in a given quadratic number field only a finite number of cases have to be considered:

4.12 Corollary. For odd prime numbers p, q with $p \equiv q \pmod{|D_m|}$ we have

$$p \text{ remains prime in } \mathbb{Q}(\sqrt{m}) \iff q \text{ remains prime in } \mathbb{Q}(\sqrt{m}). \quad \square$$

In chapter 9 another proof of this phenomenon will be given.

The proof of Proposition 4.11 suggests that the following definition could be useful.

4.13 Definition. Let $b \in \mathbb{N}^*$ with b odd and let $a \in \mathbb{Z}$. We define:

$$\left(\frac{a}{b}\right) = \prod_{p|b} \left(\frac{a}{p}\right)^{v_p(b)}.$$

This symbol is called the *Jacobi symbol*.

What makes this symbol interesting is the following theorem, which is a generalization of the Quadratic Reciprocity Law and its Subsidiary Laws. The proof is straightforward when using the following congruences:

$$b = \prod_{p|b} (1 + (p-1))^{v_p(b)} \equiv \prod_{p|b} (1 + v_p(b)(p-1)) \equiv 1 + \sum_{p|b} v_p(b)(p-1) \pmod{4}.$$

and

$$b^2 = \prod_{p|b} (1 + (p^2 - 1))^{v_p(b)} \equiv \prod_{p|b} (1 + v_p(b)(p^2 - 1)) \equiv 1 + \sum_{p|b} v_p(b)(p^2 - 1) \pmod{16}.$$

4.14 Theorem.

(i) Let $b \in \mathbb{N}^*$ be odd and $a_1, a_2 \in \mathbb{Z}$ such that $a_1 \equiv a_2 \pmod{b}$.

$$\text{Then } \left(\frac{a_1}{b}\right) = \left(\frac{a_2}{b}\right).$$

(ii) Let $b \in \mathbb{N}^*$ be odd. Then $\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}}$.

(iii) Let $b \in \mathbb{N}^*$ be odd. Then $\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}}$.

(iv) Let $a, b \in \mathbb{N}^*$ be odd such that $\gcd(a, b) = 1$.

$$\text{Then } \left(\frac{a}{b}\right) \left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2} \cdot \frac{b-1}{2}}. \quad \square$$

4.15 Application. Jacobi symbols can be computed without factorizing numbers. As a result the computation is as fast as the well known Euclidean algorithm for the computation of the greatest common divisor. Lets verify whether 1741 is a square modulo the prime 3299:

$$\begin{aligned} \left(\frac{1741}{3299}\right) &= \left(\frac{3299}{1741}\right) = \left(\frac{1558}{1741}\right) = \left(\frac{2}{1741}\right) \left(\frac{779}{1741}\right) = -\left(\frac{779}{1741}\right) = -\left(\frac{1741}{779}\right) \\ &= -\left(\frac{183}{779}\right) = \left(\frac{779}{183}\right) = \left(\frac{47}{183}\right) = -\left(\frac{183}{47}\right) = -\left(\frac{42}{47}\right) = -\left(\frac{2}{47}\right) \left(\frac{21}{47}\right) \\ &= -\left(\frac{21}{47}\right) = -\left(\frac{47}{21}\right) = -\left(\frac{5}{21}\right) = -\left(\frac{21}{5}\right) = -\left(\frac{1}{5}\right) = -1. \end{aligned}$$

So 1741 is not a square modulo 3299.

4.2 Equivalence of quadratic numbers

A fractional ideal of the quadratic number field $\mathbb{Q}(\sqrt{m})$ is a lattice $\mathbb{Z}\gamma_1 + \mathbb{Z}\gamma_2$ of $\mathbb{Q}(\sqrt{m})$. The fractional ideal is equivalent to $\mathbb{Z} + \mathbb{Z}\frac{\gamma_2}{\gamma_1}$. Our first concern is: for which $\gamma \in \mathbb{Q}(\sqrt{m}) \setminus \mathbb{Q}$ is $\mathbb{Z} + \mathbb{Z}\gamma$ a fractional ideal of $\mathbb{Q}(\sqrt{m})$? The answer is simple. We use the following terminology:

4.16 Definition. A $\gamma \in \mathbb{C}$ is called a *quadratic number* if it is a zero of an irreducible polynomial of degree 2 over \mathbb{Q} . As is easily verified, a quadratic number is the zero of a unique polynomial of the form $aX^2 + bX + c \in \mathbb{Z}[X]$, where $a > 0$ and $\gcd(a, b, c) = 1$. The integer $b^2 - 4ac$ is called the *discriminant* of the quadratic number γ . Notation: $\text{disc}(\gamma)$.

4.17 Lemma. Let $\gamma \in \mathbb{Q}(\sqrt{m}) \setminus \mathbb{Q}$ be a zero of the polynomial $aX^2 + bX + c \in \mathbb{Z}[X]$, where $a > 0$ and $\gcd(a, b, c) = 1$. Then

- (i) $\text{disc}(\gamma) = \text{disc}(a\gamma) = \text{disc}(1, a\gamma)$, the last disc standing for the discriminant of a \mathbb{Q} -basis of $\mathbb{Q}(\sqrt{m})$, and
- (ii) $(\mathbb{Z}a + \mathbb{Z}a\gamma)(\mathbb{Z}a + \mathbb{Z}a\gamma') = a(\mathbb{Z} + \mathbb{Z}a\gamma)$, where the product is the product of lattices.
- (iii) $\mathbb{Z}a + \mathbb{Z}a\gamma$ is an ideal of $\mathbb{Z}[\omega_m]$ if and only if $\mathbb{Z} + \mathbb{Z}a\gamma = \mathbb{Z}[\omega_m]$.

PROOF.

- (i) The polynomial $g = X^2 + bX + ac$ is the minimal polynomial of $a\gamma$ over \mathbb{Q} . We have $\text{disc}(\gamma) = b^2 - 4ac = \text{disc}(a\gamma) = \text{disc}(g) = \text{disc}(1, a\gamma)$.
- (ii) A straightforward computation:

$$\begin{aligned} (\mathbb{Z}a + \mathbb{Z}a\gamma)(\mathbb{Z}a + \mathbb{Z}a\gamma') &= a(\mathbb{Z}a + \mathbb{Z}a\gamma + \mathbb{Z}a\gamma' + \mathbb{Z}a\gamma\gamma') \\ &= a(\mathbb{Z}a + \mathbb{Z}b + \mathbb{Z}c + \mathbb{Z}a\gamma) = a(\mathbb{Z} + \mathbb{Z}a\gamma). \end{aligned}$$

- (iii) If $\mathbb{Z}a + \mathbb{Z}a\gamma$ is an ideal, then by (ii) $\mathbb{Z} + \mathbb{Z}a\gamma$ is an ideal as well and since it contains 1, it equals $\mathbb{Z}[\omega_m]$. Conversely, if $\mathbb{Z} + \mathbb{Z}a\gamma = \mathbb{Z}[\omega_m]$, then $\mathbb{Z}a + \mathbb{Z}a\gamma$ is an ideal: $a^2\gamma, (a\gamma)^2 = -ba\gamma - ca \in \mathbb{Z}a + \mathbb{Z}a\gamma$. \square

4.18 Theorem. Let $\gamma \in \mathbb{Q}(\sqrt{m}) \setminus \mathbb{Q}$. Then $\mathbb{Z} + \mathbb{Z}\gamma$ is a fractional ideal of $\mathbb{Z}[\omega_m]$ if and only if $\text{disc}(\gamma) = D_m$.

PROOF. Let γ be a zero of $aX^2 + bX + c \in \mathbb{Z}[X]$ with $a > 0$ and $\gcd(a, b, c) = 1$. Equivalent are the following:

- $\mathbb{Z} + \mathbb{Z}\gamma$ is a fractional ideal.
- $\mathbb{Z}a + \mathbb{Z}a\gamma$ is an ideal.
- $\mathbb{Z} + \mathbb{Z}\omega_m = \mathbb{Z} + \mathbb{Z}a\gamma$. (Lemma 4.17(iii))
- $\text{disc}(1, \omega_m) = \text{disc}(1, a\gamma)$.
- $D_m = \text{disc}(\gamma)$. (Lemma 4.17(i))

\square

4.19 Definition. Let $z \in \mathbb{C} \setminus \mathbb{Q}$ and $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_2(\mathbb{Z})$ (that is $A \in M_2(\mathbb{Z})$ and $\det(A) = \pm 1$). We define

$$Az = \frac{az + b}{cz + d}.$$

4.20 Proposition. $(A, z) \mapsto Az$ is an action of the group $\text{GL}_2(\mathbb{Z})$ on the set $\mathbb{C} \setminus \mathbb{Q}$.

PROOF. Clearly $Iz = z$. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and let $B = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$. Then

$$\begin{aligned} A(Bz) &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \frac{pz + q}{rz + s} = \frac{a \frac{pz+q}{rz+s} + b}{c \frac{pz+q}{rz+s} + d} = \frac{a(pz + q) + b(rz + s)}{c(pz + q) + d(rz + s)} \\ &= \frac{(ap + br)z + (aq + bs)}{(cp + dr)z + (cq + ds)} = (AB)z. \quad \square \end{aligned}$$

4.21 Definition. Numbers $z_1, z_2 \in \mathbb{C} \setminus \mathbb{Q}$ are called *equivalent* if there is an $A \in \text{GL}_2(\mathbb{Z})$ such that $z_2 = Az_1$. Notation: $z_1 \simeq z_2$. (So numbers are equivalent if they are in the same orbit under the action of $\text{GL}_2(\mathbb{Z})$.)

4.22 Proposition. Let $\gamma_1, \gamma_2 \in \mathbb{C} \setminus \mathbb{Q}$. Then

$$\gamma_1 \simeq \gamma_2 \iff \text{there is a } \beta \in \mathbb{C}^* \text{ such that } \mathbb{Z} + \mathbb{Z}\gamma_2 = \mathbb{Z}\beta + \mathbb{Z}\beta\gamma_1.$$

PROOF.

\Rightarrow : Suppose $\gamma_1 \simeq \gamma_2$, say $\gamma_2 = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \gamma_1$ with $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_2(\mathbb{Z})$. Then

$$\mathbb{Z} + \mathbb{Z}\gamma_2 = \mathbb{Z} + \mathbb{Z} \frac{a\gamma_1 + b}{c\gamma_1 + d} \sim \mathbb{Z}(c\gamma_1 + d) + \mathbb{Z}(a\gamma_1 + b) = \mathbb{Z} + \mathbb{Z}\gamma_1,$$

where the last equality follows from $ad - bc = \pm 1$.

\Leftarrow : Suppose there is a $\beta \in \mathbb{C}^*$ with $\mathbb{Z} + \mathbb{Z}\gamma_1 = \mathbb{Z}\beta + \mathbb{Z}\beta\gamma_2$. Then there is an $A \in \text{GL}_2(\mathbb{Z})$ such that

$$\begin{pmatrix} \gamma_2 \\ 1 \end{pmatrix} = A \begin{pmatrix} \beta\gamma_1 \\ \beta \end{pmatrix}.$$

Put $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Then

$$\gamma_2 = \frac{a\beta\gamma_1 + b\beta}{c\beta\gamma_1 + d\beta} = \frac{a\gamma_1 + b}{c\gamma_1 + d} = A\gamma_1. \quad \square$$

So for fractional ideals in a quadratic number field we have:

4.23 Corollary. Let γ_1 and γ_2 be elements of $\mathbb{Q}(\sqrt{m}) \setminus \mathbb{Q}$ with $\text{disc}(\gamma_1) = \text{disc}(\gamma_2)$. Then

$$\mathbb{Z} + \mathbb{Z}\gamma_1 \sim \mathbb{Z} + \mathbb{Z}\gamma_2 \iff \gamma_1 \simeq \gamma_2. \quad \square$$

Equivalent quadratic numbers have equal discriminants:

4.24 Proposition. *Let $\gamma_1, \gamma_2 \in \mathbb{Q}(\sqrt{m}) \setminus \mathbb{Q}$ such that $\gamma_1 \simeq \gamma_2$. Then $\text{disc}(\gamma_1) = \text{disc}(\gamma_2)$.*

PROOF. The group $\text{GL}_2(\mathbb{Z})$ is generated by the matrices $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ (exercise 6). So it remains to verify that $\text{disc}(\gamma_1) = \text{disc}(\gamma_1 + 1) = \text{disc}(-\gamma_1^{-1}) = \text{disc}(-\gamma_1)$ and this is straightforward. \square

4.3 Equivalence of lattices in \mathbb{C}

In the imaginary quadratic case the field is (embedded as) a subfield of \mathbb{C} . Thus lattices in imaginary quadratic number fields are lattices in the 2-dimensional real vector space \mathbb{C} .

4.25 Definition. Let Λ and Γ be lattices in the real vector space \mathbb{C} . Then Λ and Γ are called *equivalent* if there is an $\alpha \in \mathbb{C}$ such that $\alpha\Lambda = \Gamma$.

A lattice in the real vector space \mathbb{C} is equivalent to a lattice $\mathbb{Z} + \mathbb{Z}\gamma$ with $\Im(\gamma) > 0$: a lattice $\mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2$ is equivalent to $\mathbb{Z} + \mathbb{Z}\frac{\alpha_2}{\alpha_1} = \mathbb{Z} + \mathbb{Z}\frac{-\alpha_2}{\alpha_1}$.

The group $SL_2(\mathbb{Z})$ acts on the upper half plane $H = \{z \in \mathbb{C} \mid \Im(z) > 0\}$:

$$SL_2(\mathbb{Z}) \times H \rightarrow H, \quad \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, z \right) \mapsto \frac{az + b}{cz + d}.$$

From

$$\Im(Az) = \frac{\det A \cdot \Im(z)}{|cz + d|^2}, \tag{4.1}$$

where $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, indeed it follows that $Az \in H$ if $z \in H$ and $A \in SL_2(\mathbb{Z})$. By Proposition 4.22 and formula 4.1 we have:

4.26 Proposition. *Let $\gamma_1, \gamma_2 \in H$. Then the lattices $\mathbb{Z} + \mathbb{Z}\gamma_1$ and $\mathbb{Z} + \mathbb{Z}\gamma_2$ in \mathbb{C} are equivalent if and only if there is an $A \in SL_2(\mathbb{Z})$ with $\gamma_2 = A\gamma_1$. \square*

4.27 Notation. A domain G in the upper half plane H is defined as follows:

$$G = \{z \in \mathbb{C} \mid \Im(z) > 0, -\frac{1}{2} < \Re(z) \leq \frac{1}{2}, |z| \geq 1, |z| > 1 \text{ if } \Re(z) < 0\}.$$

See Figure 4.1.

This domain G is a fundamental domain for the action of $SL_2(\mathbb{Z})$ on H :

4.28 Theorem. *G is a system of representatives of H/\simeq .*

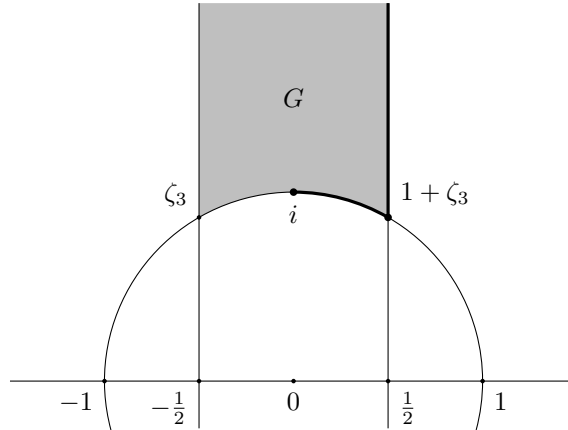


Figure 4.1: A fundamental domain for the action of $SL_2(\mathbb{Z})$ on H

PROOF. Let $z \in H$. First we prove that there is an $A \in SL_2(\mathbb{Z})$ such that $Az \in G$. For $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ we have

$$\Im(Az) = \frac{\Im(z)}{|cz + d|^2}.$$

Because $c, d \in \mathbb{Z}$, the number of pairs (c, d) with $|cz + d|$ less than a given number is finite. From this it follows that there is an $A \in SL_2(\mathbb{Z})$ with $\Im(Az)$ maximal. For $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ we have

$$\Im(TAz) = \Im(Az + 1) = \Im(Az).$$

Now let $n \in \mathbb{Z}$ be such that

$$-\frac{1}{2} < \Re(T^n Az) \leq \frac{1}{2}.$$

Then $\Im(T^n Az)$ is maximal as well. It follows that $|T^n Az| \geq 1$, since otherwise the imaginary part of $-\frac{1}{T^n Az}$ ($= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} T^n Az$) would be greater than the imaginary part of $T^n Az$. If $\Re(T^n Az) < 0$ and $|T^n Az| = 1$, then take $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} T^n Az$. Hence for each $z \in H$ there is an $A \in SL_2(\mathbb{Z})$ with $Az \in G$.

Now suppose $z_1, z_2 \in G$ with $z_1 \simeq z_2$, say $z_2 = Az_1$ with $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. We may assume that $\Im(z_2) \geq \Im(z_1)$, that is $|cz_1 + d| \leq 1$. Since $z_1 \in G$ this is only possible if $|c| \leq 1$: if $|c| \geq 2$, then

$$|\Im(cz_1 + d)| = |c| \cdot |\Im(z_1)| \geq 2 \cdot \frac{1}{2} \sqrt{3} > 1.$$

For $c = 0$: $A = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ (if necessary replace A by $-A$) and so $z_2 = z_1 + b$. Comparison of the real parts yields $b = 0$, that is $z_2 = z_1$.

For $c = 1$: from $|z_1 + d| \leq 1$ follows that there are only two possibilities left:

4.4 Algorithm for the ideal class group of an imaginary quadratic number field

1. $z_1 = \omega + 1$ and $d = -1$. Then $b = -1 - a$ and $z_2 = \frac{a(\omega+1) - (a+1)}{\omega+1-1} = 1 + \omega + a$. So $a = 0$ and $z_2 = z_1$.
2. $|z_1| = 1$ and $d = 0$. Then $b = -1$ and $z_2 = a - \bar{z}_1$. It follows that $-\bar{z}_1 = i$ and $a = 0$ (and then $z_2 = i = z_1$), or $-\bar{z}_1 = \zeta_3$ and $a = 1$ (and then $z_2 = 1 + \zeta_3 = z_1$).

For $c = -1$: replacement of A by $-A$ brings us to the case $c = 1$.

So for each $z \in H$ there is a unique $w \in G$ with $w \simeq z$. □

4.4 Algorithm for the ideal class group of an imaginary quadratic number field

In this section m is negative. Fractional ideals of an imaginary quadratic number field are lattices in \mathbb{C} and they are congruent modulo the subgroup of principal fractional ideals if and only if they are equivalent as lattices in \mathbb{C} .

4.29 Proposition. *Let $G_m = \{ \gamma \in G \cap \mathbb{Q}(\sqrt{m}) \mid \text{disc}(\gamma) = D_m \}$. Then the map*

$$G_m \rightarrow \mathcal{C}(\mathbb{Q}(\sqrt{m})), \quad \gamma \mapsto \text{class of } \mathbb{Z} + \mathbb{Z}\gamma$$

is a bijection.

PROOF. Suppose $\gamma_1, \gamma_2 \in G_m$. If $\mathbb{Z} + \mathbb{Z}\gamma_1 \sim \mathbb{Z} + \mathbb{Z}\gamma_2$, then by Proposition 4.22 $\gamma_1 \simeq \gamma_2$. Because $\gamma_1, \gamma_2 \in G$, we have by Theorem 4.28 $\gamma_1 = \gamma_2$. So the map is injective.

Now let $\gamma \in \mathbb{Q}(\sqrt{m})$ with $\text{disc}(\gamma) = D_m$. Then to prove that there is a $\gamma_0 \in G_m$ with $\mathbb{Z} + \mathbb{Z}\gamma_0 \sim \mathbb{Z} + \mathbb{Z}\gamma$. By Theorem 4.28 there is a $\gamma_0 \in G$ with $\gamma_0 \simeq \gamma$. By Proposition 4.24 we have $\text{disc}(\gamma_0) = \text{disc}(\gamma) = D_m$, and so $\gamma_0 \in G \cap \mathbb{Q}(\sqrt{m})$. Finally by Proposition 4.22: $\mathbb{Z} + \mathbb{Z}\gamma_0 \sim \mathbb{Z} + \mathbb{Z}\gamma$. □

So the fractional ideals $\mathbb{Z} + \mathbb{Z}\gamma$ with $\gamma \in G_m$ form a system of representatives of the fractional ideals modulo the principal fractional ideals. The condition $\gamma \in G_m$ is easily translated into conditions on a triple $(a, b, c) \in \mathbb{Z}^3$:

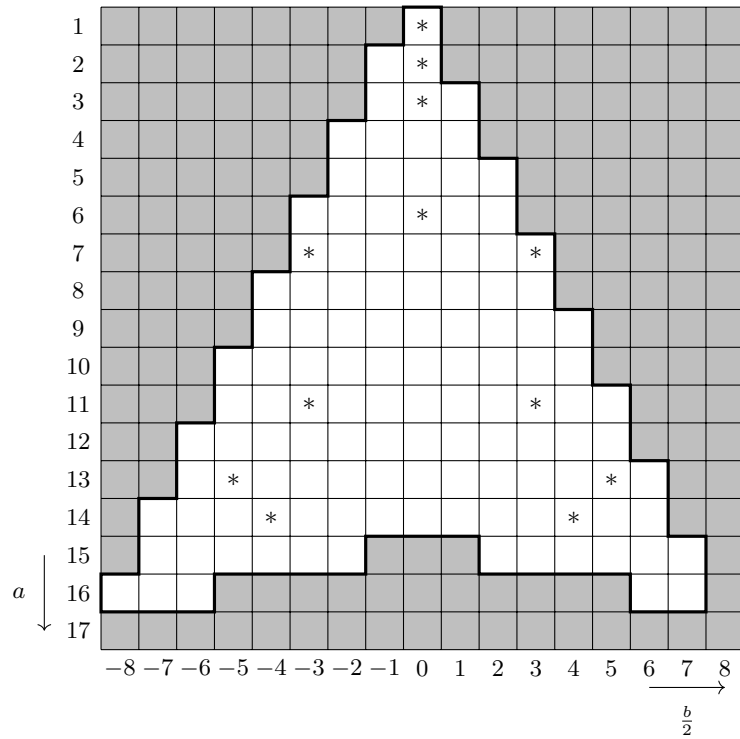
4.30 Definition.

$$V_m = \{ (a, b, c) \in \mathbb{Z}^3 \mid a > 0, b^2 - 4ac = D_m, -a \leq b < a, c \geq a, c > a \text{ if } b > 0 \}.$$

By definition of the discriminant of a quadratic number the map

$$V_m \rightarrow G_m, \quad (a, b, c) \mapsto \frac{-b + \sqrt{D_m}}{2a}$$

is a bijection.



$\left(\frac{b}{2}\right)^2 - m (= ac) :$ 286 271 258 247 238 231 226 223 222 223 226 231 238 247 258 271 286

Figure 4.2: Computation of a system of representatives of $\mathcal{C}(\mathbb{Q}(\sqrt{-222}))$

4.31 Corollary. *The map*

$$(a, b, c) \mapsto \text{class of } \mathbb{Z}a + \mathbb{Z}\frac{-b + \sqrt{D_m}}{2}$$

from V_m to $\mathcal{C}(\mathbb{Q}(\sqrt{m}))$ is a bijection. □

Again it follows that $\mathcal{C}(\mathbb{Q}(\sqrt{m}))$ is finite: let $(a, b, c) \in V_m$, then

$$4a^2 \leq 4ac = b^2 - D_m \leq a^2 - D_m$$

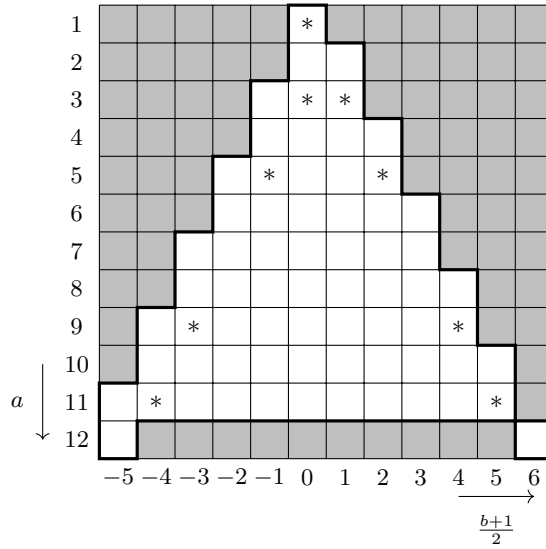
and so

$$3a^2 \leq -D_m$$

that is

$$a \leq \sqrt{\frac{-D_m}{3}}.$$

4.4 Algorithm for the ideal class group of an imaginary quadratic number field



$$\frac{b+1}{2} \cdot \frac{b-1}{2} + \frac{1-m}{4} (= ac) : \quad 153 \quad 143 \quad 135 \quad 129 \quad 125 \quad 123 \quad 123 \quad 125 \quad 129 \quad 135 \quad 143 \quad 153$$

Figure 4.3: Computation of a system of representatives of $\mathcal{C}(\mathbb{Q}(\sqrt{-491}))$

There are only finitely many such a . For each a there are finitely many b with $-a \leq b < a$, and for given a and b there is at most one c with $b^2 - 4ac = D_m$.

Since an ideal $\mathbb{Z}a + \mathbb{Z}\frac{-b+\sqrt{D_m}}{2}$ has norm a , for the λ in Proposition 3.24 we can take: $\left\lfloor \sqrt{\frac{-D_m}{3}} \right\rfloor$. That is slightly better than $\left\lfloor \frac{2}{\pi} \sqrt{-D_m} \right\rfloor$, the value that will follow from estimates obtained in chapter 5 for number fields in general: Theorem 5.17, see also Examples 5.12.

4.32 Example. $m = -222$. Then $D_m = 4m = -888$ and $\frac{-D_m}{3} = 296$. So $a \leq \lfloor \sqrt{296} \rfloor = 17$. A system of representatives of the ideal class group is the set of the following ideals (where $\omega = \sqrt{-222}$):

$$\begin{array}{cccc}
 \mathbb{Z} + \mathbb{Z}\omega & \mathbb{Z}2 + \mathbb{Z}\omega & \mathbb{Z}3 + \mathbb{Z}\omega & \mathbb{Z}6 + \mathbb{Z}\omega \\
 \mathbb{Z}7 + \mathbb{Z}(3 + \omega) & \mathbb{Z}7 + \mathbb{Z}(-3 + \omega) & \mathbb{Z}11 + \mathbb{Z}(3 + \omega) & \mathbb{Z}11 + \mathbb{Z}(-3 + \omega) \\
 \mathbb{Z}13 + \mathbb{Z}(5 + \omega) & \mathbb{Z}13 + \mathbb{Z}(-5 + \omega) & \mathbb{Z}14 + \mathbb{Z}(4 + \omega) & \mathbb{Z}14 + \mathbb{Z}(-4 + \omega)
 \end{array}$$

See Figure 4.2. By Corollary 3.22 inversion in the ideal class group is induced by $(a, b, c) \mapsto (a, -b, c)$, which in the diagram corresponds to the reflection in $b = 0$. The classes of order ≤ 2 are represented by the ideals

$$\mathbb{Z} + \mathbb{Z}\omega, \quad \mathbb{Z}2 + \mathbb{Z}\omega, \quad \mathbb{Z}3 + \mathbb{Z}\omega \quad \text{and} \quad \mathbb{Z}6 + \mathbb{Z}\omega.$$

4 Quadratic Number Fields

So the ideal class group is an abelian group of order 12 and its 2-rank is 2: its structure is $C_6 \times C_2$.

4.33 Example. $m = -491$. Then $D_m = m = -491$ and $a \leq \left\lfloor \sqrt{\frac{491}{3}} \right\rfloor = 12$. From $b^2 - 4ac = D_m$ follows that b is odd. A system of representatives of the ideal class group is formed by the ideals (with $\omega = \frac{1+\sqrt{-491}}{2}$):

$$\begin{array}{lll} \mathbb{Z} + \mathbb{Z}\omega & \mathbb{Z}3 + \mathbb{Z}\omega & \mathbb{Z}3 + \mathbb{Z}(-1 + \omega) \\ \mathbb{Z}5 + \mathbb{Z}(1 + \omega) & \mathbb{Z}5 + \mathbb{Z}(-2 + \omega) & \mathbb{Z}9 + \mathbb{Z}(3 + \omega) \\ \mathbb{Z}9 + \mathbb{Z}(-4 + \omega) & \mathbb{Z}11 + \mathbb{Z}(4 + \omega) & \mathbb{Z}11 + \mathbb{Z}(-5 + \omega) \end{array}$$

See Figure 4.3. The ideal class group is of order 9. The square of the class of an ideal of norm 3 is the class of one of the ideals of norm 9, which is not the inverse class of the ideal of norm 3. So the class of an ideal of norm 3 is of order 9. Therefore, the ideal class group is cyclic.

4.34 The product in $\{\gamma \in \mathbb{Q}(\sqrt{m}) \mid \text{disc}(\gamma) = D_m\}$. Suppose $\gamma_1, \gamma_2 \in \mathbb{Q}(\sqrt{m})$ with $\text{disc}(\gamma_1) = \text{disc}(\gamma_2) = D_m$, i.e. $\mathbb{Z} + \mathbb{Z}\gamma_1$ and $\mathbb{Z} + \mathbb{Z}\gamma_2$ are fractional ideals of $\mathbb{Z}[\omega_m]$. How to determine γ_3 such that

$$(\mathbb{Z} + \mathbb{Z}\gamma_1)(\mathbb{Z} + \mathbb{Z}\gamma_2) \sim \mathbb{Z} + \mathbb{Z}\gamma_3 ?$$

Let the quadratic numbers γ_1 and γ_2 correspond to the triples (a_1, b_1, c_1) and (a_2, b_2, c_2) . We have $\gamma_i = \frac{-b_i + \sqrt{D_m}}{2a_i}$ and $\mathbb{Z} + \mathbb{Z}\gamma_i \sim \mathbb{Z}a_i + \mathbb{Z}\frac{-b_i + \sqrt{D_m}}{2}$. The lattice $\mathbb{Z}a_i + \mathbb{Z}\frac{-b_i + \sqrt{D_m}}{2}$ is an ideal of $\mathbb{Z}[\omega_m]$ with norm a_i . So

$$\left(\mathbb{Z}a_1 + \mathbb{Z}\frac{-b_1 + \sqrt{D_m}}{2}\right)\left(\mathbb{Z}a_2 + \mathbb{Z}\frac{-b_2 + \sqrt{D_m}}{2}\right)$$

is an ideal with norm a_1a_2 . As a lattice this ideal is spanned by

$$a_1a_2, \frac{-a_2b_1 + a_2\sqrt{D_m}}{2}, \frac{-a_1b_2 + a_1\sqrt{D_m}}{2}, \frac{-b_1b_2 + D_m}{2} + \frac{b_1+b_2}{2}\sqrt{D_m}.$$

Let $d = \text{gcd}(a_2, a_1, \frac{b_1+b_2}{2})$ and let $x, y, z \in \mathbb{Z}$ be such that

$$xa_2 + ya_1 + z\frac{b_1 + b_2}{2} = d.$$

Then the lattice is

$$\mathbb{Z}a + \mathbb{Z}\frac{-xa_2b_1 - ya_1b_2 - z\frac{b_1b_2 + D_m}{2} + d\sqrt{D_m}}{2}$$

where $a \in \mathbb{Z}$. The norm is a_1a_2 , so $ad = a_1a_2$. So γ_3 corresponds to the triple (a_3, b_3, c_3) with

$$a_3 = \frac{a_1a_2}{d^2}, \quad b_3 = \frac{xa_2b_1 + ya_1b_2 + z\frac{b_1b_2 + D_m}{2}}{d}.$$

4.35 Computation of the representative in G . Suppose $\gamma \in \mathbb{Q}(\sqrt{m})$ with $\text{disc}(\gamma) = D_m$ and $\Im(\gamma) > 0$. How to find $\gamma_0 \in G$ with $\gamma_0 \simeq \gamma$?

Consider the mapping $\gamma \mapsto -\frac{1}{\gamma} + n$, where $n \in \mathbb{Z}$ such that $-\frac{1}{2} < \Re(-\frac{1}{\gamma} + n) \leq \frac{1}{2}$. If γ corresponds to (a, b, c) , then $\Im(\gamma) = \frac{\sqrt{-D_m}}{2a}$ and $\Im(-\frac{1}{\gamma} + n) = \Im(-\frac{1}{\gamma}) = \frac{\sqrt{-D_m}}{2c}$. We may assume that $-\frac{1}{2} < \Re(\gamma) \leq \frac{1}{2}$. If $\gamma \notin G$, then $a > c$, or $a = c$ and $b > 0$. If $a > c$, then $\Im(\varphi(\gamma)) = \frac{\sqrt{D_m}}{2c} > \frac{\sqrt{D_m}}{2a}$. If $a = c$ and $b > 0$, then $\varphi(\gamma) \in G$. If (a_n, b_n, c_n) corresponds to $\varphi^n(a)$, then $a_{n+1} = c_n$. There has to be an n such that $\varphi^n(\gamma) \in G$, because otherwise we would have a strictly descending sequence in \mathbb{N} :

$$a > c = a_1 > c_1 = a_2 > c_2 = a_3 \cdots$$

So we have an algorithm for finding γ_0 .

The existence of a $\gamma_0 \in G$ with $\gamma_0 \simeq \gamma$ follows from Theorem 4.28. For imaginary quadratic numbers it also follows from the above algorithm.

4.36 Example. We multiply in Example 4.32 the classes of

$$\mathbb{Z}6 + \mathbb{Z}\omega \text{ and } \mathbb{Z}14 + \mathbb{Z}(-4 + \omega).$$

We have: $a_1 = 6, b_1 = 0, a_2 = 14$ and $b_2 = 8$. Then $d = \text{gcd}(6, 14, 4) = 2$. Take $x = 0, y = 1$ and $z = -1$. Then $a_3 = \frac{6 \cdot 14}{4} = 21$ and $b_3 = \frac{48 - 444}{2} = 246$. So $\gamma_3 = \frac{-123 + \sqrt{-222}}{21} \simeq \frac{3 + \sqrt{-222}}{21} \simeq -\frac{21}{3 + \sqrt{-222}} = \frac{-3 + \sqrt{-222}}{11}$. The product is represented by the ideal $\mathbb{Z}11 + \mathbb{Z}(-3 + \omega)$.

4.5 Continued fractions

This section contains the fundamentals of continued fractions. The main result is the unique representation of irrational real numbers by infinite continued fractions (Theorem 4.52).

4.37 Definition. Define rational functions

$$\langle x_1, \dots, x_n \rangle \in \mathbb{Q}(x_1, \dots, x_n)$$

for $n \in \mathbb{N}^*$ inductively by:

$$\begin{aligned} \langle x_1 \rangle &= x_1 \\ \langle x_1, x_2 \rangle &= x_1 + \frac{1}{x_2} \\ \langle x_1, \dots, x_{n+2} \rangle &= \langle x_1, \dots, x_n, \langle x_{n+1}, x_{n+2} \rangle \rangle \quad (\text{for all } n \in \mathbb{N}). \end{aligned}$$

The function $\langle x_1, \dots, x_n \rangle$ is called the *continued fraction* of length n .

4 Quadratic Number Fields

The field $\mathbb{Q}(x_1, \dots, x_n)$ of rational functions is the field of fractions of both the polynomial rings $\mathbb{Q}[x_1, \dots, x_n]$ and $\mathbb{Z}[x_1, \dots, x_n]$. The continued fractions can be written as ordinary fractions:

$$\begin{aligned}\langle x_1 \rangle &= x_1 = \frac{x_1}{1} \\ \langle x_1, x_2 \rangle &= x_1 + \frac{1}{x_2} = \frac{x_1 x_2 + 1}{x_2} \\ \langle x_1, x_2, x_3 \rangle &= x_1 + \frac{1}{x_2 + \frac{1}{x_3}} = \frac{x_1 x_2 x_3 + x_1 + x_3}{x_2 x_3 + 1}.\end{aligned}$$

We will define polynomials $p_n(x_1, \dots, x_n), q_n(x_1, \dots, x_n) \in \mathbb{Z}[x_1, \dots, x_n]$ and will prove that they can be taken as numerator and denominator of $\langle x_1, \dots, x_n \rangle$.

4.38 Definition. Define for $n \geq -1$ polynomials $p_n(x_1, \dots, x_n), q_n(x_1, \dots, x_n) \in \mathbb{Z}[x_1, \dots, x_n]$ inductively by

$$\begin{cases} p_{-1} = 0, \\ p_0 = 1, \\ p_n = x_n p_{n-1} + p_{n-2} \quad \text{for all } n \geq 1 \end{cases} \quad \text{and} \quad \begin{cases} q_{-1} = 1, \\ q_0 = 0, \\ q_n = x_n q_{n-1} + q_{n-2} \quad \text{for all } n \geq 1. \end{cases}$$

Here p_n is shorthand for $p_n(x_1, \dots, x_n)$. Analogously for q_n .

4.39 Lemma. $q_n(x_1, \dots, x_n) = p_{n-1}(x_2, \dots, x_n)$ for all $n \geq 0$.

PROOF. The terms of the sequences $(p_n)_{n \geq -1}$ and $(q_n)_{n \geq -1}$ are determined in the same way by the two preceding terms, but the 'initial values' differ. The lemma follows from $q_0 = 0$ and $q_1 = 1$. \square

4.40 Theorem. $\langle x_1, \dots, x_n \rangle = \frac{p_n(x_1, \dots, x_n)}{q_n(x_1, \dots, x_n)}$ for all $n \in \mathbb{N}^*$.

PROOF. By induction on n . Clearly $\frac{p_1}{q_1} = x_1$ and $\frac{p_2}{q_2} = x_1 + \frac{1}{x_2}$. The induction step: for $n \geq 0$ we have

$$\begin{aligned}\langle x_1, \dots, x_{n+2} \rangle &= \langle x_1, \dots, \langle x_{n+1}, x_{n+2} \rangle \rangle = \frac{p_{n+1}(x_1, \dots, x_n, \langle x_{n+1}, x_{n+2} \rangle)}{q_{n+1}(x_1, \dots, x_n, \langle x_{n+1}, x_{n+2} \rangle)} \\ &= \frac{(x_{n+1} + \frac{1}{x_{n+2}})p_n + p_{n-1}}{(x_{n+1} + \frac{1}{x_{n+2}})q_n + q_{n-1}} = \frac{p_{n+1} + \frac{1}{x_{n+2}}p_n}{q_{n+1} + \frac{1}{x_{n+2}}q_n} = \frac{p_{n+2}}{q_{n+2}} \quad \square\end{aligned}$$

4.41 Theorem. $\begin{vmatrix} p_n & p_{n+1} \\ q_n & q_{n+1} \end{vmatrix} = (-1)^n$ for all $n \geq -1$.

PROOF. By induction on n . For $n = -1$ we have

$$\begin{vmatrix} p_{-1} & p_0 \\ q_{-1} & q_0 \end{vmatrix} = \begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix} = -1 = (-1)^{-1}.$$

Furthermore, for all $n \geq -1$:

$$\begin{vmatrix} p_{n+1} & p_{n+2} \\ q_{n+1} & q_{n+2} \end{vmatrix} = \begin{vmatrix} p_{n+1} & x_{n+2}p_{n+1} + p_n \\ q_{n+1} & x_{n+2}q_{n+1} + q_n \end{vmatrix} = \begin{vmatrix} p_{n+1} & p_n \\ q_{n+1} & q_n \end{vmatrix} = - \begin{vmatrix} p_n & p_{n+1} \\ q_n & q_{n+1} \end{vmatrix}. \quad \square$$

4.42 Lemma. $\langle x_1, \dots, x_{n+1} \rangle - \langle x_1, \dots, x_n \rangle = \frac{(-1)^{n+1}}{q_n q_{n+1}}$ for all $n \in \mathbb{N}^*$.

PROOF. $\langle x_1, \dots, x_{n+1} \rangle - \langle x_1, \dots, x_n \rangle = \frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n} = \frac{(-1)^{n+1}}{q_n q_{n+1}}$. □

4.43 Proposition. $p_n = \prod_{k=1}^n \langle x_k, \dots, x_n \rangle$ for all $n \in \mathbb{N}^*$.

PROOF. By induction on n . For $n = 1$ it is clear: $p_1 = x_1 = \langle x_1 \rangle$. If $p_n = \prod_{k=1}^n \langle x_k, \dots, x_n \rangle$ for some $n \in \mathbb{N}^*$, then by Lemma 4.39 and the induction hypothesis

$$\begin{aligned} p_{n+1} &= \langle x_1, \dots, x_{n+1} \rangle q_{n+1} = \langle x_1, \dots, x_{n+1} \rangle p_n(x_2, \dots, x_{n+1}) \\ &= \langle x_1, \dots, x_{n+1} \rangle \prod_{k=2}^{n+1} \langle x_k, \dots, x_{n+1} \rangle = \prod_{k=1}^{n+1} \langle x_k, \dots, x_{n+1} \rangle. \quad \square \end{aligned}$$

Rational functions in n variables over \mathbb{Q} can be interpreted as functions on \mathbb{R}^n defined outside the zero set of their denominator. The continued fraction $\langle x_1, \dots, x_n \rangle$ determines in particular a function

$$\mathbb{R} \times \mathbb{R}^{>0} \times \dots \times \mathbb{R}^{>0} \rightarrow \mathbb{R}, \quad (a_1, \dots, a_n) \mapsto \langle a_1, \dots, a_n \rangle,$$

because $q_n(a_1, a_2, \dots, a_n) > 0$ (and so $\neq 0$) for $a_2, \dots, a_n > 0$.

4.44 Proposition. Let $r \in \mathbb{Q}$. Then there are a_1, \dots, a_n with $a_1 \in \mathbb{Z}$ and $a_2, \dots, a_n \in \mathbb{N}^*$ such that $r = \langle a_1, \dots, a_n \rangle$. The length n of this continued fraction can be chosen to be of a given parity.

PROOF. Assume $r \neq 0$. Write $r = \frac{p}{q}$ met $p \in \mathbb{Z}$, $q \in \mathbb{N}^*$, $\gcd(p, q) = 1$. Euclid's algorithm applied to p and q gives

$$\begin{array}{ll} p = a_1 q + r_1 & \text{or:} \quad \frac{p}{q} = a_1 + \frac{r_1}{q} \\ q = a_2 r_1 + r_2 & \frac{q}{r_1} = a_2 + \frac{r_2}{r_1} \\ r_1 = a_3 r_2 + r_3 & \frac{r_1}{r_2} = a_3 + \frac{r_3}{r_2} \\ \vdots & \vdots \\ r_{n-2} = a_n r_{n-1} + r_n & \frac{r_{n-2}}{r_{n-1}} = a_n \end{array}$$

4 Quadratic Number Fields

with $q > r_1 > r_2 > \cdots > r_n = 0$ and so: $\frac{p}{q} = \langle a_1, \frac{q}{r_1} \rangle = \cdots = \langle a_1, \dots, a_n \rangle$. From $r_{n-2} > r_{n-1}$ follows $a_n = \frac{r_{n-2}}{r_{n-1}} > 1$. We have $a_n = \langle a_n - 1, 1 \rangle$. So also:

$$r = \langle a_1, \dots, a_{n-1}, a_n - 1, 1 \rangle. \quad \square$$

4.45 Lemma. *Let a_1, a_2, \dots be a sequence with $a_1 \in \mathbb{Z}$ and $a_2, a_3, \dots \in \mathbb{N}^*$. Then $\lim_{n \rightarrow \infty} \langle a_1, \dots, a_n \rangle$ exists.*

PROOF. From $q_{n+1} = a_{n+1}q_n + q_{n-1}$ follows that $q_{n+1} > q_n$ for $n \geq 2$. By Lemma 4.39 $\langle a_1, \dots, a_{n+1} \rangle - \langle a_1, \dots, a_n \rangle = \frac{(-1)^{n+1}}{q_n q_{n+1}}$. These differences form a sequence with alternately positive and negative terms with absolute values descending monotone to 0 for $n \rightarrow \infty$. \square

4.46 Definition. For a sequence a_1, a_2, \dots with $a_1 \in \mathbb{Z}$ and $a_2, a_3, \dots \in \mathbb{N}^*$ we define the *infinite continued fraction* $\langle a_1, a_2, a_3, \dots \rangle$ as follows:

$$\langle a_1, a_2, a_3, \dots \rangle = \lim_{n \rightarrow \infty} \langle a_1, \dots, a_n \rangle.$$

4.47 Lemma. $\langle a_1, a_2, \dots \rangle = \langle a_1, \langle a_2, \dots \rangle \rangle$.

PROOF.

$$\begin{aligned} \langle a_1, a_2, \dots \rangle &= \lim_{n \rightarrow \infty} \langle a_1, \dots, a_n \rangle = \lim_{n \rightarrow \infty} \langle a_1, \langle a_2, \dots, a_n \rangle \rangle \\ &= \langle a_1, \lim_{n \rightarrow \infty} \langle a_2, \dots, a_n \rangle \rangle = \langle a_1, \langle a_2, \dots \rangle \rangle. \end{aligned} \quad \square$$

4.48 Lemma. $\lfloor \langle a_1, a_2, \dots \rangle \rfloor = a_1$.

PROOF. We have $\langle a_2, \dots \rangle = a_2 + \frac{1}{\langle a_3, \dots \rangle} > a_2 \geq 1$. So $\langle a_2, \dots \rangle > 1$. Therefore, $\lfloor \langle a_1, a_2, \dots \rangle \rfloor = \lfloor a_1 + \frac{1}{\langle a_2, \dots \rangle} \rfloor = a_1$. \square

4.49 Definition. A transformation φ of $\mathbb{R} \setminus \mathbb{Q}$ is defined by:

$$\varphi(x) = \frac{1}{x - \lfloor x \rfloor}.$$

4.50 Lemma. $\varphi(\langle a_1, a_2, \dots \rangle) = \langle a_2, a_3, \dots \rangle$.

PROOF. $\varphi(\langle a_1, a_2, \dots \rangle) = \frac{1}{\langle a_1, a_2, \dots \rangle - a_1} = \frac{1}{\frac{1}{\langle a_2, \dots \rangle}} = \langle a_2, a_3, \dots \rangle$. \square

4.51 Lemma. $x = \langle \lfloor x \rfloor, \lfloor \varphi(x) \rfloor, \dots, \lfloor \varphi^{n-1}(x) \rfloor, \varphi^n(x) \rangle$ for all $n \in \mathbb{N}$.

PROOF. From $\varphi(x) = \frac{1}{x - \lfloor x \rfloor}$ follows $x = \langle \lfloor x \rfloor, \varphi(x) \rangle$, so:

$$x = \langle \lfloor x \rfloor, \varphi(x) \rangle = \langle \lfloor x \rfloor, \lfloor \varphi(x) \rfloor, \varphi^2(x) \rangle = \cdots \quad \square$$

4.52 Theorem. *The following maps are inverses of each other:*

$$\left\{ \begin{array}{l} \text{sequences } a_1, a_2, a_3, \dots \\ \text{with } a_1 \in \mathbb{Z} \\ \text{and } a_2, a_3, \dots \in \mathbb{N}^* \end{array} \right\} \begin{array}{l} \longrightarrow \\ \longleftarrow \end{array} \mathbb{R} \setminus \mathbb{Q}$$

$$a_1, a_2, a_3, \dots \longmapsto \langle a_1, a_2, a_3, \dots \rangle$$

$$\lfloor x \rfloor, \lfloor \varphi(x) \rfloor, \lfloor \varphi^2(x) \rfloor, \dots \longleftarrow x$$

PROOF. For each n we have $\lfloor \varphi^n(\langle a_1, \dots \rangle) \rfloor = \lfloor \langle a_{n+1}, \dots \rangle \rfloor = a_{n+1}$. On the other hand

$$\begin{aligned} \langle \lfloor x \rfloor, \lfloor \varphi(x) \rfloor, \dots \rangle - x &= \langle \lfloor x \rfloor, \lfloor \varphi(x) \rfloor, \dots \rangle - \langle \lfloor x \rfloor, \dots, \lfloor \varphi^{n-1}(x) \rfloor, \varphi^n(x) \rangle \\ &= \lim_{n \rightarrow \infty} \langle \lfloor x \rfloor, \dots, \lfloor \varphi^{n-1}(x) \rfloor \rangle - \langle \lfloor x \rfloor, \dots, \lfloor \varphi^{n-1}(x) \rfloor, \varphi^n(x) \rangle \\ &= \lim_{n \rightarrow \infty} \frac{(-1)^n}{q_{n+1}(\lfloor x \rfloor, \dots, \lfloor \varphi^{n-1}(x) \rfloor, \varphi^n(x)) q_n(\lfloor x \rfloor, \dots, \lfloor \varphi^{n-1}(x) \rfloor)} \\ &= 0. \end{aligned} \quad \square$$

4.53 Definition. If $x = \langle a_1, a_2, \dots \rangle$ with $a_1 \in \mathbb{Z}$ and $a_2, a_3, \dots \in \mathbb{N}^*$, the sequence a_1, a_2, \dots is called the *continued fraction expansion* of x . If there is an $n > 0$ with $a_{k+n} = a_k$ for all k greater than some natural number, then the expansion is called *repeating*. The least n for which this holds is called the *period* of the repeating continued fraction expansion. If there is an $n > 0$ with $a_{k+n} = a_k$ for all $k \in \mathbb{N}$, the expansion is called *purely repeating*. Notation:

$$\langle a_1, \dots, a_k, \overline{a_{k+1}, \dots, a_{k+n}} \rangle = \langle a_1, \dots, a_k, a_{k+1}, \dots, a_{k+n}, a_{k+1}, \dots, a_{k+n}, \dots \rangle.$$

In the next section we show that it are exactly the real quadratic numbers which have repeating continued fraction expansions.

4.54 Example.

$$\begin{aligned} \sqrt{7} &= 2 + (\sqrt{7} - 2) \\ \frac{1}{\sqrt{7} - 2} &= \frac{\sqrt{7} + 2}{3} = 1 + \frac{\sqrt{7} - 1}{3} \\ \frac{3}{\sqrt{7} - 1} &= \frac{\sqrt{7} + 1}{2} = 1 + \frac{\sqrt{7} - 1}{2} \\ \frac{2}{\sqrt{7} - 1} &= \frac{\sqrt{7} + 1}{3} = 1 + \frac{\sqrt{7} - 2}{3} \\ \frac{3}{\sqrt{7} - 2} &= \sqrt{7} + 2 = 4 + (\sqrt{7} - 2) \end{aligned}$$

So $\sqrt{7} = \langle 2, \overline{1, 1, 1, 4} \rangle$.

4.6 Continued fraction expansions of real quadratic numbers

4.55 Proposition. *If $x \in \mathbb{R} \setminus \mathbb{Q}$ has a repeating continued fraction expansion, then x is a quadratic number.*

PROOF. Clearly x is quadratic if and only if $\varphi(x)$ is. So we can assume that x has a purely repeating continued fraction expansion. Set $x = \langle \overline{a_1, \dots, a_n} \rangle$. Then

$$x = \frac{p_{n+1}(a_1, \dots, a_n, x)}{q_{n+1}(a_1, \dots, a_n, x)} = \frac{xp_n(a_1, \dots, a_n) + p_{n-1}(a_1, \dots, a_{n-1})}{xq_n(a_1, \dots, a_n) + q_{n-1}(a_1, \dots, a_{n-1})}.$$

This yields a quadratic equation for x . □

4.56 Proposition. *Let $x \in \mathbb{R} \setminus \mathbb{Q}$ be quadratic. Then $\text{disc}(\varphi(x)) = \text{disc}(x)$.*

PROOF. This follows from $\text{disc}(x+1) = \text{disc}(x)$ and $\text{disc}(\frac{1}{x}) = x$. □

Let $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ be quadratic with $\text{disc}(\alpha) = D$. Then $\alpha \in \mathbb{Q}(\sqrt{D})$. The embedding of the real quadratic field in the algebra $\mathbb{R} \times \mathbb{R}$ restricts to an injective map

$$\mathbb{Q}(\sqrt{D}) \setminus \mathbb{Q} \rightarrow (\mathbb{R} \setminus \mathbb{Q}) \times (\mathbb{R} \setminus \mathbb{Q}), \quad \gamma \mapsto (\gamma, \gamma').$$

From Proposition 4.56 follows that the transformation φ of $\mathbb{R} \setminus \mathbb{Q}$ restricts to a transformation of $\mathbb{Q}(\sqrt{D}) \setminus \mathbb{Q}$ and this transformation is compatible with the transformation $(x, y) \mapsto (x - [x], y - [x]) \mapsto (\frac{1}{x-[x]}, \frac{1}{y-[x]})$ of $(\mathbb{R} \setminus \mathbb{Q}) \times (\mathbb{R} \setminus \mathbb{Q})$:

$$\begin{array}{ccc} \gamma & \xrightarrow{\quad} & (\gamma, \gamma') \\ \downarrow & & \downarrow \\ \varphi(\gamma) & \xrightarrow{\quad} & (\varphi(\gamma), \frac{1}{\gamma' - [\gamma]}) = (\varphi(\gamma), \varphi(\gamma)') \end{array}$$

4.57 Theorem. *Real quadratic numbers have repeating continued fraction expansions.*

PROOF. Let γ be a real quadratic number and put $\text{disc}(\gamma) = D$. Then $\gamma \in \mathbb{Q}(\sqrt{D})$. Consider the embedding $\mathbb{Q}(\sqrt{D}) \rightarrow \mathbb{R} \times \mathbb{R}$, $\alpha \mapsto (\alpha, \alpha')$. The images of

$$\gamma, \varphi(\gamma), \varphi^2(\gamma), \dots$$

under the embedding in $\mathbb{R} \setminus \mathbb{Q} \times \mathbb{R} \setminus \mathbb{Q}$ are

$$(\gamma, \gamma'), (\varphi(\gamma), \varphi(\gamma)'), (\varphi^2(\gamma), \varphi^2(\gamma)'), \dots$$

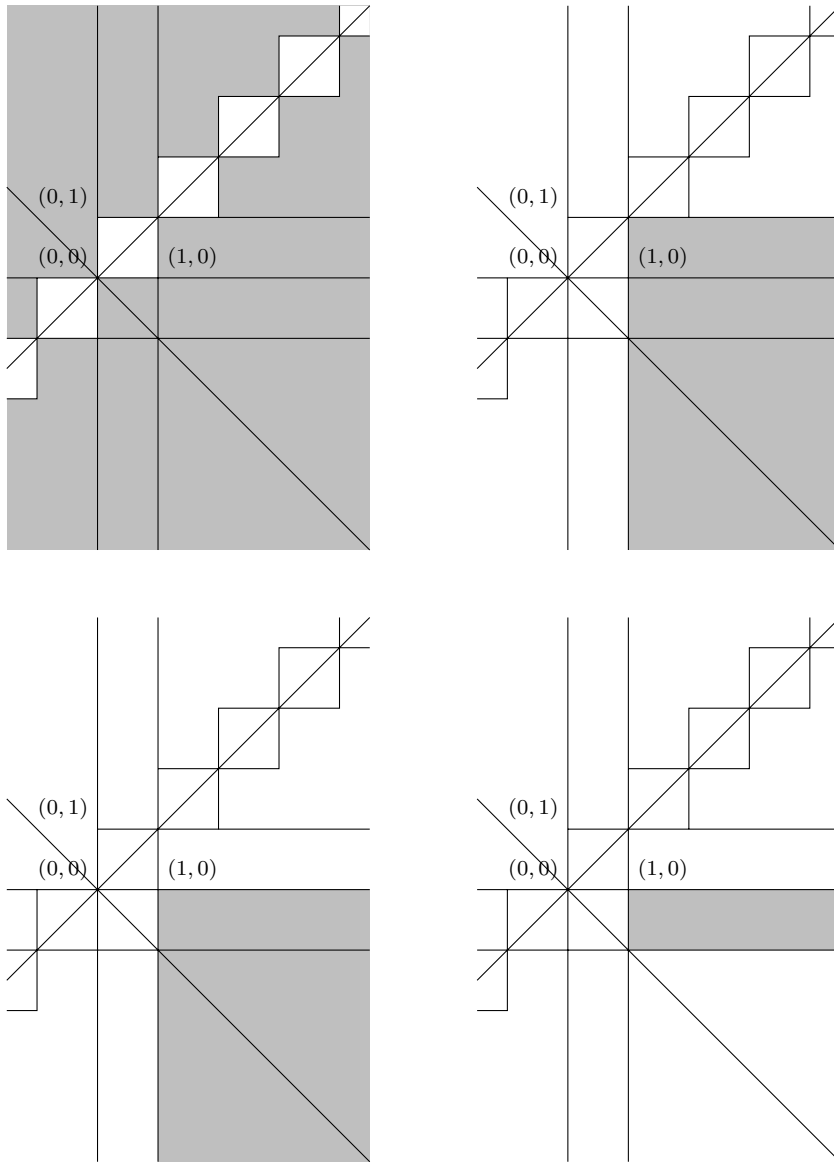


Figure 4.4: The course of points in $(\mathbb{R} \setminus \mathbb{Q})^2$ outside $\{(x, y) \mid [x] = [y]\}$ under φ

4 Quadratic Number Fields

If all elements of this sequence were in the domain $\{(x, y) \mid [x] = [y]\}$, then

$$[\varphi^n(\gamma)] = [\varphi^n(\gamma)'] \quad \text{for all } n \in \mathbb{N}.$$

From

$$\begin{aligned} \gamma &= \langle [\gamma], [\varphi(\gamma)], \dots, [\varphi^{n-1}(\gamma)], \varphi^n(\gamma) \rangle, \\ \gamma' &= \langle [\gamma], [\varphi(\gamma)], \dots, [\varphi^{n-1}(\gamma)], \varphi^n(\gamma)' \rangle, \\ \gamma' &= \langle [\gamma'], [\varphi(\gamma')], \dots, [\varphi^{n-1}(\gamma')], \varphi^n(\gamma') \rangle. \end{aligned}$$

it then follows by induction on n that $\varphi^n(\gamma') = \varphi^n(\gamma)'$. So the numbers γ and γ' would have equal continued fraction expansions. By Theorem 4.52 these numbers are equal. However, $\gamma' \neq \gamma$. So there is an n such that $[\varphi^n(\gamma)] \neq [\varphi^n(\gamma)']$. As indicated in Figure 4.4, we have for all $k \geq n + 3$

$$\varphi^k(\gamma) > 1 \quad \text{and} \quad -1 < \varphi^k(\gamma)' < 0.$$

Equivalently $[\varphi^k(\gamma)] \geq 1$ and $[\varphi^k(\gamma)'] = -1$. The domain

$$\{(x, y) \mid x > 1, -1 < y < 0\}$$

contains only finitely many (γ, γ') met $\text{disc}(\gamma) = D$: suppose the triple (a, b, c) corresponds to such a γ , then $\frac{c}{a} = \gamma\gamma' < 0$ and there are only finitely many triples (a, b, c) such that $b^2 + a(-c) = D$ and $c < 0$. It follows that for a quadratic number γ the sequence $[\gamma], [\varphi(\gamma)], [\varphi^2(\gamma)], \dots$ repeats. \square

4.58 Definition. A real quadratic number γ is called *reduced* if $\gamma > 1$ and $-1 < \gamma' < 0$.

4.59 Theorem. A real quadratic number is reduced if and only if its continued fraction expansion is purely repeating.

PROOF. First we show that the restriction of $(x, y) \mapsto (\frac{1}{x-[x]}, \frac{1}{y-[y]})$ to the domain $\{(x, y) \mid x > 1, -1 < y < 0\}$ is injective.

Suppose (x_1, y_1) and (x_2, y_2) are in this domain, $x_1 - [x_1] = x_2 - [x_2]$ and $y_1 - [y_1] = y_2 - [y_2]$. The inequalities $-1 < y_1, y_2 < 0$ imply $[y_1] = [y_2]$ and so also $x_1 = x_2$ and $y_1 = y_2$.

Let Γ be the set of reduced real quadratic numbers of discriminant D . The restriction of φ to the finite set Γ is injective. So it is a permutation of Γ . \square

4.60 Theorem. If γ is a reduced real quadratic number, then so is $-\frac{1}{\gamma'}$. If $\gamma = \langle \overline{a_1, \dots, a_n} \rangle$, then $-\frac{1}{\gamma'} = \langle \overline{a_n, \dots, a_1} \rangle$.

PROOF. We have (where $\gamma_n = \varphi^{n-1}(\gamma)$):

$$\begin{array}{ll} \gamma = \gamma_1 = a_1 + \frac{1}{\gamma_2} & -\frac{1}{\gamma'_2} = a_1 + (-\gamma'_1) \\ \gamma_2 = a_2 + \frac{1}{\gamma_3} & \text{and so} \quad -\frac{1}{\gamma'_3} = a_2 + (-\gamma'_2) \\ \vdots & \vdots \\ \gamma_n = a_n + \frac{1}{\gamma_1} & -\frac{1}{\gamma'_1} = -\frac{1}{\gamma'_1} = a_n + (-\gamma'_n). \quad \square \end{array}$$

For square roots we have in particular:

4.61 Proposition. *Let $d \in \mathbb{N}^*$ be not a square. Then*

$$\sqrt{d} = \langle a_1, \overline{a_2, \dots, a_n, a_{n+1}} \rangle$$

with a_2, \dots, a_n symmetric ($a_2 = a_n, a_3 = a_{n-1}, \dots$) and $a_{n+1} = 2a_1$.

PROOF. Put $a_1 = \lfloor \sqrt{d} \rfloor$. Then $\sqrt{d} + a_1$ is reduced and so it has a purely repeating continued fraction expansion:

$$\sqrt{d} + a_1 = \langle 2a_1, \overline{a_2, \dots, a_n} \rangle$$

and then

$$\sqrt{d} = \langle a_1, \overline{a_2, \dots, a_n, 2a_1} \rangle.$$

We have

$$\frac{-1}{(\sqrt{d} + a_1)'} = \frac{1}{\sqrt{d} - a_1} = \langle \overline{a_n, a_{n-1}, \dots, a_2, 2a_1} \rangle.$$

Hence also

$$\sqrt{d} = a_1 + \frac{1}{\langle \overline{a_n, a_{n-1}, \dots, a_2, 2a_1} \rangle} = \langle a_1, \overline{a_n, a_{n-1}, \dots, a_2, 2a_1} \rangle.$$

The proposition follows from the uniqueness of continued fraction expansions. \square

4.62 Definition. $x, y \in \mathbb{R} \setminus \mathbb{Q}$ are called *tail equivalent* if their continued fraction expansions have equal tails, notation: $x \sim_\varphi y$. So:

$$x \sim_\varphi y \iff \text{there are } k, n \in \mathbb{N} \text{ such that } \varphi^k(x) = \varphi^n(y).$$

4.63 Proposition. *Let $x \in \mathbb{R} \setminus \mathbb{Q}$ with $x > 1$ and let $\begin{pmatrix} p & r \\ q & s \end{pmatrix} \in \text{GL}_2(\mathbb{Z})$ with $q > s > 0$. Then for $y = \begin{pmatrix} p & q \\ r & s \end{pmatrix} x$ there is an $n \in \mathbb{N}^*$ such that $\varphi^n(y) = x$.*

4 Quadratic Number Fields

PROOF. Put $\frac{p}{q} = \langle a_1, \dots, a_n \rangle$ with $a_1 \in \mathbb{Z}$ and $a_2, \dots, a_n \in \mathbb{N}^*$ such that

$$\begin{vmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{vmatrix} = \begin{vmatrix} p & r \\ q & s \end{vmatrix}.$$

(Use Proposition 4.44.) Then

$$\frac{p}{q} = \frac{p_n(a_1, \dots, a_n)}{q_n(a_1, \dots, a_n)}$$

and so $p = p_n$ and $q = q_n$. From $pq_{n-1} - qp_{n-1} = ps - qr$ follows that $q \mid p(q_{n-1} - s)$ and so $q \mid q_{n-1} - s$. However, $|q_{n-1} - s| < q$, so $q_{n-1} = s$. And also $p_{n-1} = r$. We then have

$$\begin{pmatrix} p & r \\ q & s \end{pmatrix} x = \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} x = \frac{p_n x + p_{n-1}}{q_n x + q_{n-1}} = \langle a_1, \dots, a_n, x \rangle.$$

So the numbers $p_n, p_{n-1}, q_n, q_{n-1}$ are those from the continued fraction expansion of $(\frac{p}{q} \frac{r}{s})x$. Furthermore, we have $\varphi^n((\frac{p}{q} \frac{r}{s})x) = \varphi^n(\langle a_1, \dots, a_n, x \rangle) = x$. \square

4.64 Theorem. For all $x, y \in \mathbb{R} \setminus \mathbb{Q}$ we have:

$$x \simeq y \iff x \sim_\varphi y.$$

PROOF.

\Leftarrow : It suffices to show that $x \simeq \varphi(x)$. We have

$$\varphi(x) = \frac{1}{x - [x]} = \begin{pmatrix} 0 & 1 \\ 1 & -[x] \end{pmatrix} x.$$

So $x \simeq \varphi(x)$.

\Rightarrow : Now suppose that $x \simeq y$. Say $y = (\frac{a}{b} \frac{c}{d})x$. For $n \in \mathbb{N}$ we have

$$x = \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} \varphi^n(x).$$

So

$$y = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} \varphi^n(x) = \begin{pmatrix} ap_n + cq_n & ap_{n-1} + cq_{n-1} \\ bp_n + dq_n & bp_{n-1} + dq_{n-1} \end{pmatrix} \varphi^n(x).$$

We have $|x - \frac{p_n}{q_n}| < \frac{1}{q_n^2}$, that is

$$p_n = q_n x + \frac{\delta_n}{q_n}, \quad \text{where } |\delta_n| < 1.$$

4.7 Algorithm for the ideal class group of a real quadratic number field

We assume that $bx + d > 0$. (If necessary take $\begin{pmatrix} -a & -c \\ -b & -d \end{pmatrix}$). We have:

$$bp_n + dq_n = (bx + d)q_n + \frac{b\delta_n}{q_n} \rightarrow \infty \quad \text{if } n \rightarrow \infty.$$

Take n so large that $bp_{n-1} + dq_{n-1} > 0$. Furthermore,

$$bp_n + dq_n - (bp_{n-1} + dq_{n-1}) = (bx + d)(q_n - q_{n-1}) + \frac{b\delta_n}{q_n} - \frac{b\delta_{n-1}}{q_{n-1}} \rightarrow \infty$$

if $n \rightarrow \infty$. So there is an n with

$$bp_{n-1} + dq_{n-1} > 0$$

and, moreover, $bp_n + dq_n > bp_{n-1} + dq_{n-1}$. By Proposition 4.63 there is a $k \in \mathbb{N}$ such that $\varphi^k(y) = \varphi^n(x)$. So $x \sim_\varphi y$. \square

4.7 Algorithm for the ideal class group of a real quadratic number field

Let $m > 1$. In section 4.2 we constructed a bijection from $\mathcal{C}(\mathbb{Q}(\sqrt{m}))$ to

$$\{\gamma \in \mathbb{Q}(\sqrt{m}) \setminus \mathbb{Q} \mid \text{disc}(\gamma) = D_m\} / \simeq.$$

From section 4.6 it follows that this is mapped bijectively to Γ_m / \sim_φ , where

$$\Gamma_m = \{\gamma \in \mathbb{Q}(\sqrt{m}) \setminus \mathbb{Q} \mid \text{disc}(\gamma) = D_m \text{ and } \gamma \text{ reduced}\}.$$

Since the restriction of φ to Γ_m is a permutation, the ideal classes of $\mathbb{Z}[\omega_m]$ correspond to orbits of this permutation.

Let $\gamma \in \Gamma_m$ correspond to the triple (a, b, c) , then

$$0 < b + \sqrt{D_m} < 2a < -b + \sqrt{D_m}$$

and so $0 < -b < \sqrt{D_m}$. It follows that $2a < 2\sqrt{D_m}$, that is $a < \sqrt{D_m}$. From $-4ac = D_m - b^2 \leq D_m$ follows that $a < \frac{1}{2}\sqrt{D_m}$ or $-c < \frac{1}{2}\sqrt{D_m}$. So in the class or in the inverse class of an ideal \mathfrak{a} there is an ideal with norm $\leq \frac{1}{2}\sqrt{D_m}$. Since $N\mathfrak{a}' = N\mathfrak{a}$, each class contains such an ideal. This λ for real quadratic number fields is the same as the bound which will follow from Theorem 5.17, see also Examples 5.12.

4.65 Example. We compute all reduced real quadratic numbers of discriminant $4 \cdot 130$. Let $\gamma \in \Gamma_{130}$ correspond to the triple (a, b, c) . Then

$$\gamma = \frac{-b + \sqrt{4 \cdot 130}}{2a} = \frac{-\frac{b}{2} + \sqrt{130}}{a}.$$

$$130 - \left(\frac{b}{2}\right)^2:$$

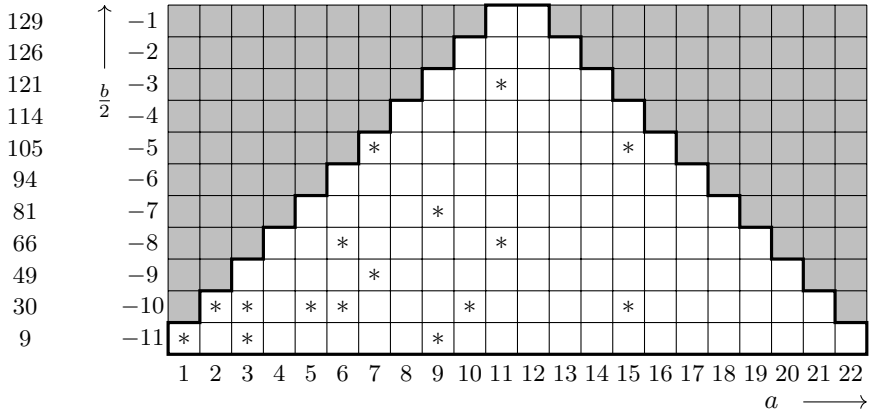


Figure 4.5: Computation of the reduced real quadratic numbers of discriminant $4 \cdot 130$

So γ is reduced if

$$0 < \sqrt{130} + \frac{b}{2} < a < \sqrt{130} - \frac{b}{2}.$$

$\lfloor \sqrt{130} \rfloor = 11$, so $-11 \leq \frac{b}{2} < 0$. The reduced real quadratic numbers of discriminant $4 \cdot 130$ are (where $\omega = \sqrt{130}$):

$$\begin{array}{llll} \frac{\omega + 11}{\omega + 11} & \frac{\omega + 11}{\omega + 10} & \frac{\omega + 7}{\omega + 10} & \text{(orbit of length 3)} \\ \frac{\omega + 11}{\omega + 10} & \frac{9}{\omega + 10} & \frac{9}{\omega + 10} & \text{(orbit of length 3)} \\ \frac{\omega + 3}{\omega + 10} & \frac{10}{\omega + 10} & \frac{3}{\omega + 5} & \frac{\omega + 9}{\omega + 5} \quad \frac{\omega + 5}{\omega + 5} \text{ (orbit of length 5)} \\ \frac{\omega + 2}{\omega + 10} & \frac{15}{\omega + 10} & \frac{7}{\omega + 8} & \frac{\omega + 9}{\omega + 3} \quad \frac{\omega + 5}{\omega + 8} \text{ (orbit of length 5)} \\ \frac{\omega + 2}{5} & \frac{15}{6} & \frac{7}{11} & \frac{\omega + 9}{11} \quad \frac{\omega + 5}{6} \end{array}$$

See Figure 4.5. So a system of representatives of $\Gamma_{130}/\sim_{\varphi}$ consists of the numbers:

$$\begin{array}{ll} \omega + 11 = \langle \overline{22, 2, 2} \rangle, & \frac{\omega + 11}{3} = \langle \overline{7, 2, 7} \rangle, \\ \frac{\omega + 10}{2} = \langle \overline{10, 1, 2, 2, 1} \rangle, & \frac{\omega + 10}{5} = \langle \overline{4, 3, 1, 1, 3} \rangle. \end{array}$$

4.7 Algorithm for the ideal class group of a real quadratic number field

$$36 - \frac{b-1}{2} \cdot \frac{b+1}{2}:$$

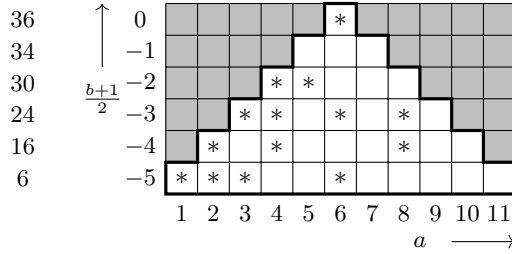


Figure 4.6: Computation of the reduced real quadratic numbers of discriminant 145

The ideal class group is of order 4. The elements are represented by the ideals

$$\begin{aligned} \mathbb{Z} + \mathbb{Z}(\omega + 11) & (= \mathbb{Z} + \mathbb{Z}\omega), \\ \mathbb{Z}3 + \mathbb{Z}(\omega + 11) & (= \mathbb{Z}3 + \mathbb{Z}(\omega - 1)) \quad \text{or} \quad \mathbb{Z}10 + \mathbb{Z}(\omega + 10) \quad (= \mathbb{Z}10 + \mathbb{Z}\omega), \\ \mathbb{Z}2 + \mathbb{Z}(\omega + 10) & (= \mathbb{Z}2 + \mathbb{Z}\omega), \\ \mathbb{Z}5 + \mathbb{Z}(\omega + 10) & (= \mathbb{Z}5 + \mathbb{Z}\omega). \end{aligned}$$

The map $\gamma \mapsto \gamma'$ corresponds to inversion in $\mathcal{O}(\mathbb{Q}(\sqrt{130}))$, and since $-\frac{1}{\gamma'} \simeq \gamma'$, the same holds for $\gamma \mapsto -\frac{1}{\gamma}$. This last map is a permutation of order 2 of Γ_m . This permutation induces the trivial permutation of the set of four orbits. Hence every element of $\mathcal{O}(\mathbb{Q}(\sqrt{130}))$ is its own inverse. So the group $\mathcal{O}(\mathbb{Q}(\sqrt{130}))$ is the Klein fourgroup.

4.66 Example. We compute all reduced real quadratic numbers of discriminant 145. Let $\gamma \in \Gamma_{145}$ correspond to the triple (a, b, c) . Then

$$\gamma = \frac{-b + \sqrt{145}}{2a} = \frac{-\frac{b+1}{2} + \frac{1+\sqrt{145}}{2}}{a}.$$

So γ is reduced if

$$0 < \frac{1 + \sqrt{145}}{2} + \frac{b-1}{2} < a < \frac{1 + \sqrt{145}}{2} - \frac{b+1}{2}.$$

4 Quadratic Number Fields

$\lfloor \frac{1+\sqrt{145}}{2} \rfloor = 6$, so $-6 \leq \frac{b-1}{2} < 0$. The reduced real quadratic numbers of discriminant 145 are (where $\omega = \omega_{145} = \frac{1+\sqrt{145}}{2}$):

$$\begin{array}{llll} \frac{\omega}{6} & \omega + 5 & \frac{\omega + 5}{\omega + 4} & \text{(orbit of length 3)} \\ \frac{\omega + 3}{\omega + 3} & \frac{\omega + 5}{\omega + 5} & \frac{\omega + 5}{\omega + 4} & \text{(orbit of length 3)} \\ \frac{3}{\omega + 3} & \frac{2}{\omega + 4} & \frac{8}{\omega + 5} & \text{(orbit of length 3)} \\ \frac{8}{\omega + 2} & \frac{2}{\omega + 2} & \frac{3}{\omega + 3} & \text{(orbit of length 5).} \\ \frac{5}{5} & \frac{6}{6} & \frac{4}{4} & \frac{\omega + 2}{4} \quad \frac{\omega + 3}{6} \end{array}$$

See Figure 4.6.

So a system of representatives of $\Gamma_{145}/\sim_{\varphi}$ consists of the numbers:

$$\begin{array}{ll} \omega + 5 = \langle \overline{11, 1, 1} \rangle, & \frac{\omega + 5}{2} = \langle \overline{5, 1, 3} \rangle, \\ \frac{\omega + 4}{2} = \langle \overline{5, 3, 1} \rangle, & \frac{\omega + 2}{4} = \langle \overline{2, 1, 1, 2} \rangle. \end{array}$$

The ideal class group is of order 4. The elements are represented by the ideals

$$\begin{array}{ll} \mathbb{Z} + \mathbb{Z}(\omega + 5) & (= \mathbb{Z} + \mathbb{Z}\omega), \\ \mathbb{Z}2 + \mathbb{Z}(\omega + 5) & (= \mathbb{Z}2 + \mathbb{Z}(\omega + 1)), \\ \mathbb{Z}2 + \mathbb{Z}(\omega + 4) & (= \mathbb{Z}2 + \mathbb{Z}\omega), \\ \mathbb{Z}4 + \mathbb{Z}(\omega + 2). & \end{array}$$

The map $\gamma \mapsto -\frac{1}{\gamma}$ leaves invariant only two of the four orbits of φ in Γ_{145} . So the group $\mathcal{C}(\mathbb{Q}(\sqrt{145}))$ is cyclic of order 4.

4.8 Algorithm for the fundamental unit of a real quadratic number field

4.67 Terminology. Let φ be a permutation of a finite set X , $\{x_1, \dots, x_n\}$ an orbit of φ of length n , $\varphi(x_i) = x_{i+1}$ for $i = 1, \dots, n-1$ and $\varphi(x_n) = x_1$. This is summarized as: (x_1, \dots, x_n) is an orbit of the permutation φ . Note that for $n > 1$ this means that $(x_1 \cdots x_n)$ is an n -cycle in the decomposition of φ as a product of disjoint cycles.

In this section the squarefree integer m is greater than 1. Orbits of the permutation induced by φ on Γ_m give rise to a nontrivial unit of $\mathbb{Z}[\omega_m]$:

4.68 Theorem. *Let $(\gamma_1, \dots, \gamma_n)$ be an orbit of the permutation φ of Γ_m . Then $\gamma_1\gamma_2 \cdots \gamma_n \in \mathbb{Z}[\omega_m]^*$ and $\gamma_1\gamma_2 \cdots \gamma_n > 1$.*

4.8 Algorithm for the fundamental unit of a real quadratic number field

PROOF. From $\gamma_i \in \Gamma_m$ follows that $\gamma_i > 1$ and so $\gamma_1 \cdots \gamma_n > 1$. We will prove that $\gamma_1 \cdots \gamma_n \in \mathbb{Z}[\omega_m]^*$ in two ways.

1. $\mathbb{Z} + \mathbb{Z}\gamma_1 = \mathbb{Z} + \mathbb{Z}([\gamma_1] + \frac{1}{\gamma_2}) = \mathbb{Z} + \mathbb{Z}\frac{1}{\gamma_2}$, so $\gamma_2(\mathbb{Z} + \mathbb{Z}\gamma_1) = \mathbb{Z} + \mathbb{Z}\gamma_2$. Continuing this way we obtain

$$\gamma_1\gamma_n\gamma_{n-1} \cdots \gamma_2(\mathbb{Z} + \mathbb{Z}\gamma_1) = \mathbb{Z} + \mathbb{Z}\gamma_1.$$

Proposition 1.12 implies that $\gamma_1 \cdots \gamma_n, (\gamma_1 \cdots \gamma_n)^{-1} \in \mathbb{Z}[\omega_m]$.

2. Let $\gamma_1 = \langle a_1, \dots, a_n, \gamma_1 \rangle$. Then

$$\begin{aligned} q_{n+1}(a_1, \dots, a_n, \gamma_1) &= p_n(a_2, \dots, a_n, \gamma_1) \\ &= \left(\prod_{k=2}^n \langle a_k, \dots, a_n, \gamma_1 \rangle \right) \cdot \gamma_1 = \gamma_1 \cdots \gamma_n. \end{aligned}$$

On the other hand $q_{n+1}(a_1, \dots, a_n, \gamma_1) = q_n\gamma_1 + q_{n-1}$ and $\gamma_1 = \frac{p_n\gamma_1 + p_{n-1}}{q_n\gamma_1 + q_{n-1}}$. So γ_1 satisfies $q_n\gamma_1^2 + (q_{n-1} - p_n)\gamma_1 - p_{n-1} = 0$ and, therefore, γ_1 corresponds to a triple (a, b, c) with $a \mid q_n$. We have $\mathbb{Z} + \mathbb{Z}a\gamma_1 = \mathbb{Z}[\omega_m]$, so $q_n\gamma_1 + q_{n-1} \in \mathbb{Z}[\omega_m]$, that is $\gamma_1 \cdots \gamma_n \in \mathbb{Z}[\omega_m]$. Similarly, $(-\frac{1}{\gamma_1}) \cdots (-\frac{1}{\gamma_n}) \in \mathbb{Z}[\omega_m]$ and so $\frac{1}{\gamma_1 \cdots \gamma_n} \in \mathbb{Z}[\omega_m]$. \square

Extra in the second proof is the identity $q_{n+1}(a_1, \dots, a_n, \gamma_1) = \gamma_1 \cdots \gamma_n$, so the continued fraction expansion of γ_1 , one of the elements in the orbit, can be used for the computation of $\gamma_1 \cdots \gamma_n$.

As remarked in Example 1.24 the existence of a unit > 1 in a real quadratic number field implies that the field has a fundamental unit. We now show that this fundamental unit is the product of the elements in any of the orbits.

4.69 Theorem. *Let $(\gamma_1, \dots, \gamma_n)$ be an orbit of the permutation φ of Γ_m and put $\varepsilon = \gamma_1 \cdots \gamma_n$. Then for each $\nu \in \mathbb{Z}[\omega_m]^*$ with $\nu > 1$ there exists an $l \in \mathbb{N}^*$ such that $\nu = \varepsilon^l$.*

PROOF. Let $\gamma = \gamma_1$ correspond to the triple (a, b, c) . Then $\mathbb{Z} + \mathbb{Z}a\gamma = \mathbb{Z}[\omega_m]$ and also $\mathbb{Z} + \mathbb{Z}a\gamma' = \mathbb{Z}[\omega_m]$. Put $\nu = p - q\gamma'$. Then $p, q \in \mathbb{Z}$ and $a \mid q$. From $\nu - \nu' > 0$ and $\nu - (-\nu') > 0$ follows that $p, q \in \mathbb{N}^*$. Put

$$A = \begin{pmatrix} p & -qN(\gamma) \\ q & p - q\text{Tr}(\gamma) \end{pmatrix},$$

where N and Tr stand for $N_{\mathbb{Q}}^{\mathbb{Q}(\sqrt{m})}$ and $\text{Tr}_{\mathbb{Q}}^{\mathbb{Q}(\sqrt{m})}$ respectively. Then $A \in M_2(\mathbb{Z})$, because $N(\gamma) = \frac{c}{a}$, $\text{Tr}(\gamma) = -\frac{b}{a}$ and $a \mid q$. Moreover,

$$\det A = p^2 - pq\text{Tr}(\gamma) + q^2N(\gamma) = N(p - q\gamma) = \pm 1.$$

4 Quadratic Number Fields

So $A \in \text{GL}_2(\mathbb{Z})$. We have $A\gamma = \frac{p\gamma - qN(\gamma)}{q\gamma + (p - q\text{Tr}(\gamma))} = \gamma$, because

$$\gamma(q\gamma + p - q\text{Tr}(\gamma)) - p\gamma + qN(\gamma) = q(\gamma^2 - \text{Tr}(\gamma)\gamma + N(\gamma)) = 0.$$

We will show that there is a $k \in \mathbb{N}^*$ such that

$$A = \begin{pmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{pmatrix},$$

where the p_k etc. come from the continued fraction expansion of γ .

We have $p - q\text{Tr}(\gamma) = p - q\gamma - q\gamma' = \nu' + q(-\gamma')$. Since $\nu\nu' = \pm 1$ and $\nu > 1$ we have $|\nu'| < 1$; moreover, $0 < -\gamma' < 1$. So $-1 < p - q\text{Tr}(\gamma) < q + 1$, that is $0 \leq p - q\text{Tr}(\gamma) \leq q$. We distinguish three cases.

1. $0 < p - q\text{Tr}(\gamma) < q$. Then Proposition 4.63 applies.

2. $0 = p - q\text{Tr}(\gamma)$. From $\begin{vmatrix} p & -qN(\gamma) \\ q & 0 \end{vmatrix} = \pm 1$, $q > 0$ and $N(\gamma) < 0$ Follows that $q = 1$ and $N(\gamma) = -1$. Then $\gamma = \begin{pmatrix} p & 1 \\ 1 & 0 \end{pmatrix} \gamma$ and so $\gamma = \langle p, \gamma \rangle = \langle \bar{p} \rangle$. In this case

$$A = \begin{pmatrix} p_1 & p_0 \\ q_1 & q_0 \end{pmatrix}.$$

3. $p - q\text{Tr}(\gamma) = q$. From $\begin{vmatrix} p & -qN(\gamma) \\ q & q \end{vmatrix} = \pm 1$ follows that $q = 1$ and $N(\gamma) = -(p \pm 1)$. If $N(\gamma) = -(p + 1)$, then $\gamma = p + \frac{1}{\gamma+1}$ and so $\gamma' = p + \frac{1}{\gamma'+1}$, contradictory to $-1 < \gamma' < 0$. So $N(\gamma) = -(p - 1)$, and then $\gamma = p - 1 + \frac{1}{\gamma+1} = \langle p - 1, 1, \gamma \rangle = \langle \overline{p-1}, 1 \rangle$. In this case

$$A = \begin{pmatrix} p_2 & p_1 \\ q_2 & q_1 \end{pmatrix}.$$

So in each case there is a $k \in \mathbb{N}^*$ such that $A = \begin{pmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{pmatrix}$. And so $\gamma = \varphi^k(\gamma)$, which implies $n \mid k$, say $k = ln$. We have $\gamma = \langle a_1, \dots, a_k, \varphi^k(\gamma) \rangle$ with $a_i = \lfloor \varphi^{i-1}(\gamma) \rfloor$ and so

$$\begin{aligned} \pm 1 &= \begin{vmatrix} p_k & p_{k+1}(a_1, \dots, a_k, \gamma) \\ q_k & q_{k+1}(a_1, \dots, a_k, \gamma) \end{vmatrix} = \begin{vmatrix} p_k - \gamma q_k & 0 \\ q_k & q_{k+1}(a_1, \dots, a_k, \gamma) \end{vmatrix} \\ &= \varepsilon^l \cdot q_{k+1}(a_1, \dots, a_k, \gamma). \end{aligned}$$

Hence $q_{k+1}(a_1, \dots, a_k, \gamma) = \nu$ (since $\nu > 0$) and, therefore, $\nu = p_k(a_2, \dots, a_k, \gamma) = \varphi(\gamma) \cdots \varphi^k(\gamma) = \varepsilon^l$. \square

4.70 Corollary. *Let $(\gamma_1, \dots, \gamma_n)$ be an orbit of the permutation φ of Γ_m . Then $\gamma_1 \cdots \gamma_n$ is the fundamental unit of $\mathbb{Q}(\sqrt{m})$.* \square

From $\varepsilon = \gamma_1 \cdots \gamma_n$ and $N(\gamma_i) < 0$ follows that $N(\varepsilon) = (-1)^n$. So either all orbits of φ are of even length or all are of odd length depending on the sign of $N(\varepsilon)$.

4.71 Examples. In Example 4.65 we had two orbits of length 3 and two of length 5. Using the remark following the proof of Theorem 4.68: $\sqrt{130} + 11 = \langle 22, 2, 2, \sqrt{130} + 11 \rangle$, so

$$5(\sqrt{130} + 11) + 2 = 57 + 5\sqrt{130}.$$

is the fundamental unit of $\mathbb{Q}(\sqrt{130})$.

Similarly, the fundamental unit of $\mathbb{Q}(\sqrt{145})$ (Example 4.66) is

$$2(2\omega_{145} + 5) + 1 = 3\omega_{145} + 11 = \frac{25 + 3\sqrt{145}}{2}.$$

For m squarefree and > 1 units of the real quadratic number field $\mathbb{Q}(\sqrt{m})$ correspond to solutions of the Pell equation $x^2 - my^2 = \pm 1$ for $m \equiv 2, 3 \pmod{4}$ and to solutions of $x^2 - my^2 = \pm 4$ for $m \equiv 1 \pmod{4}$. As indicated in exercise 3 of chapter 1, the fundamental unit can be found in principle by looking for the least $y \in \mathbb{N}$ for which $my^2 \pm 1$, respectively $my^2 \pm 4$, is a square, say x^2 . Then the fundamental unit is $x + y\sqrt{m}$, respectively $\frac{x}{2} + \frac{y}{2}\sqrt{m}$. The algorithm described in this section of course is by far better. It was already known in India in the 12th century. Bhāscarāchārya (1114–1185) found for example the least solution of $x^2 - 109y^2 = 1$, namely $y = 15\,140\,424\,455\,100$.

4.9 The 2-rank of the ideal class group

A finite abelian group is isomorphic to a product $C_{d_1} \times C_{d_2} \times \cdots \times C_{d_k}$ of cyclic groups of orders d_1, \dots, d_k . A classification of finite abelian groups is obtained by requiring that $d_{i+1} \mid d_i$ for $i = 1, \dots, k-1$ and $d_k \neq 1$. The d_1, \dots, d_k are called the *group invariants* of the finite abelian group. The 2-rank of a finite abelian group is the number of even group invariants. If r is the 2-rank of a finite abelian group A , then 2^r is the order of the subgroup ${}_2A$ of A of elements of order ≤ 2 and also of the factor group A/A^2 . In this section a formula for the 2-rank of the ideal class group of a quadratic number field is derived. We do this separately for the imaginary and the real case.

Imaginary quadratic number fields

The transformation $\mathfrak{a} \mapsto \mathfrak{a}'$ of $\mathbb{I}^+(\mathbb{Q}(\sqrt{m}))$ induces inversion in the ideal class group and corresponds to the transformation

$$\gamma \mapsto \begin{cases} -\bar{\gamma} & \text{if } |\gamma| > 1 \text{ and } \Re(\gamma) < \frac{1}{2}, \\ \gamma & \text{if } |\gamma| = 1 \text{ or } \Re(\gamma) = \frac{1}{2} \end{cases}$$

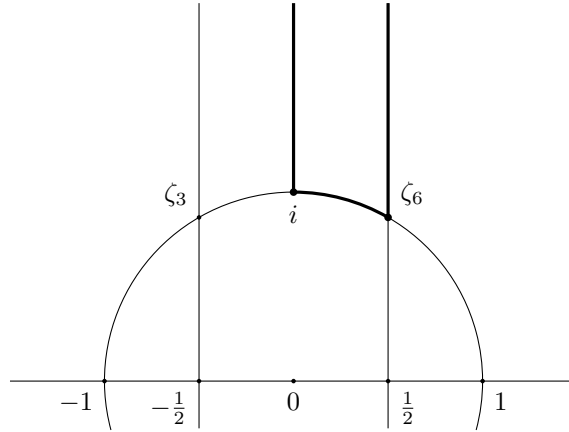


Figure 4.7: Location of the elements of G which correspond to elements of $\mathcal{C}(\mathbb{Q}(\sqrt{m}))$ of order 1 or 2




of $G \cap \{\gamma \in \mathbb{Q}(\sqrt{m}) \mid \text{disc}(\gamma) = D_m\}$. The elements of order 1 or 2 in $\mathcal{C}(\mathbb{Q}(\sqrt{m}))$ correspond to the numbers γ of discriminant D_m on the curve indicated in Figure 4.7. They correspond to triples $(a, b, c) \in V_m$ with $b = 0$ or $a = c$ or $a = -b$.



4.72 Example. In Example 4.32 the elements of order 1 or 2 are the classes represented by $\mathbb{Z} + \mathbb{Z}\omega$ (order 1), $\mathbb{Z}2 + \mathbb{Z}\omega$, $\mathbb{Z}3 + \mathbb{Z}\omega$ and $\mathbb{Z}6 + \mathbb{Z}\omega$. So the group invariants of the ideal class group are: 6, 2.

4.73 Theorem.

$$\text{rk}_2(\mathcal{C}(\mathbb{Q}(\sqrt{m}))) = r(D_m) - 1,$$

where $r(n)$ denotes the number of prime divisors of an $n \in \mathbb{Z}$.

PROOF. See Figure 4.8. Under the action of $\text{SL}_2(\mathbb{Z})$  corresponds to  etc. So the number of elements γ with $\text{disc}(\gamma) = D_m$ on  equals half of:

the number of elements on  plus the number of elements on .

First we compute the number of (a, b, c) with $a > 0$, $b^2 - 4ac = D_m$ and $b = 0$.

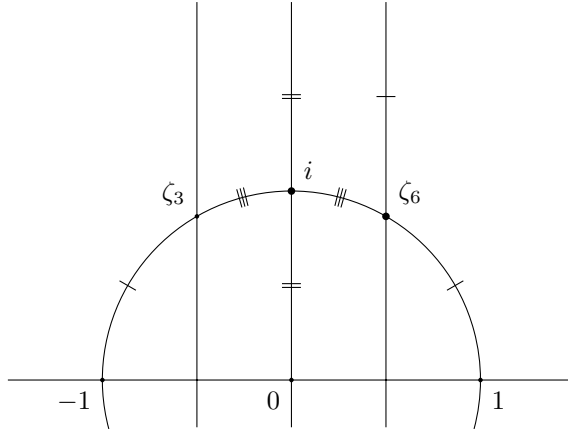


Figure 4.8: See the proof of Theorem 4.73

- For $m \equiv 1 \pmod{4}$ we have $D_m = m$ and in this case there are no a, c with $4ac = -m$.
- For $m \equiv 2, 3 \pmod{4}$ we have $ac = -m$ and then the number equals the number of divisors of $-m$, and this equals $2^{r(m)}$, because m is squarefree.

Next the number of (a, b, c) with $a > 0$, $b^2 - 4ac = D_m$ and $a = c$.

- For $m \equiv 1 \pmod{4}$: the number of (a, b) with $a > 0$ and $(2a-b)(2a+b) = -m$. This is the number of divisors of $-m$.
- For $m \equiv 2, 3 \pmod{4}$: the number of (a, b_0) with $a > 0$ and $(a-b_0)(a+b_0) = -m$. (We took $b_0 = 2b$.) This number is $2^{r(m)}$ if m is odd and 0 if m is even.

So, depending on $m \pmod{4}$, the number of elements of ${}_2\mathcal{C}(\mathbb{Q}(\sqrt{m}))$ is in the last column of the following scheme:

$m \pmod{4}$	# with $b = 0$	# with $c = a$	$\frac{1}{2} \times \text{total}$
1	0	$2^{r(m)}$	$2^{r(m)-1}$
2	$2^{r(m)}$	0	$2^{r(m)-1}$
3	$2^{r(m)}$	$2^{r(m)}$	$2^{r(m)}$

It can be summarized to $\text{rk}_2(\mathcal{C}(\mathbb{Q}(\sqrt{m}))) = r(D_m) - 1$. □

So the group $\mathcal{C}(\mathbb{Q}(\sqrt{m}))$ is of odd order (for $m < 0$) if and only if $r(D_m) = 1$. This is the case if $m = -1$, $m = -2$ or $m = -p$ (p a prime $\equiv 3 \pmod{4}$). If p is a prime $\equiv 7 \pmod{8}$, then 2 splits completely in $\mathbb{Q}(\sqrt{-p})$, and for $p > 7$ the prime ideal above 2 represent nontrivial elements of $\mathcal{C}(\mathbb{Q}(\sqrt{-p}))$: they correspond to the triples $(2, \pm 1, \frac{p \pm 1}{8})$. So: if $\mathcal{C}(\mathbb{Q}(\sqrt{m}))$ is trivial, then $m = -1$, $m = -2$, $m = -7$

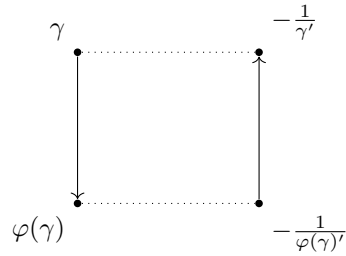
4 Quadratic Number Fields

or $m = -p$, where p is a prime $\equiv 3 \pmod{8}$. One easily verifies that $\mathcal{A}(\mathbb{Q}(\sqrt{m}))$ is trivial for $m = -3$, $m = -11$, $m = -19$, $m = -43$, $m = -67$ and $m = -163$. In 1966 it was independently shown by A. Baker and H. Stark that there are no other imaginary quadratic number fields with a trivial ideal class group.

Real quadratic number fields

The permutation $\gamma \mapsto -\frac{1}{\gamma'}$ of Γ_m corresponds to inversion in $\mathcal{A}(\mathbb{Q}(\sqrt{m}))$ and induces a permutation of the set of orbits of φ in Γ_m . If $\gamma = \langle \overline{a_1, \dots, a_n} \rangle$, then $\varphi(\gamma) = \langle \overline{a_2, \dots, a_n, a_1} \rangle$, $-\frac{1}{\varphi(\gamma)'}$ is $\langle \overline{a_1, a_n, \dots, a_2} \rangle$. Hence

$$\varphi\left(-\frac{1}{\varphi(\gamma)'}\right) = -\frac{1}{\gamma'}, \quad \text{or in a diagram:}$$



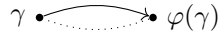
The elements of ${}_2\mathcal{A}(\mathbb{Q}(\sqrt{m}))$ correspond to orbits in Γ_m of the action of φ which under $\gamma \mapsto -\frac{1}{\gamma'}$ map to themselves. In these orbits we have elements of the following types:

Type A



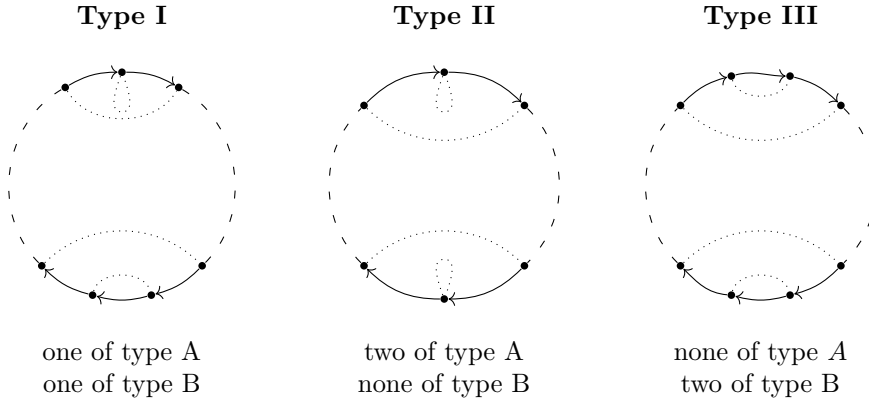
$$N(\gamma) = -1$$

Type B



$$\text{Tr}(\gamma) = [\gamma]$$

In case an orbit consists of just one element, this element is both of type A and of type B. In all other orbits there are exactly two elements of one of these types. We distinguish three types of orbits which under $\gamma \mapsto -\frac{1}{\gamma'}$ map to themselves:



An orbit of length 1 is of type I. We will count the number of elements of type A and the number of type B. The sum of these numbers equals twice the number of orbits of type I, II or III. Before doing so we first take a look at the role of the fundamental unit.

The element $\omega_m - [\omega'_m] - 1$ is of type B and is in the orbit corresponding to the trivial element of $\mathcal{C}(\mathbb{Q}(\sqrt{m}))$. Put

$$\Gamma_m^0 = \{ \gamma \in \Gamma_m \mid \gamma \simeq \omega_m - [\omega'_m] - 1 \}$$

This is the set of elements in the ‘trivial’ orbit. So we have:

$$N(\varepsilon) = -1 \iff \Gamma_m^0 \text{ contains an element of type A.}$$

On the other hand we have:

4.74 Lemma. *There is an element of type A if and only if m (and then also D_m) is a sum of two squares.*

PROOF. Suppose γ is of type A, and suppose γ corresponds to the triple (a, b, c) . Then $N(\gamma) = \frac{c}{a} = -1$, and so $D_m = b^2 + (2a)^2$. Conversely, suppose D_m equals $b^2 + (2a)^2$ with $b < 0$ and $a > 0$. Then take $\gamma = \frac{-b + \sqrt{D_m}}{2a}$. □

4.75 Theorem. *If $N(\varepsilon) = -1$, then $m = p_1 \dots p_r$ or $m = 2p_1 \dots p_r$, where p_1, \dots, p_r are different primes $\equiv 1 \pmod{4}$.*

PROOF. Suppose $N(\varepsilon) = -1$. Then Γ_m^0 contains an element of type A and so m is a sum of two squares. Because m is squarefree, the theorem follows. □

So the norm of the fundamental unit equals -1 if and only if the trivial orbit contains an element of type A. It may happen that an element of type A exists, but outside the trivial orbit. For example 34 is the sum of two squares and so there is an element of type A in Γ_{34} . The fundamental unit is of norm 1, so the element of type A is not in the trivial orbit. In this case the trivial orbit is of length 4 and is of type III. There is another orbit and this one is of length 6 and of type II.

4 Quadratic Number Fields

First we determine the number of elements of type A.

4.76 Definition. Let $n \in \mathbb{N}^*$. We define $E(n)$ as a fourth of the number of ways n is the sum of two squares. More precisely:

$$E(n) = \frac{1}{4} \cdot \#\{(x, y) \in \mathbb{Z}^2 \mid x^2 + y^2 = n\}.$$

4.77 Lemma. $E(n) = \#\{\mathfrak{a} \mid \mathfrak{a} \text{ is an ideal of } \mathbb{Z}[i] \text{ with } N(\mathfrak{a}) = n\}$.

PROOF.

$$\begin{aligned} E(n) &= \frac{1}{4} \cdot \#\{(x, y) \in \mathbb{Z}^2 \mid x^2 + y^2 = n\} = \frac{1}{4} \cdot \#\{\alpha \in \mathbb{Z}[i] \mid N(\alpha) = n\} \\ &= \#\{\mathfrak{a} \mid \mathfrak{a} \text{ is an ideal of } \mathbb{Z}[i] \text{ with } N(\mathfrak{a}) = n\}. \quad \square \end{aligned}$$

The splitting behavior of primes in $\mathbb{Z}[i]$ implies that for p a prime number and $r \in \mathbb{N}^*$ we have

$$E(p^r) = \begin{cases} 1 & \text{if } p = 2, \\ 1 & \text{if } p \equiv 3 \pmod{4} \text{ and } r \text{ is even,} \\ 0 & \text{if } p \equiv 3 \pmod{4} \text{ and } r \text{ is odd,} \\ r + 1 & \text{if } p \equiv 1 \pmod{4}, \end{cases}$$

and $E(n) = \prod_{p|n} E(p^{v_p(n)})$ for $n \in \mathbb{N}^*$.

4.78 Proposition. Let m be the sum of two squares. Then the number of elements of Γ_m of type A equals $2^{r(m)-1}$.

PROOF.

$$\begin{aligned} &\#\{\gamma \in \Gamma_m \mid N(\gamma) = -1\} \\ &= \#\{\gamma \in \mathbb{Q}(\sqrt{m}) \setminus \mathbb{Q} \mid \gamma > 1, \text{disc}(\gamma) = D_m, N(\gamma) = -1\} \\ &= \#\{(a, b, c) \in \mathbb{Z}^3 \mid a > 0, b^2 - 4ac = D_m, b < 0 \text{ and } c = -a\} \\ &= \#\{(a, b) \in \mathbb{N}^{*2} \mid (2a)^2 + b^2 = D_m\} \end{aligned}$$

For $m \equiv 1 \pmod{4}$ this number equals

$$\frac{1}{2}E(m) = \frac{1}{2} \prod_{p|m} E(p) = \frac{1}{2} \cdot 2^{r(m)} = 2^{r(m)-1}$$

and for $m \equiv 2 \pmod{4}$

$$E(m) = 2^{r(m)-1}. \quad \square$$

For the computation of the number of elements γ of type B we distinguish two kinds of elements:

Type B1: $[\gamma]$ is even, **Type B2:** $[\gamma]$ is odd.

4.79 Lemma. *The number of elements of type B1 equals*

$$\begin{cases} 0 & \text{if } m \equiv 1 \pmod{4}, \\ 2^{r(m)-1} & \text{if } m \equiv 2, 3 \pmod{4}. \end{cases}$$

PROOF. Let γ be of type B1 and let it correspond to the triple (a, b, c) . Then

$$[\gamma] = \text{Tr}(\gamma) = -\frac{b}{a}.$$

It follows that $2a \mid b$. From $b^2 - 4ac = D_m$ follows that $4a \mid D_m$. For $m \equiv 1 \pmod{4}$ this is not possible. Now we assume that $m \equiv 2, 3 \pmod{4}$. Then $a \mid m$. If conversely $a \in \mathbb{N}^*$ is a divisor of m , then for

$$\alpha = \frac{\sqrt{m}}{a}$$

we have $\text{disc}(\alpha) = 4m$. Every γ corresponding to a triple $(a, *, *)$ such that $\text{Tr}(\gamma) \in 2\mathbb{Z}$ and $\gamma > \gamma'$ equals $n + \alpha$ for some $n \in \mathbb{N}^*$. If we require that $\text{Tr}(\gamma) = [\gamma]$, then γ is unique: it is $[\alpha] + \alpha$. Finally there is the condition $\gamma > 1$. We have $[\gamma] = 2 \cdot [\alpha]$. Hence:

$$\gamma > 1 \iff [\gamma] \geq 1 \iff [\alpha] \geq \frac{1}{2} \iff [\alpha] \geq 1 \iff \alpha > 1 \iff m > a^2.$$

Because m is not a square, the number of divisors a of m with $a^2 < m$ is half the total number of divisors. So the number of elements of type B1 equals $2^{r(m)-1}$. \square

4.80 Lemma. *The number of elements of type B2 equals*

$$\begin{cases} 0 & \text{if } m \equiv 2 \pmod{4}, \\ 2^{r(m)-1} & \text{if } m \equiv 1, 3 \pmod{4}. \end{cases}$$

PROOF. Let γ be of type B2 and let it correspond to the triple (a, b, c) . From

$$[\gamma] = \text{Tr}(\gamma) = -\frac{b}{a}$$

follows that $a \mid b$. We distinguish two cases.

First case: $m \equiv 1 \pmod{4}$. From $b^2 - 4ac = m$ follows that $a \mid m$. Conversely, if $a \mid m$, then

$$\alpha = \frac{a + \sqrt{m}}{2a}$$

4 Quadratic Number Fields

has discriminant m . Every γ of discriminant m corresponding to a triple $(a, *, *)$ satisfying $\text{Tr}(\gamma) \in \mathbb{Z}$ and $\gamma > \gamma'$ equals $n + \alpha$ for some $n \in \mathbb{N}^*$. If, moreover, $\text{Tr}(\gamma) = \lfloor \gamma \rfloor$, then $\gamma = \lfloor \alpha \rfloor - 1 + \alpha$. So the number of elements γ satisfying these conditions equals the number of (positive) divisors of m , being $2^{r(m)}$. The condition $\gamma > 1$ will be considered further on.

Second case: $m \equiv 2, 3 \pmod{4}$. From $b^2 - 4ac = 4m$ follows that b is even. Because $\frac{b}{a}$ is odd, a is even. So $(\frac{b}{2})^2 - 2 \cdot \frac{a}{2}c = m$ with $\frac{a}{2}, \frac{b}{2} \in \mathbb{Z}$. Since $\frac{b}{a}$ is odd, $\frac{a}{2}$ and $\frac{b}{2}$ have the same parity. It follows that $m \equiv 2 \pmod{4}$ is not possible. Now we assume that $m \equiv 3 \pmod{4}$. We have $\frac{a}{2} \mid m$. Conversely, suppose $d \mid m$. Put $a = 2d$. The argument goes as in the case $m \equiv 1 \pmod{4}$, now using

$$\alpha = \frac{d + \sqrt{m}}{a}.$$

The number of elements γ of discriminant $4m$ satisfying $\text{Tr}(\gamma) = \lfloor \gamma \rfloor$ and $\gamma > \gamma'$ equals $2^{r(m)}$.

In both cases we have $\alpha = \frac{a + \sqrt{D_m}}{2a}$ and $\gamma = \lfloor \alpha \rfloor - 1 + \alpha$, and so $\lfloor \gamma \rfloor = 2\lfloor \alpha \rfloor - 1$. So

$$\gamma > 1 \iff \lfloor \gamma \rfloor \geq 1 \iff \lfloor \alpha \rfloor \geq 1 \iff \alpha > 1 \iff D_m > a^2.$$

For $m \equiv 1 \pmod{4}$ the number of elements of type B2 equals the number of divisors a of m with $m > a^2$, and for $m \equiv 3 \pmod{4}$ the number of even divisors d of m with $4m > (2d)^2$, that is $m > d^2$. In both cases this number is $2^{r(m)-1}$. \square

Summarizing,

$m \pmod{4}$	sum of 2 squares	type A	type B1	type B2	$\frac{1}{2} \times \text{total}$
1	yes	$2^{r(m)-1}$	0	$2^{r(m)-1}$	$2^{r(m)-1}$
1	no	0	0	$2^{r(m)-1}$	$2^{r(m)-2}$
2	yes	$2^{r(m)-1}$	$2^{r(m)-1}$	0	$2^{r(m)-1}$
2	no	0	$2^{r(m)-1}$	0	$2^{r(m)-2}$
3	no	0	$2^{r(m)-1}$	$2^{r(m)-1}$	$2^{r(m)-1}$

So in particular:

4.81 Theorem. *Let m be squarefree > 1 . Then*

$$\text{rk}_2(\mathcal{C}(\mathbb{Q}(\sqrt{m}))) = \begin{cases} r(D_m) - 1 & \text{if } m \text{ is the sum of two squares,} \\ r(D_m) - 2 & \text{if } m \text{ is not the sum of two squares.} \end{cases} \quad \square$$

4.82 Corollary. *Let $m > 1$ be squarefree. Then $\#(\mathcal{C}(\mathbb{Q}(\sqrt{m})))$ is odd if and only if m is either a prime or a product of two primes $\not\equiv 1 \pmod{4}$.* \square

It is unknown whether there are infinitely many m such that $\mathbb{Z}[\omega_m]$ is a principal ideal domain.

For another, more advanced, computation of the 2-rank of the ideal class group see exercises 8 and 9 of chapter 12. In chapter 15 this 2-rank will be computed using class field theory. This computation is far less technical than the computation in this section, thus showing the strength of class field theory (Example 15.30).

EXERCISES

- Let $m, n \in \mathbb{Z}$ be different, squarefree and $\neq 1$. Put $k = \frac{mn}{\gcd(m, n)^2}$.
 - Let p be a prime number which splits completely in both $\mathbb{Q}(\sqrt{m})$ and $\mathbb{Q}(\sqrt{n})$. Show that p splits completely in $\mathbb{Q}(\sqrt{k})$ as well.
 - Let p be a prime number which remains prime in both $\mathbb{Q}(\sqrt{m})$ and $\mathbb{Q}(\sqrt{n})$. What is its splitting behavior in $\mathbb{Q}(\sqrt{k})$?
 - Let p be a prime number which ramifies in both $\mathbb{Q}(\sqrt{m})$ and $\mathbb{Q}(\sqrt{n})$. Show, by giving examples, what the splitting behavior of p in $\mathbb{Q}(\sqrt{k})$ could be.
- Verify whether 255 is a quadratic residue modulo the prime number 1151.
 - Is $\overline{41}$ a square in $\mathbb{Z}/(225)$?
 - What is the splitting behavior of the prime number 10007 in $\mathbb{Q}(\sqrt{7429})$?
- For which prime numbers p is 5 a quadratic residue modulo p ? And for which p is 7 a quadratic residue modulo p ?
- Describe the splitting behavior of prime numbers in $\mathbb{Q}(\sqrt{-15})$ and compute the ideal class group of this field.
- Let $m \in \mathbb{Z}$ be squarefree $\neq 1$ and p a prime number which splits completely in $\mathbb{Q}(\sqrt{m})$. Let q be a prime number satisfying $q \equiv -p \pmod{|D_m|}$. Show that q splits completely in $\mathbb{Q}(\sqrt{m})$ if $m > 1$ and that q remains prime if $m < 0$.
- Show that the group $\mathrm{GL}_2(\mathbb{Z})$ is generated by the matrices $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$. Also show that the first two generate the subgroup $\mathrm{SL}_2(\mathbb{Z})$ of matrices of determinant 1. Use that \mathbb{Z} is Euclidean and also the identity $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$.
- In the exercises 9 and 13 of chapter 2 the ideal class groups of $\mathbb{Q}(\sqrt{-6})$ and $\mathbb{Q}(\sqrt{-23})$ have been computed. Compute them now using the algorithm described in section 4.4.
- Compute, using the algorithm in section 4.4, the ideal class group of $\mathbb{Q}(\sqrt{-34})$, giving for each ideal class a representative. Show that the group is cyclic.
- Let $m \in \mathbb{Z}$ be squarefree $\neq 1$. Prove that the quadratic number field $\mathbb{Q}(\sqrt{m})$ is a subfield of the cyclotomic field $\mathbb{Q}(\zeta_N)$, where $N = |D_m|$.

4 Quadratic Number Fields

10. Compute the elements of $\mathcal{C}(\mathbb{Q}(\sqrt{-185}))$.
 - (i) Determine the 2-rank of this group.
 - (ii) Determine the group structure.
 - (iii) Determine the order of $[\mathfrak{p}]$, where \mathfrak{p} is a prime ideal above 3.
11. (i) Compute the ideal class group of $\mathbb{Q}(\sqrt{-41})$. Show that this group is cyclic. Which element is of order 2?
 - (ii) Determine the prime ideal factorization of the ideals $(2 - \sqrt{-41})$, $(3 + \sqrt{-41})$, $(2 - \sqrt{-41}, 3 + \sqrt{-41})$ and $(2 - \sqrt{-41}) \cap (3 + \sqrt{-41})$ of $\mathbb{Z}[\sqrt{-41}]$.
 - (iii) Which elements of the ideal class group of $\mathbb{Q}(\sqrt{-41})$ are of order 4?
12. In Example 4.32 the ideal class group of $\mathbb{Q}(\sqrt{-222})$ has been computed.
 - (i) Determine the prime ideal factorization of the principal ideals $(11 + \sqrt{-222})$ and $(3 + \sqrt{-222})$.
 - (ii) Which of the classes in $\mathcal{C}(\mathbb{Q}(\sqrt{-222}))$ are squares in this group?
13. Let $n \in \mathbb{N}^*$. Determine the continued fraction expansion of $\sqrt{n^2 + 1}$.
14. Let m and n be natural numbers. Compute $\langle n, \overline{m, 2n} \rangle$.
15. (i) Prove that $p_n(x_1, \dots, x_n) = p_n(x_n, \dots, x_1)$.
 - (ii) Let $x = \langle a_1, \overline{a_2, \dots, a_n} \rangle$, where $(a_2, \dots, a_{n-1}) = (a_{n-1}, \dots, a_2)$ and $a_n = 2a_1$. Prove using (i) that $x^2 \in \mathbb{Q}$. Show that this also follows from Theorem 4.60.
16. Determine all reduced quadratic numbers with discriminant 20.
17. Show that the ring of integers of $\mathbb{Q}(\sqrt{7})$ is a principal ideal domain. Compute also the narrow ideal class group of this field. (The *narrow ideal class group* of a real quadratic number field K is the group $\mathbb{I}(K)/\mathbb{P}^+(K)$, where $\mathbb{P}^+(K)$ is the group of principal fractional ideals generated by an $\alpha \in K$ with $N_{\mathbb{Q}}^K(\alpha) > 0$.)
18. (i) Compute the ideal class groups of the fields $\mathbb{Q}(\sqrt{79})$ and $\mathbb{Q}(\sqrt{111})$.
 - (ii) Compute the fundamental units of these fields.
 - (iii) Compute the narrow ideal class groups of these fields. (See exercise 17.)
19. (i) Compute $\mathcal{C}(\mathbb{Q}(\sqrt{58}))$.
 - (ii) Let \mathfrak{a} be an ideal of $\mathbb{Z}[\sqrt{58}]$ which is not a principal ideal. Show that there is an $\alpha \in \mathfrak{a}$ such that $|N_{\mathbb{Q}}^K(\alpha)| = 2 \cdot N(\mathfrak{a})$.
 - (iii) Which primes do ramify in $\mathbb{Q}(\sqrt{58})$? The ideal of $\mathbb{Z}[\sqrt{58}]$ generated by such a prime is the square of a prime ideal. Is this prime ideal principal?
 - (iv) Compute the fundamental unit of $\mathbb{Q}(\sqrt{58})$.

5 Geometric Methods

In chapter 1 we embedded a number field of degree n in a real n -dimensional vector space $\mathbb{R}^r \times \mathbb{C}^s$. For imaginary and real quadratic number fields we considered in the chapters 1 and 4 the images in \mathbb{C} , respectively \mathbb{R}^2 , of their rings of integers. These images are lattices in the 2-dimensional vector space. As was shown by Minkowski, this approach leads to results, both computationally and theoretically, for number fields in general.

The standard inner product on \mathbb{R}^n determines a metric on \mathbb{R}^n . Together with this metric \mathbb{R}^n is the n -dimensional Euclidean space, here also denoted by \mathbb{R}^n . The standard Lebesgue measure on this Euclidean space is denoted by vol . It is a translation invariant metric (a Haar-measure) on \mathbb{R}^n . Lattices in subspaces of \mathbb{R}^n can be characterized as discrete subgroups of the additive metric group \mathbb{R}^n (section 5.1). Minkowski theory (section 5.2) is about the existence of nonzero lattice elements in a measurable subset of \mathbb{R}^n . In a few occasions we will need to compute $\text{vol}(E)$ for some simple Lebesgue measurable subsets E .

In chapter 3 a bound λ , depending on the number field, was found such that every ideal class of that number field contains an ideal of norm less than λ . In section 5.3, as an application of Minkowski theory, a much sharper bound is obtained, the Minkowski bound. Minkowski theory is also applied in section 5.4 in a proof of Dirichlet's theorem, a description of the structure of the group of units. The group of units determines a positive real number, the regulator of the field. This number will come up again in the chapters 9 and 13, where complex analytic methods will be used. The regulator is defined in the last section.

5.1 Discrete subgroups of \mathbb{R}^n

5.1 Definition. A subgroup Γ of the additive group \mathbb{R}^n is called *discrete* if the standard topology of \mathbb{R}^n induces the discrete topology on Γ .

Later, in section 19.2 we will consider topological groups. Here the emphasis is on the additive group \mathbb{R}^n with its standard topology.

We will show that the discrete subgroups of \mathbb{R}^n are lattices in linear subspaces of \mathbb{R}^n .

5.2 Definition and notation. Let Λ be lattice in \mathbb{R}^n . For a given \mathbb{Z} -basis (x_1, \dots, x_n) of Λ the subset

$$F = \left\{ \sum_{i=1}^n t_i x_i \mid 0 \leq t_i < 1 \text{ for } i = 1, \dots, n \right\}$$

of \mathbb{R}^n is called a *fundamental parallelootope* or a *mesh* of the lattice Λ . From Lemma 1.40 it follows easily that the volume of F is independent of the choice of the basis of Λ . We denote this volume by $\delta(\Lambda)$.

5.3 Proposition. Let Γ be a subgroup of the additive group \mathbb{R}^n . Then the following are equivalent:

- a) Γ is discrete.
- b) For all bounded subsets B of \mathbb{R}^n the set $B \cap \Gamma$ is finite.
- c) Γ is a lattice in an \mathbb{R} -linear subspace of \mathbb{R}^n .

PROOF.

a) \Rightarrow b): Let B be a bounded set of \mathbb{R}^n . Then its closure \overline{B} is compact. Since Γ is closed in \mathbb{R}^n , the subset $\overline{B} \cap \Gamma$ is both discrete and compact, which implies that it is finite.

b) \Rightarrow c): Lattices in subspaces of \mathbb{R}^n have rank $\leq n$. Choose one in Γ of maximal rank. Say it is $\Lambda = \mathbb{Z}v_1 + \dots + \mathbb{Z}v_m$, where (v_1, \dots, v_m) is \mathbb{R} -independent. Then $\Gamma \subseteq \mathbb{R}v_1 + \dots + \mathbb{R}v_m$: for each $v \in \Gamma$ the collection (v, v_1, \dots, v_m) is \mathbb{R} -dependent by the maximality of Λ . We will show that Γ is a lattice in $\mathbb{R}v_1 + \dots + \mathbb{R}v_m$. Let F be a mesh of Λ . Then every coset of Λ in Γ is represented by an element of F . Since F is bounded, the set $\Gamma \cap F$ is finite. It follows that Γ/Λ is finite, say of order r . Then $r\Gamma \subseteq \Lambda$. We have $\Lambda \subseteq \Gamma \subseteq \frac{1}{r}\Lambda$. Since Γ is sandwiched between two lattices in the subspace $\mathbb{R}v_1 + \dots + \mathbb{R}v_m$, it is itself a lattice in that subspace.

c) \Rightarrow a): Let Γ be a lattice in an m -dimensional subspace W of \mathbb{R}^n . Then $\Gamma = \mathbb{Z}v_1 + \dots + \mathbb{Z}v_m$, where (v_1, \dots, v_m) is a basis of W . Extend (v_1, \dots, v_m) to a basis (v_1, \dots, v_n) of \mathbb{R}^n . Then for each $v \in \Gamma$

$$B_v = \{ v + t_1 v_1 + \dots + t_n v_n \mid -1 < t_i < 1 \text{ for } i = 1, \dots, n \}$$

is an open neighborhood of v such that $B_v \cap \Gamma = \{v\}$. □

5.2 Minkowski theory

5.4 Proposition (Minkowski). *Let Λ be a lattice in \mathbb{R}^n and E a measurable subset of \mathbb{R}^n with $\text{vol}(E) > \delta(\Lambda)$. Then there exist $u, v \in E$ such that $u \neq v$ and $u - v \in \Lambda$.*

PROOF. Let F be a mesh of Λ . Then \mathbb{R}^n is the disjoint union of all $x + F$ with $x \in \Lambda$ and so E is the disjoint union of all $(x + F) \cap E$ with $x \in \Lambda$ and for the volume we have:

$$\text{vol}(E) = \sum_{x \in \Lambda} \text{vol}((x + F) \cap E) = \sum_{x \in \Lambda} \text{vol}(F \cap (-x + E)).$$

Because $\text{vol}(E) > \text{vol}(F)$, the subsets $F \cap (-x + E)$ of F are not all disjoint of each other, so there are $x, y \in \Lambda$ with $x \neq y$ such that $(F \cap (-x + E)) \cap (F \cap (-y + E)) \neq \emptyset$. Say w is an element of this intersection. Take $u = x + w$ and $v = y + w$, then $u, v \in E$, $u \neq v$ and $u - v = x - y \in \Lambda$. \square

5.5 Definition. A subset E of \mathbb{R}^n is called *convex* if for all $x, y \in E$ and all $t \in [0, 1]$ also $tx + (1-t)y \in E$. The subset E is called *symmetric* if for all $x \in E$ also $-x \in E$.

Crucial for this chapter is *Minkowski's Lattice Point Theorem*:

5.6 Theorem (Minkowski). *Let Λ be a lattice in \mathbb{R}^n and let E be a convex, symmetric, measurable subset of \mathbb{R}^n such that*

$$\text{vol}(E) > 2^n \delta(\Lambda).$$

Then E contains a nonzero element of Λ . If, furthermore, E is compact then the condition $\text{vol}(E) \geq 2^n \delta(\Lambda)$ suffices.

PROOF. Since $\text{vol}(\frac{1}{2}E) = \frac{1}{2^n} \text{vol}(E) > \delta(\Lambda)$, it follows from Proposition 5.4 that there are $u, v \in \frac{1}{2}E$ such that $u \neq v$ and $u - v \in \Lambda$. By symmetry $-v \in \frac{1}{2}E$ and by convexity $\frac{1}{2}u + \frac{1}{2}(-v) \in \frac{1}{2}E$. So $u - v \in E$ and $u - v \in \Lambda \setminus \{0\}$.

In case E is compact and $\text{vol}(E) \geq 2^n \delta(\Lambda)$: apply the above to $(1 + \frac{1}{m})E$ for $m = 1, 2, \dots$. There is a nonzero $x_m \in (1 + \frac{1}{m})E \cap \Lambda$ for all m . The sequence (x_m) is contained in $2E \cap \Lambda$, which by Proposition 5.3 is a finite set. It follows that there is an i such that $x_i \in (1 + \frac{1}{m})E$ for infinitely many m . For this i we have $x_i \in E$. \square

5.3 The Minkowski bound

In this section K is a number field of degree n . The ring of integers \mathcal{O}_K is a lattice in the \mathbb{Q} -vector space K (Corollary 1.39). In section 1.1 we embedded K into the \mathbb{R} -algebra $\mathbb{R}^r \times \mathbb{C}^s$, which is a real vector space of dimension $n = r + 2s$:

$$\iota: K \rightarrow \mathbb{R}^r \times \mathbb{C}^s, \quad \alpha \mapsto (\sigma_1(\alpha), \dots, \sigma_r(\alpha), \tau_1(\alpha), \dots, \tau_s(\alpha)),$$

where $\sigma_1, \dots, \sigma_r: K \rightarrow \mathbb{R}$ are the real embeddings of K and τ_1, \dots, τ_s are (half of) the complex embeddings of K . Via $z \mapsto (\Re z, \Im z)$ we identify this embedding with an embedding in \mathbb{R}^n :

$$\iota: K \rightarrow \mathbb{R}^n, \quad \alpha \mapsto (\sigma_1(\alpha), \dots, \sigma_r(\alpha), \Re(\tau_1(\alpha)), \Im(\tau_1(\alpha)), \dots, \Re(\tau_s(\alpha)), \Im(\tau_s(\alpha))).$$

The image of \mathcal{O}_K under ι is a lattice in \mathbb{R}^n and we will denote this image by Λ_K .

5.7 Proposition. $\delta(\Lambda_K) = \frac{1}{2^s} \sqrt{|\text{disc}(K)|}$.

PROOF. Let $\alpha_1, \dots, \alpha_n$ be an integral basis of K . Then the lattice Λ_K is spanned by $\iota(\alpha_1), \dots, \iota(\alpha_n)$. The number $\delta(\Lambda_K)$ is equal to the absolute value of the determinant of the $n \times n$ -matrix having as i -th row

$$\sigma_1(\alpha_i), \dots, \sigma_r(\alpha_i), \Re(\tau_1(\alpha_i)), \Im(\tau_1(\alpha_i)), \dots, \Re(\tau_s(\alpha_i)), \Im(\tau_s(\alpha_i))$$

The effect on the determinant of replacing columns

$$\begin{pmatrix} \Re(\tau_1(\alpha_1)) \\ \vdots \\ \Re(\tau_1(\alpha_n)) \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} \Im(\tau_1(\alpha_1)) \\ \vdots \\ \Im(\tau_1(\alpha_n)) \end{pmatrix}$$

by

$$\begin{pmatrix} \tau_1(\alpha_1) \\ \vdots \\ \tau_1(\alpha_n) \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} \overline{\tau_1(\alpha_1)} \\ \vdots \\ \overline{\tau_1(\alpha_n)} \end{pmatrix}.$$

is a multiplication by $(2i)^s$. By Proposition 1.28 the square of the determinant of the matrix thus obtained equals $\text{disc}(K)$. \square

For an ideal $\mathfrak{a} \neq 0$ the image $\Lambda_{\mathfrak{a}} := \iota(\mathfrak{a})$ is a lattice in \mathbb{R}^n and since $(\Lambda_K : \Lambda_{\mathfrak{a}}) = (\mathcal{O}_K : \mathfrak{a}) = N(\mathfrak{a})$ we have:

5.8 Corollary. *Let \mathfrak{a} be a nonzero ideal of \mathcal{O}_K . Then*

$$\delta(\Lambda_{\mathfrak{a}}) = \frac{1}{2^s} \sqrt{|\text{disc}(K)|} \cdot N(\mathfrak{a}). \quad \square$$

In section 3.3 it was shown that the ideal class group of a number field is finite. The main ingredient of the proof is the existence of a λ such that every nonzero ideal \mathfrak{a} of \mathcal{O}_K contains a nonzero element α such that $|\mathbf{N}_{\mathbb{Q}}^K(\alpha)| \leq \lambda N(\mathfrak{a})$. For computations it is worthwhile to have a small λ with this property. We will apply Minkowski's Lattice Point Theorem.

5.9 Proposition. *Let A be a compact, convex, symmetric, measurable subset of $\mathbb{R}^r \times \mathbb{C}^s$ with $\text{vol}(A) > 0$. Suppose that*

$$|N(a)| \leq 1 \quad \text{for all } a \in A.$$

Then every lattice Λ in $\mathbb{R}^r \times \mathbb{C}^s$ contains an $x \neq 0$ such that

$$|\mathbf{N}(x)| \leq \frac{2^n}{\text{vol}(A)} \delta(\Lambda).$$

(\mathbf{N} is the norm on $\mathbb{R}^r \times \mathbb{C}^s$ of Definition 1.20, which via the embedding ι is compatible with $\mathbf{N}_{\mathbb{Q}}^K$ on the field K .)

PROOF. Apply Theorem 5.6 to $E = tA$, where t is determined by

$$\text{vol}(tA) = t^n \text{vol}(A) = 2^n \delta(\Lambda).$$

So take $t = 2 \cdot \sqrt[n]{\frac{\delta(\Lambda)}{\text{vol}(A)}}$. Then there is a nonzero $x \in tA \cap \Lambda$. For this x we have

$$|\mathbf{N}(x)| = t^n |\mathbf{N}(\frac{x}{t})| \leq t^n = \frac{2^n}{\text{vol}(A)} \delta(\Lambda). \quad \square$$

This implies that for a nonzero ideal \mathfrak{a} of \mathcal{O}_K there is a nonzero α in \mathfrak{a} such that

$$|\mathbf{N}_{\mathbb{Q}}^K(\alpha)| \leq \frac{2^n}{2^s \text{vol}(A)} \sqrt{|\text{disc}(K)|} \cdot \mathbf{N}(\mathfrak{a}) = \frac{2^{r+s}}{\text{vol}(A)} \sqrt{|\text{disc}(K)|} \cdot \mathbf{N}(\mathfrak{a}). \quad (5.1)$$

This means that we can take $\lambda = \frac{2^{r+s}}{\text{vol}(A)} \sqrt{|\text{disc}(K)|}$. For a small λ , we need, of course, an A satisfying the conditions of Proposition 5.9 with $\text{vol}(A)$ large.

5.10 Definition. For $r, s \in \mathbb{N}$, not both equal to 0, we define

$$A_{r,s} = \{ (x_1, \dots, x_r, z_1, \dots, z_s) \in \mathbb{R}^r \times \mathbb{C}^s \mid |x_1| + \dots + |x_r| + 2|z_1| + \dots + 2|z_s| \leq n \}.$$

The domain $A_{r,s}$ satisfies the conditions for A in Proposition 5.9:

5.11 Lemma. $A_{r,s}$ is compact, convex, symmetric and measurable subset of \mathbb{R}^n . Furthermore, $|\mathbf{N}(a)| \leq 1$ for all $a \in A_{r,s}$.

PROOF. $A_{r,s}$ clearly is compact, convex and symmetric. It is also measurable: what is more, we will compute $\text{vol}(A_{r,s})$ in Proposition 5.14. Let $a \in A_{r,s}$, say $a = (x_1, \dots, x_r, z_1, \dots, z_s)$. Consider the numbers

$$|x_1|, \dots, |x_s|, |z_1|, |\bar{z}_1|, \dots, |z_s|, |\bar{z}_s|.$$

Their geometric mean is $\sqrt[n]{|\mathbf{N}(a)|}$ and their arithmetic mean is at most 1. Since the geometric mean of nonnegative reals is less than or equal to the arithmetic mean, we have for all $a \in A_{r,s}$ the inequality $\sqrt[n]{|\mathbf{N}(a)|} \leq 1$, that is $|\mathbf{N}(a)| \leq 1$. \square

5.12 Examples.

- a) $A_{1,0} = \{ x \in \mathbb{R} \mid |x| \leq 1 \}$ and $\text{vol}(A_{1,0}) = 2$. So for the field \mathbb{Q} we obtain $\lambda = 1$, which is not surprising.

- b) $A_{0,1} = \{z \in \mathbb{C} \mid |z| \leq 1\}$ and $\text{vol}(A_{0,1}) = \pi$. So for an imaginary quadratic number field K we get $\lambda = \frac{2}{\pi} \sqrt{-\text{disc}(K)}$.
- c) $A_{2,0} = \{(x_1, x_2) \mid |x_1| + |x_2| \leq 2\}$ and $\text{vol}(A_{2,0}) = 8$. Then $\lambda = \frac{1}{2} \sqrt{\text{disc}(K)}$ for real quadratic K . See Figure 1.7 on page 29.

5.13 Example. Using the algorithm given in chapter 4 one easily verifies that the ideal class group of $\mathbb{Q}(\sqrt{m})$ is trivial for $m = -43, -67, -163$. This is also easily shown using the bound λ in example b) above. For example the bound for $K = \mathbb{Q}(\sqrt{-43})$ is $\frac{2}{\pi} \sqrt{43}$. Every ideal class contains an ideal \mathfrak{b} with $N(\mathfrak{b}) \leq \frac{2}{\pi} \sqrt{43} < 5$. The ideal (2) is the only prime ideal of norm < 5 . So $\mathcal{O}_K = \mathbb{Z}[\frac{1}{2} + \frac{1}{2}\sqrt{-43}]$ is a principal ideal domain.

The computation of $\text{vol}(A_{r,s})$ is done by standard techniques of calculus.

5.14 Proposition. $\text{vol}(A_{r,s}) = \frac{n^n}{n!} \cdot 2^r \cdot \left(\frac{\pi}{2}\right)^s$, where $n = r + 2s$.

PROOF. Put

$$V_{r,s}(t) = \text{vol}(\{(x_1, \dots, z_1, \dots) \in \mathbb{R}^r \times \mathbb{C}^s \mid |x_1| + \dots + |x_r| + 2|z_1| + \dots + 2|z_s| \leq t\})$$

Note that $V_{r,s}(t) = t^n V_{r,s}(1)$ and $\text{vol}(A_{r,s}) = V_{r,s}(n)$. We will show that

$$V_{r,s}(1) = \frac{2^r}{n!} \left(\frac{\pi}{2}\right)^s.$$

This will be done inductively. For this it suffices to show that

- (i) $V_{1,0}(1) = 2$ and $V_{0,1} = \frac{\pi}{4}$,
- (ii) $V_{0,s+1}(1) = \frac{\pi}{2} \cdot \frac{1}{(2s+1)(2s+2)} \cdot V_{0,s}(1)$ for all $s \in \mathbb{N}^*$,
- (iii) $V_{r+1,s}(1) = \frac{2}{r+2s+1} \cdot V_{r,s}(1)$ for all $(r,s) \in \mathbb{N}^2 \setminus \{(0,0)\}$.

Proofs of (i), (ii) and (iii):

- (i) This is clear, see also the examples a) and b) in 5.12.
- (ii)

$$\begin{aligned} V_{0,s+1}(1) &= \iint_{x^2+y^2 \leq \frac{1}{2}} V_{0,s}(1 - 2\sqrt{x^2+y^2}) \, dx \, dy \\ &= \int_0^{2\pi} \int_0^{\frac{1}{2}} V_{0,s}(1 - 2\rho) \rho \, d\rho \, d\varphi = 2\pi \int_0^{\frac{1}{2}} (1 - 2\rho)^{2s} \rho \, d\rho \cdot V_{0,s}(1) \\ &= 2\pi \int_1^0 u^{2s} \cdot \frac{1}{2}(1-u)\left(-\frac{1}{2}\right) \, du \cdot V_{0,s}(1) \\ &= \frac{\pi}{2} \int_0^1 (u^{2s} - u^{2s+1}) \, du \cdot V_{0,s}(1) = \frac{\pi}{2} \cdot \frac{1}{(2s+1)(2s+2)} \cdot V_{0,s}(1). \end{aligned}$$

(iii)

$$\begin{aligned} V_{r+1,s}(1) &= 2 \int_0^1 V_{r,s}(1-x) dx = 2 \int_0^1 (1-x)^{r+2s} dx \cdot V_{r,s}(1) \\ &= \frac{2}{r+2s+1} \cdot V_{r,s}(1). \quad \square \end{aligned}$$

5.15 Corollary. *Let Λ be a lattice in $\mathbb{R}^r \times \mathbb{C}^s$. Then Λ contains an $x \neq 0$ such that*

$$|\mathbf{N}(x)| \leq \frac{n!}{n^n} \cdot \left(\frac{8}{\pi}\right)^s \cdot \delta(\Lambda),$$

where $n = r + 2s$.

PROOF. Apply Proposition 5.9 to $A_{r,s}$ given in Definition 5.10, and use Proposition 5.14: there is an $x \neq 0$ in Λ such that

$$|\mathbf{N}(x)| \leq \frac{2^n}{\text{vol}(A_{r,s})} \delta(\Lambda) = \frac{n!}{n^n} \cdot \frac{2^{r+2s}}{2^r} \left(\frac{8}{\pi}\right)^s \delta(\Lambda) = \frac{n!}{n^n} \cdot \left(\frac{8}{\pi}\right)^s \cdot \delta(\Lambda). \quad \square$$

In particular inequality (5.1) becomes:

5.16 Corollary. *Let $\mathfrak{a} \neq 0$ be an ideal of \mathcal{O}_K . Then \mathfrak{a} contains an $\alpha \neq 0$ such that*

$$|\mathbf{N}(\alpha)| \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|\text{disc}(K)|} \cdot \mathbf{N}(\mathfrak{a}). \quad \square$$

Now we have much a better λ than in the proof of Proposition 3.24, so Corollary 3.25 now becomes:

5.17 Theorem. *Every ideal class of \mathcal{O}_K contains a nonzero ideal \mathfrak{b} satisfying*

$$\mathbf{N}(\mathfrak{b}) \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|\text{disc}(K)|}. \quad \square$$

The number $\frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|\text{disc}(K)|}$ is called the *Minkowski bound* for the number field K .

5.18 Example. Let $K = \mathbb{Q}(\sqrt[3]{2})$. Then $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{2}]$ (exercise 8 of chapter 1) and $\text{disc}(K) = -27 \cdot 4$. Every ideal class contains an ideal \mathfrak{b} with $\mathbf{N}(\mathfrak{b}) \leq \frac{8}{9\pi} \cdot 2 \cdot 3\sqrt{3} < 3$. The only prime ideal with norm < 3 is $(\sqrt[3]{2})$ and this is a principal ideal. So $\mathbb{Z}[\sqrt[3]{2}]$ is a principal ideal domain.

5.19 Example. Let $K = \mathbb{Q}(\zeta_5)$. Then $\mathcal{O}_K = \mathbb{Z}[\zeta_5]$ and $\text{disc}(K) = 5^3$. Every ideal class contains an ideal \mathfrak{b} with

$$N(\mathfrak{b}) \leq \frac{15\sqrt{5}}{2\pi^2} < \frac{15\sqrt{5}}{18} < 2.$$

So every ideal class contains the ideal (1). The ring $\mathbb{Z}[\zeta_5]$ is a principal ideal domain.

5.20 Example. We will show that $\mathbb{Z}[\zeta_7]$ is a principal ideal domain. In every ideal class there is an ideal \mathfrak{b} with

$$N(\mathfrak{b}) \leq \frac{6!}{6^6} \left(\frac{4}{\pi}\right)^3 \sqrt{7^5} = \frac{2^4 \cdot 5 \cdot 7^2 \sqrt{7}}{3^4 \cdot \pi^3} < \frac{2^4 \cdot 5 \cdot 7^2 \sqrt{7}}{3^7} < \frac{7^2 \sqrt{7}}{3^3} < 5.$$

The minimal polynomial Φ_7 of ζ_7 has over \mathbb{F}_2 two irreducible factors of degree 3 and these correspond to prime ideals of $\mathbb{Z}[\zeta_7]$ of norm 8. Over \mathbb{F}_3 the polynomial is irreducible. So there are no prime ideals of norm less than 5.

For primes p the class number h_p of the cyclotomic field $\mathbb{Q}(\zeta_p)$ equals 1 only for $p \leq 19$. For $p = 23$ the class number is 3. Later, in chapter 7, we will see that the class number h_p^+ of the subfield $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ is a divisor of h_p (Theorem 7.72). The quotient h_p/h_p^+ is usually denoted by h_p^- and is called the relative class number. The relative class number h_p^- has been computed for $p < 521$, e.g. h_{257}^- is equal to the following product of three primes:

$$257 \cdot 20738946049 \cdot 1022997744563911961561298698183419037149697.$$

The class number h_p^+ is hard to compute. Kummer computed h_p for $p \leq 67$ and for these primes we have $h_p^+ = 1$. Probably the smallest prime p with $h_p^+ > 1$ is 163 (it depends on the so-called generalized Riemann hypothesis): $h_{163}^+ = 4$. Kummer's results:

p	h_p	p	h_p	p	h_p	p	h_p	p	h_p
23	3	37	37	43	211	53	4889	61	41 · 1861
31	3 ²	41	11 ²	47	5 · 139	59	3 · 59 · 233	67	67 · 12739

Kummer solved Fermat's Last Theorem for regular primes, primes p with $p \nmid h_p$. It has been shown, however, that there are infinitely many irregular primes, whereas it is unknown whether the number of regular ones is infinite. Apparently, the primes 37, 59 and 67 are irregular. A well-known conjecture is *Vandiver's Conjecture*: $p \nmid h_p^+$ for all primes p .

5.21 Example. Let $K = \mathbb{Q}(\sqrt[3]{5})$. Then $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{5}]$ (exercise 8 of chapter 1) and $\text{disc}(K) = -27 \cdot 5^2$. The Minkowski bound for this field is

$$\frac{3!}{3^3} \cdot \frac{4}{\pi} \sqrt{27 \cdot 5^2} = \frac{8}{9\pi} \sqrt{27 \cdot 5^2} = \frac{40}{\pi\sqrt{3}} < 8.$$

The factorizations of (2), (3), (5) and (7) have been computed in Example 3.9. The only prime ideals of norm less than 8 are

$$(2, 1 + \alpha), \quad (2, 1 + \alpha + \alpha^2), \quad (3, 1 + \alpha) \quad \text{and} \quad (5, \alpha),$$

where $\alpha = \sqrt[3]{5}$. They are of norm 2, 4, 3 and 5 respectively. Clearly $(5, \alpha) = (\alpha)$, a principal ideal. From $N_{\mathbb{Q}}^K(\alpha - 2) = 5 - 8 = -3$ it follows that $(3, 1 + \alpha) = (\alpha - 2)$. So $(3, 1 + \alpha)$ is principal. From $N_{\mathbb{Q}}^K(\alpha + 1) = 5 + 1 = 6$ follows that $(\alpha + 1) = (2, 1 + \alpha)(3, 1 + \alpha)$. Therefore, $(2, 1 + \alpha)$ is also principal and since $(2) = (2, 1 + \alpha)(2, 1 + \alpha + \alpha^2)$, the prime ideal of norm 4 is principal as well. So $\mathbb{Q}(\sqrt[3]{5})$ has class number 1.

5.22 Example. We will show that the field $K = \mathbb{Q}(\sqrt[3]{7})$ has class number 3. We have $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{7}]$. Put $\alpha = \sqrt[3]{7}$. The Minkowski bound is less than 11, so we factorize the ideals (2), (3), (5) and (7):

$$\begin{aligned} (2) &= (2, \alpha + 1)(2, \alpha^2 + \alpha + 1), \\ (3) &= (3, \alpha - 1)^3, \\ (5) &= (5, \alpha - 3)(5, \alpha^2 + 3\alpha + 2), \\ (7) &= (7, \alpha)^3. \end{aligned}$$

The prime ideals of norm less than 11 are

$$(2, \alpha + 1), \quad (2, \alpha^2 + \alpha + 1), \quad (3, \alpha - 1), \quad (5, \alpha - 3) \quad \text{and} \quad (7, \alpha).$$

Their norms are 2, 4, 3, 5 and 7 respectively. The ideal $(7, \alpha)$ is the principal ideal generated by α . The identities

$$(2) = (2, \alpha + 1)(2, \alpha^2 + \alpha + 1) \quad \text{and} \quad (\alpha - 2) = (2, \alpha + 1)(3, \alpha - 1)$$

imply that $(2, \alpha^2 + \alpha + 1)$ and $(3, \alpha - 1)$ represent the same ideal class, i.e. the inverse of the class represented by $(2, \alpha + 1)$. Since $N_{\mathbb{Q}}^K(\alpha + 2) = 15$, we have

$$(\alpha + 2) = (3, \alpha - 1)(5, \alpha - 3).$$

So $(5, \alpha - 3)$ is equivalent to $(2, \alpha + 1)$. Hence, the ideal class group is generated by the class of $(2, \alpha + 1)$. Its inverse is the class of $(3, \alpha - 1)$ and since $(3, \alpha - 1)^3$ is principal, the ideal class group is either of order 1 or of order 3. We will show that $(2, \alpha + 1)$ is not principal. Suppose $(2, \alpha + 1)$ is principal, then there is an element of norm ± 2 . By direct computation

$$N_{\mathbb{Q}}^K(x + y\alpha + z\alpha^2) = x^3 + 7y^3 + 49z^3 - 21xyz$$

and so

$$N_{\mathbb{Q}}^K(x + y\alpha + z\alpha^2) \equiv x^3 \pmod{7}.$$

However, there is no $x \in \mathbb{Z}$ such that $x^3 \equiv \pm 2 \pmod{7}$.

5.23 Example. An integral basis of $K = \mathbb{Q}(\sqrt{-2}, \sqrt{3})$ is $(1, \sqrt{3}, \sqrt{-2}, \frac{\sqrt{-6} + \sqrt{-2}}{2})$ (Exercise 9 of chapter 1). We have $\text{disc}(K) = 2^8 \cdot 3^2$. The Minkowski bound is less than 8. Put $\alpha = \frac{\sqrt{-6} + \sqrt{-2}}{2}$. Then $\alpha^2 = -2 - \sqrt{3}$ and the minimal polynomial of α over \mathbb{Q} is $X^4 + 4X^2 + 1$. So

$$\begin{aligned} \text{disc}(1, \alpha, \alpha^2, \alpha^3) &= \text{disc}(X^4 + 4X^2 + 1) = N_{\mathbb{Q}}^K(4\alpha^3 + 8\alpha) \\ &= 4^4 N_{\mathbb{Q}}^K(\alpha) N_{\mathbb{Q}}^K(\alpha^2 + 2) = 4^4 N_{\mathbb{Q}}^K(-\sqrt{3}) = 4^4 \cdot 3^2 = 2^8 \cdot 3^2. \end{aligned}$$

It follows that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Hence we can use the polynomial $X^4 + 4X^2 + 1$ for the factorization of prime numbers in K :

$$\begin{aligned} (2) &= (2, \alpha + 1)^4, \\ (3) &= (3, \alpha - 1)^2(3, \alpha + 1)^2, \\ (5) &= (5, \alpha^2 - 2\alpha - 1)(5, \alpha^2 + 2\alpha - 1), \\ (7) &= (7, \alpha^2 - \alpha - 1)(7, \alpha^2 + \alpha - 1). \end{aligned}$$

There are three prime ideals of norm less than 8:

$$\mathfrak{p}_2 = (2, \alpha + 1), \quad \mathfrak{p}_3 = (3, \alpha + 1) \quad \text{and} \quad \mathfrak{p}'_3 = (3, \alpha - 1).$$

The elements $\alpha + 1$ and $\alpha - 1$ both are of norm 6. So $(\alpha + 1) = \mathfrak{p}_2 \mathfrak{p}_3$ and $(\alpha - 1) = \mathfrak{p}_2 \mathfrak{p}'_3$. Hence $\mathcal{C}(K)$ is generated by $[\mathfrak{p}_2]$ and from $\mathfrak{p}_2^4 = (2)$ it follows that the order of the group is a divisor of 4. Since $N_{\mathbb{Q}}^K(\sqrt{-2}) = 4$, we have $(\sqrt{-2}) = \mathfrak{p}_2^2$ and so $[\mathfrak{p}_2]^2 = 1$. Suppose K contains an element β of norm ± 2 . Then from

$$N_{\mathbb{Q}}^K(\beta) = N_{\mathbb{Q}}^{\mathbb{Q}(\sqrt{-6})}(N_{\mathbb{Q}(\sqrt{-6})}^K(\beta))$$

it would follow that $\mathbb{Q}(\sqrt{-6})$ contains an element of norm ± 2 , which is not the case. Hence $\mathcal{C}(K)$ is of order 2 and is generated by $[\mathfrak{p}_2]$.

5.24 Example. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Then $(1, \sqrt{2}, \sqrt{3}, \frac{\sqrt{2} + \sqrt{6}}{2})$ is an integral basis of K . We have $\text{disc}(K) = 2^8 \cdot 3^3$ and in the same way as in the previous example we see that $\mathcal{O}_K = \mathbb{Z}[\alpha]$, where $\alpha = \frac{\sqrt{2} + \sqrt{6}}{2}$. The Minkowski bound is less than 5. The minimal polynomial $X^4 - 4X^2 + 1$ of α over \mathbb{Q} can be used for the splitting of primes. This way we find that $\mathfrak{p}_2 = (2, \alpha + 1)$ is the only prime ideal with norm less than 5. We have $N_{\mathbb{Q}}^K(\alpha + 1) = 1 - 4 + 1 = -2$, so \mathfrak{p}_2 is the principal ideal generated by $\alpha + 1$. Hence $\mathcal{C}(K)$ is trivial.

From Theorem 3.30 together with the computation of the Minkowski bound it follows that \mathbb{Q} has no unramified extensions:

5.25 Theorem. *Let $K \neq \mathbb{Q}$. Then there is a prime number which ramifies in K .*

PROOF. Put $[K : \mathbb{Q}] = n$ and $n = r + 2s$, where r is the number of real embeddings and s the number of pairs of complex embeddings. We have $n \geq 2$ and since norms of ideals are ≥ 1 , we have by Theorem 5.17:

$$\sqrt{|\text{disc}(K)|} \geq \frac{n^n}{n!} \left(\frac{\pi}{4}\right)^s.$$

We will use that $\frac{n^n}{n!} \geq 2^{n-1}$ for all $n \geq 2$. This is easily proved by induction: for $n = 2$ this is true and the induction step goes as follows

$$\begin{aligned} \frac{(n+1)^{n+1}}{(n+1)!} &= \frac{n^n}{n!} \cdot \frac{(n+1)^{n+1}}{n^n} \cdot \frac{1}{n+1} = \frac{n^n}{n!} \left(1 + \frac{1}{n}\right)^n \geq 2^{n-1} \left(1 + \frac{1}{n}\right)^n \\ &\geq 2^{n-1} \left(1 + n \cdot \frac{1}{n}\right) = 2^n. \end{aligned}$$

Hence

$$\sqrt{|\text{disc}(K)|} \geq 2^{n-1} \left(\frac{\pi}{4}\right)^s = 2^{r-1} \pi^s$$

and so

$$|\text{disc}(K)| \geq 4^{r-1} \pi^{2s} = \frac{1}{4} 4^r \pi^{2s} \geq \frac{1}{4} \pi^{r+2s} = \frac{1}{4} \pi^n \geq \frac{1}{4} \pi^2 > 2.$$

It follows that $|\text{disc}(K)| \geq 3$ and so there is a prime divisor of the discriminant of K . By Theorem 3.30 this prime number ramifies in K . \square

5.4 Dirichlet's Unit Theorem

In this section K is a number field. Dirichlet's Unit Theorem gives a complete description of the structure of the unit group \mathcal{O}_K^* . We will use the embedding $\iota: K \rightarrow \mathbb{R}^r \times \mathbb{C}^s$. This ring homomorphism induces a group homomorphism

$$\iota: K^* \rightarrow (\mathbb{R}^r \times \mathbb{C}^s)^* (= \mathbb{R}^{*r} \times \mathbb{C}^{*s}).$$

5.26 Notations. The map $L: \mathbb{R}^{*r} \times \mathbb{C}^{*s} \rightarrow \mathbb{R}^{r+s}$ is defined by

$$L: (x_1, \dots, x_r, z_1, \dots, z_s) \mapsto (\log |x_1|, \dots, \log |x_r|, \log z_1 \bar{z}_1, \dots, \log z_s \bar{z}_s).$$

It is a homomorphism from the multiplicative group $\mathbb{R}^{*r} \times \mathbb{C}^{*s}$ to the additive group \mathbb{R}^{r+s} . For the real embeddings σ_i ($1 \leq i \leq r$) let $\lambda_i: K^* \rightarrow \mathbb{R}$ be the composition

$$K^* \xrightarrow{\sigma_i} \mathbb{R}^* \xrightarrow{|\cdot|} \mathbb{R}$$

and for the complex embeddings $\tau_j: K \rightarrow \mathbb{C}$ ($1 \leq j \leq s$) the composition

$$K^* \xrightarrow{\tau_j} \mathbb{C}^* \xrightarrow{2 \log|\cdot|} \mathbb{R}$$

is denoted by λ_{r+j} . Thus the composition $L: K^* \rightarrow \mathbb{R}^{r+s}$ is the homomorphism

$$\alpha \mapsto (\lambda_1(\alpha), \dots, \lambda_{r+s}(\alpha)).$$

This homomorphism will be denoted by l and its restriction to \mathcal{O}_K^* by ψ . So we have a commutative diagram

$$\begin{array}{ccc} K^* & \xrightarrow{l} & \mathbb{R}^{*r} \times \mathbb{C}^{*s} \\ \uparrow \subset & \searrow l & \downarrow L \\ \mathcal{O}_K^* & \xrightarrow{\psi} & \mathbb{R}^{r+s} \end{array}$$

We will determine the structure of \mathcal{O}_K^* by studying the kernel and the image of the group homomorphism $\psi: \mathcal{O}_K^* \rightarrow \mathbb{R}^{r+s}$.

5.27 Lemma. *Let B be a bounded subset of \mathbb{R}^{r+s} . Then $L^{-1}(B)$ is a bounded subset of $\mathbb{R}^r \times \mathbb{C}^s$.*

PROOF. Since B is bounded, it is contained in a cube $[-a, a]^{r+s}$ for some positive real a . The lemma follows from:

- (i) The inverse image of $[-a, a]$ under $\mathbb{R}^* \rightarrow \mathbb{R}$, $x \mapsto \log|x|$ is $[-e^a, -e^{-a}] \cup [e^{-a}, e^a]$, which is contained in $[-e^a, e^a]$.
- (ii) The inverse image of $[-a, a]$ under $\mathbb{C}^* \rightarrow \mathbb{R}$, $z \mapsto \log z\bar{z}$ is $\{z \in \mathbb{C} \mid e^{-\frac{a}{2}} \leq |z| \leq e^{\frac{a}{2}}\}$. It is contained in the disc $\{z \in \mathbb{C} \mid |z| \leq e^{\frac{a}{2}}\}$. \square

5.28 Proposition. $\text{Ker}(\psi) = \mu(K)$.

PROOF. The only element of finite order in the additive group \mathbb{R}^{r+s} is 0. So ψ maps elements of finite order to 0, that is $\mu(K) \subseteq \text{Ker}(\psi)$. Since $\{0\}$ is a bounded subset of \mathbb{R}^{r+s} , by Lemma 5.27 its inverse image $L^{-1}(\{0\}) = \text{Ker}(L)$ in $\mathbb{R}^{*r} \times \mathbb{C}^{*s}$ is a bounded subset of $\mathbb{R}^r \times \mathbb{C}^s$. By Proposition 5.3 it contains only finitely many elements of the lattice Λ_K . So $\text{Ker}(\psi)$ is a finite subgroup of K^* and its elements are, therefore, of finite order, that is they are roots of unity. \square

5.29 Notation. Let $m \in \mathbb{N}^*$. The $m - 1$ -dimensional subspace

$$\{(x_1, \dots, x_m) \in \mathbb{R}^m \mid x_1 + \dots + x_m = 0\}$$

of the \mathbb{R} -vector space \mathbb{R}^m will be denoted by H_m .

5.30 Lemma. $\psi(\mathcal{O}_K^*)$ is a discrete subgroup of \mathbb{R}^{r+s} and is contained in H_{r+s} .

PROOF. Put $\Gamma = \psi(\mathcal{O}_K^*)$. Let B be a bounded subset of \mathbb{R}^{r+s} . Then by Lemma 5.27 $L^{-1}(B)$ is a bounded subset of $\mathbb{R}^r \times \mathbb{C}^s$. The inverse image of $\Gamma \cap B$ is contained in $\Lambda_K \cap L^{-1}(B)$, and is, since Λ_K is a lattice in $\mathbb{R}^r \times \mathbb{C}^s$, a finite set by Proposition 5.3. So $\Gamma \cap B$ is finite. Hence by Proposition 5.3 the group Γ is a discrete subgroup of \mathbb{R}^{r+s} . It is contained in H_{r+s} : for $\varepsilon \in \mathcal{O}_K^*$ we have

$$N_{\mathbb{Q}}^K(\varepsilon) = \sigma_1(\varepsilon) \cdots \sigma_r(\varepsilon) \tau_1(\varepsilon) \overline{\tau_1(\varepsilon)} \cdots \tau_s(\varepsilon) \overline{\tau_s(\varepsilon)} = \pm 1$$

and so

$$\log |\sigma_1(\varepsilon)| + \cdots + \log |\sigma_r(\varepsilon)| + \log \tau_1(\varepsilon) \overline{\tau_1(\varepsilon)} + \cdots + \log \tau_s(\varepsilon) \overline{\tau_s(\varepsilon)} = 0. \quad \square$$

We will show that $\psi(\mathcal{O}_K^*)$ is a lattice in H_{r+s} .

5.31 Proposition. Let $c_1, \dots, c_{r+s} \in \mathbb{R}^{>0}$ such that

$$\prod_{i=1}^{r+s} c_i \geq \left(\frac{2}{\pi}\right)^s \sqrt{|\text{disc}(K)|}.$$

Then there exists a nonzero β in \mathcal{O}_K such that

$$|\sigma_i(\beta)| \leq c_i \quad \text{for } i = 1, \dots, r$$

and

$$\tau_j(\beta) \overline{\tau_j(\beta)} \leq c_{i+j} \quad \text{for } j = 1, \dots, s.$$

PROOF. Let E be the subset of $\mathbb{R}^r \times \mathbb{C}^s$ of all $(x_1, \dots, x_r, z_1, \dots, z_s)$ such that

$$|x_1| \leq c_1, \dots, |x_r| \leq c_r, z_1 \overline{z_1} \leq c_{r+1}, \dots, z_s \overline{z_s} \leq c_{r+s}.$$

Then E is convex, symmetric and measurable, and for its volume we have

$$\text{vol}(E) = 2^r c_1 \cdots c_r \cdot \pi^s c_{r+1} \cdots c_{r+s} \geq 2^{r+s} \sqrt{|\text{disc}(K)|} = 2^n \delta(\Lambda_K).$$

By Theorem 5.6 there is a nonzero $x \in \Lambda_R \cap E$. Take $\beta \in \mathcal{O}_K$ with $\iota(\beta) = x$. \square

5.32 Lemma. Let $k \in \mathbb{N}^*$ with $1 \leq k \leq r+s$. Then there exists an $\varepsilon \in \mathcal{O}_K^*$ such that $\lambda_i(\varepsilon) < 0$ for all $i \neq k$.

PROOF. Let α be a nonzero element of \mathcal{O}_K . Choose $c_1, \dots, c_{r+s} \in \mathbb{R}^{>0}$ such that for all $i \neq k$

$$\begin{aligned} c_i &< |\sigma_i(\alpha)| & \text{if } i \leq r, \\ c_i &< |\tau_{i-r}(\alpha)|^2 & \text{if } i > r \end{aligned}$$

and

$$\prod_{i=1}^{r+s} c_i = \left(\frac{2}{\pi}\right)^2 \sqrt{|\text{disc}(K)|}.$$

By Proposition 5.31 there exists a nonzero $\beta \in \mathcal{O}_K$ such that $\lambda_i(\beta) < \log c_i$ for $i = 1, \dots, r + s$. So $\lambda_i(\beta) < \lambda_i(\alpha)$ for all $i \neq k$. Thus we can form a sequence $\alpha_1, \alpha_2, \dots$ of nonzero elements of \mathcal{O}_K such that for all $m \in \mathbb{N}^*$

$$\lambda_i(\alpha_{m+1}) < \lambda_i(\alpha_m) \quad \text{for all } i \neq k$$

and

$$|\mathbb{N}_{\mathbb{Q}}^K(\alpha_m)| < \left(\frac{2}{\pi}\right)^2 \sqrt{|\text{disc}(K)|}.$$

Because there is an upperbound for the norm of the principal ideals (α_m) , there are only finitely many of them. Hence there exist m_1 and m_2 such that $m_1 < m_2$ and $(\alpha_{m_1}) = (\alpha_{m_2})$. Take $\varepsilon = \alpha_{m_1}^{-1} \alpha_{m_2}$. \square

5.33 Lemma. *Let (a_{ij}) be an $m \times m$ -matrix with entries in \mathbb{R} such that*

- a) $a_{ii} > 0$ for $i = 1, \dots, m$,
- b) $a_{ij} < 0$ for $i \neq j$,
- c) $\sum_j a_{ij} = 0$ for $i = 1, \dots, m$.

Then (a_{ij}) is a matrix of rank $m - 1$.

PROOF. We show that the first $m - 1$ columns are independent. Suppose that to the contrary

$$\lambda_1 \begin{pmatrix} a_{11} \\ \vdots \\ a_{m1} \end{pmatrix} + \dots + \lambda_{m-1} \begin{pmatrix} a_{1,m-1} \\ \vdots \\ a_{m,m-1} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix},$$

where not all λ_i equal 0. Divide by λ_k with $|\lambda_k|$ maximal: we may assume that $\lambda_k = 1$ and $\lambda_j \leq 1$ for $j \neq k$. Consider the k -th row:

$$0 = \sum_{j=1}^{m-1} \lambda_j a_{kj} = a_{kk} + \sum_{\substack{j=1 \\ j \neq k}}^{m-1} \lambda_j a_{kj} \geq a_{kk} + \sum_{\substack{j=1 \\ j \neq k}}^{m-1} a_{kj} = \sum_{j=1}^{m-1} a_{kj} > \sum_{j=1}^m a_{kj} = 0.$$

Contradiction. \square

5.34 Proposition. $\psi(\mathcal{O}_K^*)$ is a lattice in H_{r+s} .

PROOF. By Lemma 5.32 there exist $\varepsilon_1, \dots, \varepsilon_{r+s} \in \mathcal{O}_K^*$ such that:

the i -th component of $l(\varepsilon_k)$ is negative for all i, k with $i \neq k$.

Write $l(\varepsilon_k) = (a_{k1}, \dots, a_{k, r+s})$. The matrix (a_{ij}) satisfies the conditions of Lemma 5.33 (with $m = r + s$). So the rank of this matrix equals $r + s - 1$. This means that the subgroup $\psi(\mathcal{O}_K^*)$ contains a lattice in H_{r+s} . Since $\psi(\mathcal{O}_K^*)$ is a discrete subgroup of \mathbb{R}^{r+s} , it follows from Proposition 5.3 that it is a lattice in H_{r+s} . \square

From Proposition 5.28 it follows that we have a short exact sequence

$$1 \longrightarrow \mu(K) \longrightarrow \mathcal{O}_K^* \xrightarrow{\psi} \psi(\mathcal{O}_K^*) \longrightarrow 0$$

and since by Proposition 5.34 $\psi(\mathcal{O}_K^*)$ is a free abelian group of rank $r + s - 1$, this sequence splits and we can choose $\varepsilon_1, \dots, \varepsilon_{r+s-1} \in \mathcal{O}_K^*$ which map under ψ to a \mathbb{Z} -basis of $\psi(\mathcal{O}_K^*)$. This leads to *Dirichlet's Unit Theorem*:

5.35 Theorem (Dirichlet). *There are $\varepsilon_1, \dots, \varepsilon_{r+s-1} \in \mathcal{O}_K^*$ such that each $\varepsilon \in \mathcal{O}_K^*$ can be written in a unique way as*

$$\varepsilon = \zeta \varepsilon_1^{k_1} \dots \varepsilon_{r+s-1}^{k_{r+s-1}}$$

with ζ a root of unity and $k_1, \dots, k_{r+s-1} \in \mathbb{Z}$. \square

5.36 Definition. A system $\varepsilon_1, \dots, \varepsilon_{r+s-1}$ as in Theorem 5.35 is called a *fundamental system of units* of K .

5.37 Example. We compute \mathcal{O}_K^* for the field $K = \mathbb{Q}(\sqrt{-2}, \sqrt{3})$ of Example 5.23. It is easily verified that -1 is the only nontrivial root of unity in K . By Dirichlet's Unit Theorem the group of units is of rank 1: $\mathcal{O}_K^* = \langle -1, \varepsilon \rangle$ for some $\varepsilon \in \mathcal{O}_K^*$. For the quadratic subfields we have $\mathbb{Z}[\sqrt{-2}]^* = \mathbb{Z}[\sqrt{-6}]^* = \langle -1 \rangle$ and $\mathbb{Z}[\sqrt{3}]^* = \langle -1, 2 + \sqrt{3} \rangle$. Let $\nu \in \mathcal{O}_K^*$. Let $\sigma, \tau \in \text{Gal}(K : \mathbb{Q})$ such that $K^\sigma = \mathbb{Q}(\sqrt{-2})$ and $K^\tau = \mathbb{Q}(\sqrt{3})$. Then $K^{\sigma\tau} = \mathbb{Q}(\sqrt{-6})$ and

$$\begin{aligned} \nu \cdot \sigma(\nu) &\in \mathbb{Z}[\sqrt{-2}]^* = \langle -1 \rangle, \\ \nu \cdot \tau(\nu) &\in \mathbb{Z}[\sqrt{3}]^* = \langle -1, 2 + \sqrt{3} \rangle, \\ \nu \cdot \sigma\tau(\nu) &\in \mathbb{Z}[\sqrt{-6}]^* = \langle -1 \rangle. \end{aligned}$$

For the product of these elements we obtain

$$\nu^2 \cdot \mathbf{N}_{\mathbb{Q}}^K(\nu) \in \langle -1, 2 + \sqrt{3} \rangle,$$

and so $\nu^2 \in \langle -1, 2 + \sqrt{3} \rangle$. By the way, in this special case this result already implies that the group \mathcal{O}_K^* is of rank 1. It suffices to verify whether there exist $k, l \in \{0, 1\}$

with k and l not both 0 such that $(-1)^k(2 + \sqrt{3})^l$ is a square in K . The number -1 is not a square since $i \notin K$. If $2 + \sqrt{3}$ were a square, it would be the square of a real number and, therefore, the square of a number in $\mathbb{Q}(\sqrt{3})$. Since $2 + \sqrt{3}$ is the fundamental unit in this quadratic number field, it is not a square in that field. In Example 5.23 we saw that for $\alpha = \frac{\sqrt{-6} + \sqrt{-2}}{2}$ we have $\alpha^2 = -2 - \sqrt{3}$. Hence $\mathcal{O}_K^* = \langle -1, \alpha \rangle$.

5.38 Example. We compute \mathcal{O}_K^* for the field $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ of Example 5.24. For the quadratic subfields we have $\mathbb{Z}[\sqrt{2}]^* = \langle -1, 1 + \sqrt{2} \rangle$, $\mathbb{Z}[\sqrt{3}]^* = \langle -1, 2 + \sqrt{3} \rangle$ and $\mathbb{Z}[\sqrt{6}]^* = \langle -1, 5 + 2\sqrt{6} \rangle$. Let $\nu \in \mathcal{O}_K^*$. As in the previous example we conclude that

$$\nu^2 \in \langle -1, 1 + \sqrt{2}, 2 + \sqrt{3}, 5 + 2\sqrt{6} \rangle.$$

From this and also from Dirichlet's Unit Theorem it follows that \mathcal{O}_K^* is of rank 3. Since the field is a subfield of \mathbb{R} , ν^2 is a positive real number. It suffices to look for $\nu \in K$ with $\nu^2 = (1 + \sqrt{2})^k(2 + \sqrt{3})^l(5 + 2\sqrt{6})^m$, where $k, l, m \in \{0, 1\}$. The ideal $\mathfrak{p}_2 = (\alpha + 1)$ is the unique ideal of norm 2. So $\mathfrak{p}^2 = (\sqrt{2}) = (1 + \sqrt{3}) = (2 + \sqrt{6})$. The number $\nu_1 = \frac{1 + \sqrt{3}}{\sqrt{2}} \in \mathcal{O}_K^*$ satisfies $\nu_1^2 = 2 + \sqrt{3}$ and the number $\nu_2 = \frac{2 + \sqrt{6}}{\sqrt{2}} \in \mathcal{O}_K^*$ satisfies $\nu_2^2 = 5 + 2\sqrt{6}$. We have $\nu_1 = \alpha$ and $\nu_2 = \sqrt{2} + \sqrt{3}$. Then

$$\nu^2 = (1 + \sqrt{2})^k \nu_1^{2l} \nu_2^{2m}$$

and so

$$\left(\frac{\nu}{\nu_1^l \nu_2^m} \right)^2 = (1 + \sqrt{2})^k.$$

The number $1 + \sqrt{2}$ is not a square in K : its image is negative under an automorphism which maps $\sqrt{2}$ to $-\sqrt{2}$. So $k = 0$ and $\nu = \nu_1^l \nu_2^m$. Hence

$$\mathcal{O}_K^* = \left\langle -1, 1 + \sqrt{2}, \sqrt{2} + \sqrt{3}, \frac{\sqrt{2} + \sqrt{6}}{2} \right\rangle.$$

For the computation of the ideal class group knowledge of the group of units sometimes is helpful. The following is an example of this phenomenon.

5.39 Example. Let $K = \mathbb{Q}(\sqrt[3]{11})$. Put $\alpha = \sqrt[3]{11}$. Then $\mathcal{O}_K = \mathbb{Z}[\alpha]$ and $\text{disc}(K) = -27 \cdot 11^2$ (exercise 9 of chapter 1). The Minkowski bound is $\frac{88}{9\pi} \sqrt{3} < 6$. We factorize the primes less than 6 by factorizing $X^3 - 11$ modulo these primes:

$$\begin{aligned} (2) &= (2, \alpha + 1)(2, \alpha^2 + \alpha + 1) \\ (3) &= (3, \alpha + 1)^3 \\ (5) &= (5, \alpha - 1)(5, \alpha^2 + \alpha + 1). \end{aligned}$$

The ideal class group is generated by the classes of the prime ideals of norm less than 6: $\mathfrak{p}_2 = (2, \alpha + 1)$, $\mathfrak{p}'_2 = (2, \alpha^2 + \alpha + 1)$, $\mathfrak{p}_3 = (3, \alpha + 1)$ and $\mathfrak{p}_5 = (5, \alpha - 1)$.

The factorization of (2) implies that \mathfrak{p}'_2 is in the inverse of the class of \mathfrak{p}_2 . From $N_{\mathbb{Q}}^K(\alpha - 1) = -(1^3 - 11) = 10$ follows that $(\alpha - 1) = \mathfrak{p}_2\mathfrak{p}_5$, so also \mathfrak{p}_5 is in the inverse of the class of \mathfrak{p}_2 . Furthermore, $N_{\mathbb{Q}}^K(\alpha - 2) = -(2^3 - 11) = 3$, so the class of \mathfrak{p}_3 is the unity element. From all this it follows that $\mathcal{C}(K)$ is generated by $[\mathfrak{p}_2]$. The remaining problem is to determine the order of $[\mathfrak{p}_2]$. We have $N_{\mathbb{Q}}^K(\alpha^2 - 5) = -(5^3 - 121) = -4$. Modulo \mathfrak{p}_2 we have $\alpha^2 - 5 \equiv (\alpha + 1)^2 \equiv 0$ and so $\mathfrak{p}_2 \mid (\alpha^2 - 5)$. Hence $(\alpha^2 - 5) = \mathfrak{p}_2^2$. So $\mathcal{C}(K)$ is of order 1 or 2. We will show that it is of order 2 by showing that the ideal \mathfrak{p}_2 is not principal.

By Dirichlet's Unit Theorem $\mathbb{Z}[\alpha]^* = \langle -1, \varepsilon \rangle$, where ε is a unit > 1 , the fundamental unit of K . The ideal \mathfrak{p}_3 is principal and $\mathfrak{p}_3^3 = (3)$. So $\nu = \frac{(\alpha-2)^3}{3} \in \mathbb{Z}[\alpha]^*$. Since $\nu > 0$, it is a power of ε . We will show that it is an odd power of ε . From

$$3\nu = (\alpha - 2)^3 \equiv (-1)^3 \equiv 4 \pmod{\mathfrak{p}_5}$$

follows that $\bar{\nu} \in \mathbb{Z}[\alpha]/\mathfrak{p}_5 = \mathbb{F}_5$ is not a square. Therefore, ν is not a square in $\mathbb{Z}[\alpha]$. Hence ν is an odd power of ε , say $\nu = \varepsilon^k$ for an odd $k \in \mathbb{Z}$. This will be used to show that \mathfrak{p}_2 is not principal. Later, in Example 5.44, we will see that in fact $k = -1$.

Suppose \mathfrak{p}_2 is principal, say $\mathfrak{p}_2 = (\beta)$. Then $(\beta^2) = \mathfrak{p}_2^2 = (\alpha^2 - 5)$ and so for some $l \in \mathbb{Z}$

$$\beta^2 = \pm \varepsilon^l (\alpha^2 - 5).$$

Raising to the power k yields

$$\beta^{2k} = \pm \nu^l (\alpha^2 - 5)^k$$

and, since $\beta^{2k} > 0$, $\alpha^2 - 5 < 0$ and k odd, we have in fact

$$\beta^{2k} = -\nu^l (\alpha^2 - 5)^k.$$

The prime 19 splits completely in K : $(19) = (19, \alpha + 2)(19, \alpha + 3)(19, \alpha - 5)$. Modulo $\mathfrak{p}_{19} = (19, \alpha - 5)$ we have

$$3\nu = (\alpha - 2)^3 \equiv 3^3 \pmod{\mathfrak{p}_{19}}$$

and so $\nu \equiv 3^2 \pmod{\mathfrak{p}_{19}}$. Hence, since $\alpha^2 - 5 \equiv 1 \pmod{\mathfrak{p}_{19}}$,

$$\beta^{2k} \equiv -3^{2l} \pmod{\mathfrak{p}_{19}},$$

from which it follows that -1 is a square modulo 19. This, however, is not the case since $19 \equiv 3 \pmod{4}$. So \mathfrak{p}_2 is not principal and $\mathcal{C}(K)$ is of order 2.

Cubic fields with one real embedding

Let K be of degree 3 with one real embedding. Let's assume that K is in fact a subfield of \mathbb{R} . Then the real embedding is just the inclusion map and K has one pair $(\tau, \bar{\tau})$ of complex embeddings. Examples of such fields are the pure cubic fields; see exercise 8 of chapter 1. Since K is real, we have $\mu(K) = \{\pm 1\}$. By Dirichlet's Unit Theorem \mathcal{O}_K^* is of rank 1. It follows that there is a 'fundamental unit' $\varepsilon > 1$ such that $\mathcal{O}_K^* = \langle -1, \varepsilon \rangle$. The following lemma of Artin is useful when computing the fundamental unit, because it gives a lower bound for positive units.

5.40 Lemma. *Let $\nu \in \mathcal{O}_K^*$ with $\nu > 1$. Then $|\text{disc}(K)| < 4\nu^3 + 24$.*

PROOF. We have $N_{\mathbb{Q}}^K(\nu) = \nu\tau(\nu)\overline{\tau(\nu)} > 0$, so $N_{\mathbb{Q}}^K(\nu) = 1$. Since $\nu \notin \mathbb{Q}$ and $\nu \in \mathcal{O}_K$, we have that $K = \mathbb{Q}(\nu)$ and that $\mathbb{Z}[\nu]$ is a number ring of K . So $d = \text{disc}(1, \nu, \nu^2) = m^2 \cdot \text{disc}(K)$, where $m = (\mathcal{O}_K : \mathbb{Z}[\nu])$. There are unique $\rho \in (0, \infty)$ and $\vartheta \in (0, \pi)$ such that

$$\nu = \rho^2 \quad \text{and} \quad \tau(\nu) = \rho^{-1}e^{i\vartheta}$$

(assuming that $\tau(\nu)$ has a positive imaginary part). We see d as a function of ϑ (keeping ρ fixed):

$$\begin{aligned} \sqrt{d} = \sqrt{d(\vartheta)} &= \begin{vmatrix} 1 & \rho^2 & \rho^4 \\ 1 & \rho^{-1}e^{i\vartheta} & \rho^{-2}e^{2i\vartheta} \\ 1 & \rho^{-1}e^{-i\vartheta} & \rho^{-2}e^{-2i\vartheta} \end{vmatrix} = (\rho^3 + \rho^{-3})(e^{-i\vartheta} - e^{i\vartheta}) + e^{2i\vartheta} - e^{-2i\vartheta} \\ &= -2i((\rho^3 + \rho^{-3})\sin \vartheta - \sin 2\vartheta). \end{aligned}$$

Set $y = \frac{1}{2}(\rho^3 + \rho^{-3})$. Then

$$\sqrt{d} = -4i(y \sin \vartheta - \sin \vartheta \cos \vartheta)$$

and $|d|$ has a maximum only when the derivative of $y \sin \vartheta - \sin \vartheta \cos \vartheta$ vanishes. Say this is the case for $\vartheta = \vartheta_0$. Then

$$y \cos \vartheta_0 - 2 \cos 2\vartheta_0 = 0$$

and

$$|\sqrt{d}| = 4|(y - \cos \vartheta) \sin \vartheta| \leq 4|(y - \cos \vartheta_0) \sin \vartheta_0|.$$

Put $z = \cos \vartheta_0$. Then

$$2z^2 - yz - 1 = 0 \quad \text{and} \quad |d| \leq 16(y - z)^2(1 - z^2).$$

Hence,

$$|d| \leq 16(y^2 - 2yz + z^2)(1 - z^2) = 16(y^2 - 2yz + z^2 - y^2z^2 + 2yz^3 - z^4)$$

$$= 16(y^2 - 2(2z^2 - 1) + z^2 - (2z^2 - 1)^2 + 2(2z^2 - 1)z^2 - z^4) = 16(y - z^2 - z^4) \\ = 4(\rho^6 + 6 + \rho^{-6} - 4z^2 - 4z^4).$$

So it suffices to show that $\rho^{-6} < 4z^2 + 4z^4$. The polynomial $2X^2 - yX - 1$ has two zeros, one of them is z . One root is positive and, since $y = \frac{1}{2}(\rho^3 + \rho^{-3}) > 1$, in fact greater than 1:

$$\frac{y + \sqrt{y^2 + 8}}{4} > \frac{1 + \sqrt{9}}{4} = 1.$$

So $z = \cos \vartheta$ is the other zero. The quadratic polynomial takes in $-\frac{1}{2}\rho^{-3}$ a negative value:

$$2(-\frac{1}{2}\rho^{-3})^2 - y(-\frac{1}{2}\rho^{-3}) - 1 = \frac{3}{4}(\rho^{-6} - 1) < 0.$$

Therefore, $z < -\frac{1}{2}\rho^{-3}$ and so $z^2 > \frac{1}{4}\rho^{-6}$. This implies $\rho^{-6} < 4z^2 < 4z^2 + 4z^4$. \square

5.41 Corollary. Suppose $|\text{disc}(K)| > 28$. Let $\eta \in \mathcal{O}_K^*$ with $\eta > 1$, say $\eta = \varepsilon^k$. Then k satisfies

$$\left(\frac{|\text{disc}(K)| - 24}{4}\right)^k < \eta^3.$$

PROOF. By Lemma 5.40 $\frac{|\text{disc}(K)| - 24}{4} < \varepsilon^3$ and so

$$\left(\frac{|\text{disc}(K)| - 24}{4}\right)^k < \varepsilon^{3k} = \eta^3. \quad \square$$

Note that only finitely many k are possible:

$$k < \frac{3 \log \eta}{\log \rho}, \text{ where } \rho = \frac{1}{4}(|\text{disc}(K)| - 24).$$

5.42 Example. The ring of integers of $K = \mathbb{Q}(\sqrt[3]{2})$ is $\mathbb{Z}[\sqrt[3]{2}]$ (exercise 8 of chapter 1). Put $\alpha = \sqrt[3]{2}$. We have $\text{disc}(K) = \text{disc}(1, \alpha, \alpha^2) = -N_{\mathbb{Q}}^K(3\alpha^2) = -3^3 \cdot 4$. Clearly $\alpha - 1$ is a unit. Its inverse is $\alpha^2 + \alpha + 1$, a unit > 1 . We have $(\alpha^2 + \alpha + 1)^3 < (2 + 2 + 1)^3 = 125$ and for all $k \geq 2$

$$\left(\frac{|\text{disc}(K)| - 24}{4}\right)^k = 21^k \geq 21^2 > 125.$$

By Corollary 5.41 $\alpha^2 + \alpha + 1$ is the fundamental unit.

5.43 Example. The ring of integers of $K = \mathbb{Q}(\sqrt[3]{7})$ is $\mathbb{Z}[\sqrt[3]{7}]$. Put $\alpha = \sqrt[3]{7}$. We have $-1 = \alpha^3 - 8 = (\alpha - 2)(\alpha^2 + 2\alpha + 4)$, so $\alpha - 2$ is a unit and $-(\alpha^2 + 2\alpha + 4)$ is its inverse. Put $\eta = \alpha^2 + 2\alpha + 4$. Then $\eta \in \mathcal{O}_K^*$ and $\eta = \frac{1}{2-\alpha} > 1$. We have $\eta = (\alpha + 1)^2 + 3 < 3^2 + 3 = 12$. For all $k \geq 2$

$$\left(\frac{|\text{disc}(K)| - 24}{4}\right)^k = \left(\frac{1299}{4}\right)^k > 324^k \geq 324^2 > 12^3 > \eta^3.$$

By Corollary 5.41 η is the fundamental unit.

5.44 Example. In Example 5.39 the ideal class group of $K = \mathbb{Q}(\sqrt[3]{11})$ has been computed. Now we compute its group of units. We use the notation of Example 5.39. Put $\eta = \nu^{-1}$. Then η is a unit > 1 . We know already that it is an odd power of the fundamental unit ε . We have

$$\frac{|\text{disc}(K)| - 24}{4} = \frac{27 \cdot 11^2 - 24}{4} = \frac{3243}{4} > 810$$

and (using $\alpha < \frac{9}{4}$)

$$\eta = \frac{3}{(\alpha - 2)^3} = \frac{(\alpha^2 + 2\alpha + 4)^3}{9} = 18\alpha^2 + 40\alpha + 89 < 271$$

and so $\eta^3 < 271^3$. Since $(\frac{|\text{disc}(K)| - 24}{4})^3 > 810^3 > 271^3 > \eta^3$, by Corollary 5.41 $\eta = \varepsilon^k$, where $1 \leq k < 3$. Since k is odd, only $k = 1$ is possible and so $\eta = \varepsilon$.

Cyclotomic fields

Let $m \in \mathbb{N}$ with $m > 2$. The m -th cyclotomic field $\mathbb{Q}(\zeta_m)$ is totally imaginary, i.e. all embeddings are complex. Put $L = \mathbb{Q}(\zeta_m)$. The rank of \mathcal{O}_L^* is by Dirichlet's Unit Theorem equal to $\frac{\varphi(m)}{2} - 1$. Let $K = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$. This field is totally real, all its $\frac{\varphi(m)}{2}$ embeddings are real. So, again by Dirichlet's Unit theorem, the groups \mathcal{O}_K^* and \mathcal{O}_L^* have equal rank. Since they are finitely generated, the index of \mathcal{O}_K^* in \mathcal{O}_L^* is finite and so is the index of $\mathcal{O}_K^* \mu(L)$ in \mathcal{O}_L^* . In fact this index is at most 2. This will be shown for a wider class of extensions. First a useful lemma.

5.45 Lemma. *Let α be an algebraic integer, all of whose conjugates have absolute value 1. Then α is a root of unity.*

PROOF. Let $f = X^n - a_1 X^{n-1} + \dots + (-1)^n a_n \in \mathbb{Z}[X]$ be the minimal polynomial of α over \mathbb{Q} . Then $f = (X - \alpha_1) \cdots (X - \alpha_n)$ with $\alpha_1, \dots, \alpha_n$ the conjugates of α . We have $a_k = s_k^{(n)}(\alpha_1, \dots, \alpha_n)$ for $k = 1, \dots, n$, where $s_k^{(n)}$ is the k -th elementary symmetric polynomial in n variables. The condition $|\alpha_k| = 1$ for $k = 1, \dots, n$ yields a bound for the a_k :

$$|a_k| = |s_k^{(n)}(\alpha_1, \dots, \alpha_n)| \leq s_k^{(n)}(1, \dots, 1) = \binom{n}{k}.$$

It follows that only finitely many algebraic integers of degree $\leq n$ over \mathbb{Q} satisfy the condition in the lemma. So the set of all powers of α is finite. This means that α is of finite order in \mathbb{C}^* , that is α is a root of unity. \square

5.46 Definition. A totally complex number field which is a quadratic extension of a totally real field is called a *CM-field*. (CM stands for Complex Multiplication.)

Let the CM-field L be a quadratic extension of the totally real field K . Then by Dirichlet's Unit Theorem \mathcal{O}_K^* and \mathcal{O}_L^* are finitely generated abelian groups of equal rank. So the index of $\mu(L)\mathcal{O}_K^*$ in \mathcal{O}_L^* is finite.

5.47 Definition. Let L be a CM-field and K the totally real subfield of L with $[L : K] = 2$. The index $(\mathcal{O}_L^* : \mu(L)\mathcal{O}_K^*)$ is called the *Hasse index* or *unit index* of L . Notation: $Q(L)$.

Let $L : \mathbb{Q}$ be a Galois extension and τ the automorphism of L induced by complex conjugation. We assume that τ is of order 2—so L has only complex embeddings—and also that τ is central in $\text{Gal}(L : \mathbb{Q})$. This last condition implies that $K := L^\tau$ is totally real. So L is a CM-field with the property that $L : \mathbb{Q}$ is a Galois extension. For each $\nu \in \mathcal{O}_L^*$ and all $\sigma \in \text{Gal}(L : \mathbb{Q})$

$$\left| \sigma \left(\frac{\nu}{\tau(\nu)} \right) \right| = \frac{|\sigma(\nu)|}{|\sigma\tau(\nu)|} = \frac{|\sigma(\nu)|}{|\tau\sigma(\nu)|} = 1.$$

By Lemma 5.45 we have $\frac{\nu}{\tau(\nu)} \in \mu(L)$. Thus we have a map

$$f : \mathcal{O}_L^* \rightarrow \mu(L), \quad \nu \mapsto \frac{\nu}{\tau(\nu)}.$$

This map clearly is a group homomorphism.

5.48 Proposition. Let L be a CM-field such that $L : \mathbb{Q}$ be a Galois extension and let $K = L^\tau$, where τ is induced by complex conjugation. Then

$$\mu(L)\mathcal{O}_K^* = \left\{ \nu \in \mathcal{O}_L^* \mid \frac{\nu}{\tau(\nu)} \in \mu(L)^2 \right\}$$

and hence $Q(L) \leq 2$.

PROOF. We show that the kernel of the homomorphism $f' : \mathcal{O}_L^* \rightarrow \mu(L)/\mu(L)^2$ induced by f as described above is the group $\mu(L)\mathcal{O}_K^*$. Clearly $\mu(L)$ and \mathcal{O}_K^* are contained in the kernel of f' . Let $\nu \in \text{Ker}(f')$, that is $\frac{\nu}{\tau(\nu)} \in \mu(L)^2$, say $\frac{\nu}{\tau(\nu)} = \zeta^2$ for a $\zeta \in \mu(L)$. Then $\frac{\nu}{\zeta} = \tau\left(\frac{\nu}{\zeta}\right)$ and so $\frac{\nu}{\zeta} \in \mathcal{O}_K^*$. Since $\mu(L)/\mu(L)^2$ is of order 2, it follows that $Q(L) \leq 2$. \square

Here we considered CM-fields which are Galois extensions of \mathbb{Q} . with a little more effort it can be shown that this proposition holds in fact for CM-fields in general.

5.49 Example. The biquadratic number field $K = \mathbb{Q}(\sqrt{-2}, \sqrt{3})$ is a CM-field. Its real subfield is the quadratic number field $\mathbb{Q}(\sqrt{3})$. From the computation of \mathcal{O}_K^* in Example 5.37 follows that $Q(K) = 2$.

We compute the Hasse index of a cyclotomic field $\mathbb{Q}(\zeta_m)$ with $m > 2$. It is a CM-field with $\mathbb{Q}(\zeta_m + \zeta_m^{-1})$ as its totally real subfield. For m not a prime power we will use the following Lemma.

5.50 Lemma. Let $m \in \mathbb{N}^*$ be not a prime power. Then $1 - \zeta_m \in \mathbb{Z}[\zeta_m]^*$.

PROOF. For each $k \in \mathbb{N}^*$ the cyclotomic polynomial Φ_k is the minimal polynomial of ζ_k over \mathbb{Q} . We will prove that $\Phi_m(1) = \pm 1$ and so $N_{\mathbb{Q}(\zeta_m)}^{\mathbb{Q}}(1 - \zeta_m) = \pm 1$.

Let $r(k)$ denote the number of prime divisors of $k \in \mathbb{N}^*$. We have $X^m - 1 = \prod_{d|m} \Phi_d(X)$ and write this as follows

$$\frac{X^m - 1}{X - 1} = \prod_{\substack{d|m \\ r(d)=1}} \Phi_d(X) \cdot \prod_{\substack{d|m \\ r(d)>1}} \Phi_d(X).$$

So for the values in 1:

$$m = \prod_{\substack{d|m \\ r(d)=1}} \Phi_d(1) \cdot \prod_{\substack{d|m \\ r(d)>1}} \Phi_d(1) = \prod_{p|m} p^{v_p(m)} \cdot \prod_{\substack{d|m \\ r(d)>1}} \Phi_d(1) = m \cdot \prod_{\substack{d|m \\ r(d)>1}} \Phi_d(1).$$

It follows that $\Phi_m(1) = \pm 1$. □

In fact $\Phi_m(1) = 1$ if m is not a prime power, because the norm of a nonreal algebraic integer is positive. It also follows by induction from the product given in the proof of this lemma.

5.51 Theorem. *Let $m \in \mathbb{N}$ with $m > 2$ and $m \not\equiv 2 \pmod{4}$. Then*

$$Q(\mathbb{Q}(\zeta_m)) = \begin{cases} 1 & \text{if } m \text{ is a prime power,} \\ 2 & \text{otherwise.} \end{cases}$$

PROOF. Put $L = \mathbb{Q}(\zeta_m)$ and $K = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$. We distinguish three cases.

Case 1: m is a power of an odd prime p . Let $\nu \in \mathcal{O}_L^*$. We have to show that $\frac{\nu}{\tau(\nu)} \in \mu(L)^2$. Put $\nu = a_0 + a_1\zeta_m + \cdots + a_{n-1}\zeta_m^{n-1}$, where $n = \varphi(m)$ and $a_0, \dots, a_{n-1} \in \mathbb{Z}$. We have $\nu \equiv a_0 + \cdots + a_{n-1} \pmod{1 - \zeta_m}$. Also $\tau(\nu) = a_0 + a_1\zeta_m^{-1} + \cdots + a_{n-1}\zeta_m^{-(n-1)} \equiv a_0 + \cdots + a_{n-1} \pmod{1 - \zeta_m}$. So $\frac{\nu}{\tau(\nu)} \equiv 1 \pmod{1 - \zeta_m}$. On the other hand $\frac{\nu}{\tau(\nu)} \in \mu(L) = \langle -\zeta_m \rangle$. Since $\frac{\nu}{\tau(\nu)} \equiv 1 \pmod{1 - \zeta_m}$, it follows that $\frac{\nu}{\tau(\nu)} \in \langle \zeta_m \rangle = \mu(L)^2$.

Case 2: m is a power of 2, say $m = 2^r$ with $r \geq 2$. Let $\nu \in \mathcal{O}_L^*$. Suppose that $\frac{\nu}{\tau(\nu)} \notin \mu(L)^2$. We have $\mu(L) = \langle \zeta_{2^r} \rangle$ and $\mu(L)^2 = \langle \zeta_{2^{r-1}} \rangle$, so $\frac{\nu}{\tau(\nu)}$ is a primitive m -th root of unity. Since $N_{\mathbb{Q}(\zeta_{2^k})}^{\mathbb{Q}(\zeta_{2^{k-1}})}(\zeta_{2^k}) = \zeta_{2^{k-1}}$ for $k = 2, \dots, r$, we have $N_{\mathbb{Q}(i)}^{\mathbb{Q}(\zeta_{2^r})}(\zeta_{2^r}) = i$. But $N_{\mathbb{Q}(i)}^{\mathbb{Q}(\zeta_m)}(\nu)$ is a unit of $\mathbb{Z}[i]$, say $N_{\mathbb{Q}(i)}^{\mathbb{Q}(\zeta_m)}(\nu) = i^t$. Then $N_{\mathbb{Q}(i)}^{\mathbb{Q}(\zeta_m)}\left(\frac{\nu}{\tau(\nu)}\right) = \frac{i^t}{i^{-t}} = i^{2t} = (-1)^t \neq i$. Contradiction. So also in this case $\frac{\nu}{\tau(\nu)} \in \mu(L)^2$.

Case 3: m is not a prime power. By Lemma 5.50 we have $1 - \zeta_m \in \mathcal{O}_L^*$. The homomorphism $f: \mathcal{O}_L^* \rightarrow \mu(L)$ maps this unit to

$$\frac{1 - \zeta_m}{\tau(1 - \zeta_m)} = \frac{1 - \zeta_m}{1 - \zeta_m^{-1}} = -\zeta_m^{-1}.$$

Since $-\zeta_m^{-1}$ generates $\mu(L)$, the homomorphism f is surjective. □

5.5 Regulators

Let K be a number field of degree n with r real embeddings $\sigma_1, \dots, \sigma_r$ and s pairs $\{\tau_1, \bar{\tau}_1\}, \dots, \{\tau_s, \bar{\tau}_s\}$ of complex embeddings. By Proposition 5.34 the image of

$$\psi: \mathcal{O}_K^* \rightarrow \mathbb{R}^{r+s}, \quad \varepsilon \mapsto l(\varepsilon)$$

is a lattice in the subspace H_{r+s} of \mathbb{R}^{r+s} . We consider \mathbb{R}^{r+s} to be the standard Euclidean space of dimension $r + s$ and equipped with the standard Lebesgue measure vol . Moreover, H_{r+s} is a Euclidean subspace of dimension $r + s - 1$. Let $(\varepsilon_1, \dots, \varepsilon_{r+s-1})$ be a system of units. Then $(\psi(\varepsilon_1), \dots, \psi(\varepsilon_{r+s-1}))$ is a basis of H_{r+s} if and only if $\langle \varepsilon_1, \dots, \varepsilon_{r+s-1} \rangle$ is a free abelian group of rank $r + s - 1$, or equivalently, if and only if this group is of finite index in \mathcal{O}_K^* . It is a fundamental system of units if and only if $(\psi(\varepsilon_1), \dots, \psi(\varepsilon_{r+s-1}))$ is a \mathbb{Z} -basis of the lattice $\psi(\mathcal{O}_K^*)$ in H_{r+s} . If $\langle \varepsilon_1, \dots, \varepsilon_{r+s-1} \rangle$ is of rank $r + s - 1$, the volume of a mesh of $\psi(\mathcal{O}_K^*)$ is equal to the volume of the parallelotope in \mathbb{R}^{r+s} spanned by

$$(\psi(\varepsilon_1), \dots, \psi(\varepsilon_{r+s-1}), v),$$

where $v = \frac{1}{\sqrt{r+s}}(1, \dots, 1)$, a vector of length 1 perpendicular to H_{r+s} . Thus this volume is the absolute value of

$$\begin{vmatrix} \log |\sigma_1(\varepsilon_1)| & \cdots & \log |\sigma_r(\varepsilon_1)| & 2 \log |\tau_1(\varepsilon_1)| & \cdots & 2 \log |\tau_s(\varepsilon_1)| \\ \log |\sigma_1(\varepsilon_2)| & \cdots & \log |\sigma_r(\varepsilon_2)| & 2 \log |\tau_1(\varepsilon_2)| & \cdots & 2 \log |\tau_s(\varepsilon_2)| \\ \vdots & & \vdots & \vdots & & \vdots \\ \vdots & & \vdots & \vdots & & \vdots \\ \log |\sigma_1(\varepsilon_{r+s-1})| & \cdots & \log |\sigma_r(\varepsilon_{r+s-1})| & 2 \log |\tau_1(\varepsilon_{r+s-1})| & \cdots & 2 \log |\tau_s(\varepsilon_{r+s-1})| \\ \frac{1}{\sqrt{r+s}} & \cdots & \frac{1}{\sqrt{r+s}} & \frac{1}{\sqrt{r+s}} & \cdots & \frac{1}{\sqrt{r+s}} \end{vmatrix}.$$

The sum of the column vectors is $\begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ \sqrt{r+s} \end{pmatrix}$, so the volume equals $\sqrt{r+s}$ times

the absolute value of the determinant of any of the $(r + s - 1) \times (r + s - 1)$ -minors

of the matrix

$$\begin{pmatrix} \log |\sigma_1(\varepsilon_1)| & \cdots & \log |\sigma_r(\varepsilon_1)| & 2 \log |\tau_1(\varepsilon_1)| & \cdots & 2 \log |\tau_s(\varepsilon_1)| \\ \log |\sigma_1(\varepsilon_2)| & \cdots & \log |\sigma_r(\varepsilon_2)| & 2 \log |\tau_1(\varepsilon_2)| & \cdots & 2 \log |\tau_s(\varepsilon_2)| \\ \vdots & & \vdots & \vdots & & \vdots \\ \vdots & & \vdots & \vdots & & \vdots \\ \log |\sigma_1(\varepsilon_{r+s-1})| & \cdots & \log |\sigma_r(\varepsilon_{r+s-1})| & 2 \log |\tau_1(\varepsilon_{r+s-1})| & \cdots & 2 \log |\tau_s(\varepsilon_{r+s-1})| \end{pmatrix}.$$

5.52 Definition. The absolute value of the determinant of an $(r+s-1) \times (r+s-1)$ -minor of the above matrix is called the *regulator* of $\langle \varepsilon_1, \dots, \varepsilon_{r+s-1} \rangle$. Notation: $\text{Reg}(\varepsilon_1, \dots, \varepsilon_{r+s-1})$. For $(\varepsilon_1, \dots, \varepsilon_{r+s-1})$ a fundamental system of units this number is called the *regulator* of the number field K . The notation for this number is $\text{Reg}(K)$. More generally, for X a subgroup of \mathcal{O}_K^* of finite index we define the *regulator* of X as the regulator of a maximal free subgroup of X . It is denoted by $\text{Reg}(X)$.

So by definition of the regulator:

$$\delta(\psi(X)) = \sqrt{r+s} \cdot \text{Reg}(X).$$

In particular

$$\delta(\psi(\mathcal{O}_K^*)) = \sqrt{r+s} \cdot \text{Reg}(K)$$

and we have

$$\text{Reg}(X) = (\psi(\mathcal{O}_K^*) : \psi(X)) \cdot \text{Reg}(K).$$

Alternatively, $\text{Reg}(\varepsilon_1, \dots, \varepsilon_{r+s-1})$ can be defined more symmetrically as the absolute value of

$$\begin{vmatrix} \log |\sigma_1(\varepsilon_1)| & \cdots & \log |\sigma_r(\varepsilon_1)| & 2 \log |\tau_1(\varepsilon_1)| & \cdots & 2 \log |\tau_s(\varepsilon_1)| \\ \log |\sigma_1(\varepsilon_2)| & \cdots & \log |\sigma_r(\varepsilon_2)| & 2 \log |\tau_1(\varepsilon_2)| & \cdots & 2 \log |\tau_s(\varepsilon_2)| \\ \vdots & & \vdots & \vdots & & \vdots \\ \vdots & & \vdots & \vdots & & \vdots \\ \log |\sigma_1(\varepsilon_{r+s-1})| & \cdots & \log |\sigma_r(\varepsilon_{r+s-1})| & 2 \log |\tau_1(\varepsilon_{r+s-1})| & \cdots & 2 \log |\tau_s(\varepsilon_{r+s-1})| \\ \frac{1}{n} & \cdots & \frac{1}{n} & \frac{2}{n} & \cdots & \frac{2}{n} \end{vmatrix}.$$

By analytic methods (chapter 8) so-called class number formulas are derived. These formulas are in fact formulas for $h(K) \text{Reg}(K)$, the product of the class number $h(K) = \#(\mathcal{C}(K))$ and the regulator of a number field K .

5.53 Examples.

1. The regulator of \mathbb{Q} and also of imaginary quadratic number fields is the determinant of a 0×0 -matrix, which is taken to be equal to 1.
2. The regulator of a real quadratic number field equals the absolute value of the logarithm of the fundamental unit. The same holds for cubic fields with one real embedding.

EXERCISES

1. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{-3})$. Show that \mathcal{O}_K is a principal ideal domain.
2. Show that $\mathbb{Z}[\zeta_7 + \zeta_7^{-1}]$ is a principal ideal domain.
3. Let $\alpha \in \mathbb{R}$ be such that $\alpha^3 = \alpha + 7$. Show that $\mathbb{Z}[\alpha]$ is a principal ideal domain.
4. Let $K = \mathbb{Q}(\sqrt[3]{17})$. Show that \mathcal{O}_K is a principal ideal domain.
5. Let $K = \mathbb{Q}(\sqrt[3]{19})$. Compute $\mathcal{C}(K)$.
6. Prove that $\mathbb{Z}[\zeta_9]$ and $\mathbb{Z}[\zeta_9 + \zeta_9^{-1}]$ are principal ideal domains.
7. Let K be a number field.
 - (i) Let \mathfrak{a} be a nonzero ideal of \mathcal{O}_K and m be the order of $[\mathfrak{a}]$ in $\mathcal{C}(K)$. Then \mathfrak{a}^m is a principal ideal of \mathcal{O}_K , say $\mathfrak{a}^m = \alpha \mathcal{O}_K$. Put $L = K(\sqrt[m]{\alpha})$. Show that $\mathfrak{a} \mathcal{O}_L$ is a principal ideal of \mathcal{O}_L .
 - (ii) Show that there is a finite extension $L : K$ such that $\mathfrak{a} \mathcal{O}_L$ is principal for every ideal \mathfrak{a} of \mathcal{O}_K .
 - (iii) Let $K = \mathbb{Q}(\sqrt{-21})$. Find a finite extension $L : K$ such that $\mathfrak{a} \mathcal{O}_L$ is principal for every ideal \mathfrak{a} of \mathcal{O}_K .
8. Let $K = \mathbb{Q}(\alpha)$, where $\alpha \in \mathbb{C}$ such that $\alpha^4 + 4\alpha^2 + 2 = 0$. Compute

$$\mathcal{O}_K, \quad \mathcal{C}(\mathcal{O}_K), \quad \mathcal{O}_K^* \quad \text{and} \quad \text{Reg}(K).$$

9. Compute $\mathbb{Z}[\zeta_5]^*$.
10. Let $K = \mathbb{Q}(i, \sqrt{6})$. Put $\alpha = \frac{\sqrt{6} + \sqrt{-6}}{2}$.
 - (i) Show that the set $\{(5, \sigma(\alpha) + 1) \mid \sigma \in \text{Gal}(K : \mathbb{Q})\}$ consists of all four prime ideals above 5.
 - (ii) Compute $\mathcal{C}(K)$.
 - (iii) Show that $(i + 1) = (2 + \sqrt{6}) = (2, \sqrt{-6})$, the ideals being ideals of \mathcal{O}_K .
 - (iv) Compute \mathcal{O}_K^* and $\text{Reg}(K)$.
11. Compute the fundamental unit of $\mathbb{Q}(\sqrt[3]{3})$.
12. Let $\alpha \in \mathbb{R}$ be such that $\alpha^3 + \alpha - 3 = 0$. Compute the fundamental unit of $\mathbb{Q}(\alpha)$.
13. Let $\alpha \in \mathbb{R}$ be such that $\alpha^3 - 2\alpha + 3 = 0$. Compute the fundamental unit of $\mathbb{Q}(\alpha)$.
14. Let $K = \mathbb{Q}(\vartheta)$, where $\vartheta = \zeta_7 + \zeta_7^{-1}$.
 - (i) Show that ϑ and $\vartheta - 1$ are units of $\mathbb{Z}[\vartheta]$.
 - (ii) What is the image of $\mathbb{Z}[\vartheta]^*$ in $(\mathbb{Z}[\vartheta]/(13))^*$?
 - (iii) Show that the index of $\langle \vartheta, \vartheta - 1 \rangle$ in $\mathbb{Z}[\vartheta]^*$ is finite.

5 Geometric Methods

15. Show that the alternative definition of the regulator on page 128 agrees with the definition given in Definition 5.52.
16. Let L be a CM-field and K its maximal real subfield. Show that $Q(L) \operatorname{Reg}(L) = 2^r \operatorname{Reg}(K)$, where $r = [K : \mathbb{Q}] - 1$.

6 Localization of Dedekind Domains

In commutative algebra localization forces given elements of a commutative ring to become invertible. In section 6.3 for Dedekind domains a slightly more general type of localization is described. The idea is to force maximal ideals to become the unit ideal. For its formalization discrete valuations are used. A first application of localization is a description of residue class rings of a Dedekind domain. In the last section some terminology is introduced for the case of rings of integers of number fields.

6.1 Discrete valuations

6.1 Definition. Let K be a field. A surjective group homomorphism $v: K^* \rightarrow \mathbb{Z}$ is called a *discrete valuation* on K if

$$v(a + b) \geq \min(v(a), v(b)) \quad \text{for all } a, b \in K.$$

Here it is understood that $v(0) = \infty$ and that $\infty \geq n$ for all $n \in \mathbb{Z}$. So v is actually seen as being a map $K \rightarrow \mathbb{Z} \cup \{\infty\}$.

Each maximal ideal of a Dedekind domain determines a discrete valuation on its field of fractions:

6.2 Proposition. Let R be a Dedekind domain, K its field of fractions and $\mathfrak{p} \in \text{Max}(R)$. The \mathfrak{p} -adic valuation $v_{\mathfrak{p}}: K^* \rightarrow \mathbb{Z}$, defined in Definition 2.37, is a discrete valuation on K .

PROOF. Since $\mathfrak{p}^2 \neq \mathfrak{p}$, there is a $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$. So the group homomorphism $v_{\mathfrak{p}}$ is surjective: $v_{\mathfrak{p}}(\pi) = 1$. Let $a, b \in K^*$ such that $a + b \neq 0$. There is a nonzero $c \in R$ such that $ca, cb \in R$. Then

$$(ca + cb)R \subseteq caR + cbR.$$

Hence by Proposition 2.14

$$\begin{aligned} v_{\mathfrak{p}}(c) + v_{\mathfrak{p}}(a + b) &= v_{\mathfrak{p}}(c(a + b)) = v_{\mathfrak{p}}((ca + cb)R) \geq v_{\mathfrak{p}}(caR + cbR) \\ &= \min(v_{\mathfrak{p}}(caR), v_{\mathfrak{p}}(cbR)) = \min(v_{\mathfrak{p}}(c) + v_{\mathfrak{p}}(a), v_{\mathfrak{p}}(c) + v_{\mathfrak{p}}(b)) \\ &= v_{\mathfrak{p}}(c) + \min(v_{\mathfrak{p}}(a), v_{\mathfrak{p}}(b)). \end{aligned}$$

So $v_{\mathfrak{p}}(a + b) \geq \min(v_{\mathfrak{p}}(a), v_{\mathfrak{p}}(b))$. If one of the elements a , b and $a + b$ equals 0, then this inequality is trivially true. \square

The \mathfrak{p} -adic valuation of an element is by definition the \mathfrak{p} -adic valuation of the fractional ideal it generates. On the other hand the \mathfrak{p} -adic valuation of a fractional ideal is determined by the \mathfrak{p} -adic valuations of its elements.

6.3 Proposition. *Let R be a Dedekind domain, K its field of fractions, $\mathfrak{p} \in \text{Max}(R)$ and $\mathfrak{a} \in \mathbb{I}(R)$. Then*

$$v_{\mathfrak{p}}(\mathfrak{a}) = \min_{a \in \mathfrak{a}} v_{\mathfrak{p}}(a).$$

PROOF. We can assume that $\mathfrak{a} \in \mathbb{I}^+(R)$. Clearly, $v_{\mathfrak{p}}(\mathfrak{a}) \leq v_{\mathfrak{p}}(a)$ for all $a \in \mathfrak{a}$. By Proposition 2.28 there is an ideal \mathfrak{b} in the inverse of the class of \mathfrak{a} such that \mathfrak{b} and $\mathfrak{p}\mathfrak{a}$ are comaximal. Then $\mathfrak{a}\mathfrak{b} = cR$ for a $c \in \mathfrak{a}$ and, since $v_{\mathfrak{p}}(\mathfrak{b}) = 0$, we have $v_{\mathfrak{p}}(\mathfrak{a}) = v_{\mathfrak{p}}(\mathfrak{a}\mathfrak{b}) = v_{\mathfrak{p}}(cR) = v_{\mathfrak{p}}(c)$. \square

6.4 Proposition. *Let R be a Dedekind domain with field of fractions K . Then*

$$R = \{a \in K \mid v_{\mathfrak{p}}(a) \geq 0 \text{ for all } \mathfrak{p} \in \text{Max}(R)\}.$$

and

$$R^* = \{a \in K \mid v_{\mathfrak{p}}(a) = 0 \text{ for all } \mathfrak{p} \in \text{Max}(R)\}.$$

PROOF. Because R is integrally closed and Noetherian, we have

$$R = \{a \in K \mid aR \subseteq R\} \quad \text{and} \quad R^* = \{a \in K \mid aR = R\}. \quad \square$$

6.5 Proposition. *Let v be a discrete valuation on a field K . Then the valuation ring*

$$R_v := \{a \in K \mid v(a) \geq 0\}$$

is a local subring of K .

PROOF. From the definition of discrete valuation it follows that R_v is a subring of K and that the set $\mathfrak{m} = \{a \in K \mid v(a) > 0\}$ is an ideal of R_v . Since $R_v \setminus \mathfrak{m} = R_v^*$, it is a local ring with maximal ideal \mathfrak{m} . \square

6.6 Corollary. *Let v be a discrete valuation on a field K and $a, b \in K$ such that $v(a) \neq v(b)$. Then*

$$v(a + b) = \min(v(a), v(b)).$$

PROOF. Let R_v and \mathfrak{m} be as in the proposition. Suppose that $v(a) < v(b)$. Then $a \neq 0$ and $v(a + b) = v(a)v(1 + \frac{b}{a}) = v(a)$, because $1 + \frac{b}{a} \in R_v \setminus \mathfrak{m} = R_v^*$. \square

6.7 Definition. An integral domain R_v as in Proposition 6.5 is called a *discrete valuation ring*.

A more intrinsic characterization of a discrete valuation ring is given by:

6.8 Proposition. *Let R be a local integral domain with maximal ideal \mathfrak{m} . Then the following are equivalent:*

- a) R is a discrete valuation ring;
- b) R is a principal ideal domain;
- c) R is a Dedekind domain.

PROOF.

- a) \Rightarrow b) Let v be a discrete valuation on a field K such that $R = R_v$. Let \mathfrak{a} be a nonzero ideal of R . Put $k = \min_{a \in \mathfrak{a}} v(a)$ and let $a_0 \in \mathfrak{a}$ such that $v(a_0) = k$. Then for all nonzero $a \in \mathfrak{a}$ we have $v(\frac{a}{a_0}) = v(a) - v(a_0) \geq 0$ and so $\frac{a}{a_0} \in R$. It follows that $a \in a_0 R$ for all $a \in \mathfrak{a}$. Since $a_0 \in \mathfrak{a}$, we have $\mathfrak{a} = a_0 R$.
- b) \Rightarrow c) Principal ideal domains are Dedekind domains.
- c) \Rightarrow a) Let K be the field of fractions of R . The maximal ideal \mathfrak{m} determines the discrete valuation $v_{\mathfrak{m}}$ on K . By Proposition 6.4 we have that R is the valuation ring of $v_{\mathfrak{m}}$. \square

So an alternative definition for ‘discrete valuation ring’ is: a discrete valuation ring is a local Dedekind domain.

The monoid $\mathbb{I}^+(R)$ of nonzero ideals of a discrete valuation ring is isomorphic to the additive monoid \mathbb{N} : if \mathfrak{p} is the unique maximal ideal, then the nonzero ideals are $\mathfrak{p}^0 (= R)$, $\mathfrak{p}^1 (= \mathfrak{p})$, \mathfrak{p}^2 , \mathfrak{p}^3 , \dots . They are all principal: $\mathfrak{p}^n = (a)$ for any $a \in R$ with $v(a) = n$. In particular, if $\pi \in R$ satisfies $v(\pi) = 1$, then $\mathfrak{p}^n = (\pi^n)$.

6.9 Definition. Let v be a discrete valuation of a field K and let $\pi \in K$ satisfy $v(\pi) = 1$. Then π is called a *uniformizer* of the discrete valuation v .

So the uniformizer of a discrete valuation generates the unique maximal ideal of its valuation ring.

6.2 Localization at a prime ideal

In commutative algebra we have the notion of localization. Here we consider only localization for integral domains.

6.10 Definition. Let R be an integral domain. A *multiplicative system* in R is a submonoid of the multiplicative monoid $R \setminus \{0\}$. I.e. a multiplicative system is a subset of $R \setminus \{0\}$ which is closed under multiplication and contains 1.

For S a multiplicative system in an integral domain R with field of fractions K we can extend R by allowing elements of S as denominators. This yields the ring

$$S^{-1}R = \left\{ \frac{a}{s} \mid a \in R \text{ and } s \in S \right\}.$$

It is a subring of K and since $R \subseteq S^{-1}R \subseteq K$, the field K is the field of fractions of $S^{-1}R$ as well.

6.11 Examples. Let R be an integral domain. Examples of multiplicative systems in R :

- a) Submonoids S of the group R^* . For such S it is clear that $S^{-1}R = R$.
- b) $S = R \setminus \{0\}$. The ring $S^{-1}R$ is the field of fractions of R .
- c) Let \mathfrak{p} be a prime ideal of R . Then $S = R \setminus \mathfrak{p}$ is a multiplicative system by definition of prime ideals.

Let's have a closer look at the last example.

6.12 Definition and notation. Let R be an integral domain, \mathfrak{p} a prime ideal of R and $S = R \setminus \mathfrak{p}$. Then the ring $S^{-1}R$ is called the *localization* of R at \mathfrak{p} . Notation: $S^{-1}R = R_{\mathfrak{p}}$.

The localization at a prime ideal is a local ring:

6.13 Proposition. *Let R be an integral domain, \mathfrak{p} a prime ideal of R . Then:*

- (i) $\mathfrak{a}R_{\mathfrak{p}} = \left\{ \frac{a}{s} \mid a \in \mathfrak{a} \text{ and } s \notin \mathfrak{p} \right\}$ for each ideal \mathfrak{a} of R ;
- (ii) $R_{\mathfrak{p}}$ is a local ring with maximal ideal $\mathfrak{p}R_{\mathfrak{p}}$;
- (iii) $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$ is the field of fractions of R/\mathfrak{p} .

PROOF.

- (i) Obviously, $\frac{a}{s} = a \cdot \frac{1}{s} \in \mathfrak{a}R_{\mathfrak{p}}$. The extended ideal $\mathfrak{a}R_{\mathfrak{p}}$ consists of finite sums of elements $a \frac{r}{s}$ with $a \in \mathfrak{a}$, $r \in R$ and $s \notin \mathfrak{p}$. Such a sum clearly is equal to an $\frac{a}{s}$ with $a \in \mathfrak{a}$ and $s \notin \mathfrak{p}$.
- (ii) From (i) it follows that

$$R_{\mathfrak{p}} \setminus \mathfrak{p}R_{\mathfrak{p}} = \left\{ \frac{t}{s} \mid t, s \notin \mathfrak{p} \right\} = (R_{\mathfrak{p}})^*.$$

This implies that $\mathfrak{p}R_{\mathfrak{p}}$ is the unique maximal ideal of the ring $R_{\mathfrak{p}}$.

- (iii) The inclusion $R \subseteq R_{\mathfrak{p}}$ induces a ring homomorphism

$$R/\mathfrak{p} \longrightarrow R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}.$$

From $\mathfrak{p}R_{\mathfrak{p}} \cap R = \mathfrak{p}$ follows that we have an embedding of the integral domain R/\mathfrak{p} in the field $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$. An element of this field represented by $\frac{r}{s}$ is the quotient of the images of the classes represented by r and s . \square

For Dedekind domains the localization at a maximal ideal is a discrete valuation ring:

6.14 Proposition. *Let R be a Dedekind domain, $\mathfrak{p} \in \text{Max}(R)$ and K the field of fractions of R . Then $R_{\mathfrak{p}}$ is the valuation ring of the discrete valuation $v_{\mathfrak{p}}$ of K . Moreover, the inclusion $R \subseteq R_{\mathfrak{p}}$ induces an isomorphism $R/\mathfrak{p} \xrightarrow{\sim} R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$.*

PROOF. For $r \in R$ and $s \notin \mathfrak{p}$ we have $v_{\mathfrak{p}}(\frac{r}{s}) = v_{\mathfrak{p}}(r) \geq 0$. So the localization at \mathfrak{p} is contained in the valuation ring of $v_{\mathfrak{p}}$. Let $x \in K^*$ be in the valuation ring of $v_{\mathfrak{p}}$. For the fractional ideal xR we have $xR = \mathfrak{a}\mathfrak{b}^{-1}$, where \mathfrak{a} and \mathfrak{b} are nonzero ideals of R and we may assume that $\mathfrak{p} \nmid \mathfrak{b}$. Take $b \in \mathfrak{b} \setminus \mathfrak{p}$. Then $bR = \mathfrak{b}\mathfrak{c}$ for an ideal \mathfrak{c} of R . We have $\mathfrak{a}\mathfrak{c} = \mathfrak{a}\mathfrak{b}\mathfrak{b}^{-1} = bxR$. So $bx \in R$ and $xR = \mathfrak{a}\mathfrak{b}^{-1} = \mathfrak{a}\mathfrak{c}(\mathfrak{b}\mathfrak{c})^{-1} = \frac{bx}{b}R$. Hence $x \in R_{\mathfrak{p}}$. Since R/\mathfrak{p} is a field, the last assertion follows from Proposition 6.13(iii). \square

So the localization of a Dedekind domain at a prime ideal is a discrete valuation ring; it is a local Dedekind domain. We will show that, conversely, a Noetherian domain for which the localizations at the maximal ideals are discrete valuation rings is a Dedekind domain. This is another characterization of Dedekind domains.

6.15 Lemma. *Let R be an integral domain. Then $R = \bigcap_{\mathfrak{m} \in \text{Max}(R)} R_{\mathfrak{m}}$.*

PROOF. Clearly, $R \subseteq \bigcap_{\mathfrak{m} \in \text{Max}(R)} R_{\mathfrak{m}}$. Let $x \in \bigcap_{\mathfrak{m} \in \text{Max}(R)} R_{\mathfrak{m}}$. To prove that $x \in R$. We will assume that $x \neq 0$. Consider the ideal $\mathfrak{b} = \{b \in R \mid bx \in R\}$. We will prove that $\mathfrak{b} = R$. Let $\mathfrak{m} \in \text{Max}(R)$. Because $x \in R_{\mathfrak{m}}$, there exists a $b \in R \setminus \mathfrak{m}$ such that $bx \in R$, that is $(R \setminus \mathfrak{m}) \cap \mathfrak{b} \neq \emptyset$ and this means that $\mathfrak{b} \not\subseteq \mathfrak{m}$. This holds for all $\mathfrak{m} \in \text{Max}(R)$. So $\mathfrak{b} = R$. \square

6.16 Theorem. *Let R be a Noetherian integral domain. Then R is a Dedekind domain if and only if $R_{\mathfrak{m}}$ is a discrete valuation ring for all $\mathfrak{m} \in \text{Max}(R)$.*

PROOF. By Proposition 6.14 and Theorem 2.43 it remains to prove that if $R_{\mathfrak{m}}$ is a discrete valuation ring for all maximal ideals of R , the ring R is integrally closed and that nonzero prime ideals are maximal. So assume that all localizations $R_{\mathfrak{m}}$ are discrete valuation rings. First we prove that R is integrally closed. Let $a \in K^*$ be integral over R . Then a is integral over $R_{\mathfrak{m}}$ for all maximal ideals of R . Discrete valuation rings are integrally closed, so $a \in \bigcap_{\mathfrak{m} \in \text{Max}(R)} R_{\mathfrak{m}}$. By Lemma 6.15 we have $a \in R$. This means that R is integrally closed.

Let \mathfrak{p} be a nonzero prime ideal of R and \mathfrak{m} a maximal ideal such that $\mathfrak{m} \supseteq \mathfrak{p}$. Then $\mathfrak{p}R_{\mathfrak{m}}$ is a prime ideal of $R_{\mathfrak{m}}$: if $\frac{a}{s} \cdot \frac{b}{t} = \frac{c}{u}$ with $a, b \in R, c \in \mathfrak{p}$ and $s, t, u \in R \setminus \mathfrak{m}$, then $abu = cst \in \mathfrak{p}$ and so $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. The ideal $\mathfrak{m}R_{\mathfrak{m}}$ is the unique prime ideal of the discrete valuation domain $R_{\mathfrak{m}}$. It follows that $\mathfrak{p}R_{\mathfrak{m}} = \mathfrak{m}R_{\mathfrak{m}}$. Let $a \in \mathfrak{m}$. Then $a \in \mathfrak{p}R_{\mathfrak{m}}$, so $a = \frac{b}{s}$ with $b \in \mathfrak{p}$ and $s \in R \setminus \mathfrak{m}$. From $as = b \in \mathfrak{p}$ and $s \notin \mathfrak{p}$ follows that $a \in \mathfrak{p}$. Hence $\mathfrak{p} = \mathfrak{m}$. So the nonzero prime ideal \mathfrak{p} is a maximal ideal. \square

We will have a closer look at the residue class ring R/\mathfrak{a} of a nonzero ideal \mathfrak{a} of a Dedekind domain R . The Chinese Remainder Theorem implies that we can focus on the case of \mathfrak{a} being the power of a maximal ideal: if $\mathfrak{a} = \mathfrak{p}_1^{k_1} \cdots \mathfrak{p}_r^{k_r}$ with $\mathfrak{p}_1, \dots, \mathfrak{p}_r$

different maximal ideals and $k_1, \dots, k_r \in \mathbb{N}^*$, then the maps $R \rightarrow R/\mathfrak{p}_i^{k_i}$ induce an isomorphism

$$R/\mathfrak{a} \xrightarrow{\sim} R/\mathfrak{p}_1^{k_1} \times \cdots \times R/\mathfrak{p}_r^{k_r}.$$

So we consider R/\mathfrak{p}^k for R a Dedekind domain, $\mathfrak{p} \in \text{Max}(R)$ and $k \in \mathbb{N}^*$. We will construct a convenient system of representatives of R/\mathfrak{p}^k .

6.17 Proposition. *Let R be a Dedekind domain, \mathfrak{p} a maximal ideal of R and $k \in \mathbb{N}^*$. Then inclusion $R \rightarrow R_{\mathfrak{p}}$ induces an isomorphism $R/\mathfrak{p}^k \xrightarrow{\sim} R_{\mathfrak{p}}/(\mathfrak{p}R_{\mathfrak{p}})^k$.*

PROOF. The induced ring homomorphism $R/\mathfrak{p}^k \rightarrow R_{\mathfrak{p}}/(\mathfrak{p}R_{\mathfrak{p}})^k$ is an isomorphism if and only if $R \cap (\mathfrak{p}R_{\mathfrak{p}})^k = \mathfrak{p}^k$ and $R + (\mathfrak{p}R_{\mathfrak{p}})^k = R_{\mathfrak{p}}$. The first identity follows from

$$R \cap (\mathfrak{p}R_{\mathfrak{p}})^k = R \cap \{x \in K \mid v_{\mathfrak{p}}(x) \geq k\} = \{x \in R \mid v_{\mathfrak{p}}(x) \geq k\}$$

and for the second let $\frac{a}{s} \in R_{\mathfrak{p}}$, where $a \in R$ and $s \in R \setminus \mathfrak{p}$. Since $v_{\mathfrak{p}}(s) = 0$, the ideals (s) and \mathfrak{p}^k of R are comaximal. So there are $b \in R$ and $c \in \mathfrak{p}^k$ such that $a = bs + c$. Then $\frac{a}{s} = b + \frac{c}{s} \in R + (\mathfrak{p}R_{\mathfrak{p}})^k$. \square

Let's consider first the special case of a discrete valuation ring.

6.18 Proposition. *Let R be a discrete valuation ring with maximal ideal \mathfrak{p} , $\pi \in R$ such that $\mathfrak{p} = \pi R$, $k \in \mathbb{N}^*$, $x \in R$ and $S \subseteq R$ a system of representatives of R/\mathfrak{p} . Then there are unique $s_0, \dots, s_{k-1} \in S$ such that*

$$x \equiv s_0 + s_1\pi + \cdots + s_{k-1}\pi^{k-1} \pmod{\mathfrak{p}^k}.$$

PROOF. For $k = 1$ this is trivially true. Suppose for some $k \in \mathbb{N}^*$ there are unique $s_0, \dots, s_{k-1} \in S$ such that

$$x \equiv s_0 + s_1\pi + \cdots + s_{k-1}\pi^{k-1} \pmod{\mathfrak{p}^k},$$

that is

$$x - (s_0 + s_1\pi + \cdots + s_{k-1}\pi^{k-1}) \in \mathfrak{p}^k,$$

say

$$x - (s_0 + s_1\pi + \cdots + s_{k-1}\pi^{k-1}) = y\pi^k$$

with $y \in R$. For the unique $s_k \in S$ with $y \equiv s_k \pmod{\mathfrak{p}}$ we have

$$x - (s_0 + s_1\pi + \cdots + s_{k-1}\pi^{k-1}) \equiv s_k\pi^k \pmod{\mathfrak{p}^{k+1}}. \quad \square$$

In general we have:

6.19 Theorem. *Let R be a Dedekind domain, $\mathfrak{p} \in \text{Max}(R)$, $\pi \in R$ such that $v_{\mathfrak{p}}(\pi) = 1$, $k \in \mathbb{N}^*$, $x \in R$ and $S \subseteq R$ a system of representatives of R/\mathfrak{p} . Then there are unique $s_0, \dots, s_{k-1} \in S$ such that*

$$x \equiv s_0 + s_1\pi + \cdots + s_{k-1}\pi^{k-1} \pmod{\mathfrak{p}^k}.$$

PROOF. This follows from Proposition 6.18. Note that S is a system of representatives of $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$ as well. \square

The class \bar{x} is invertible in the local ring R/\mathfrak{p}^k if and only if $x \notin \mathfrak{p}$ and this is equivalent to $s_0 \notin \mathfrak{p}$. If the representative of \mathfrak{p} is chosen to be 0, then the condition becomes $s_0 \neq 0$.

6.20 Example. Let p be a prime number and $k \in \mathbb{N}^*$. Take $S = \{0, 1, \dots, p-1\}$. Then for each $x \in \mathbb{Z}$ there are unique $s_0, \dots, s_{k-1} \in S$ such that

$$x \equiv s_0 + s_1p + \dots + s_{k-1}p^{k-1} \pmod{p^k}.$$

This unique way of representing classes modulo p^k can be used for counting arguments. For example the class of x is invertible in the ring $\mathbb{Z}/(p^k)$ if and only if $s_0 \neq 0$, from which it follows that $\#(\mathbb{Z}/(p^k))^* = (p-1)p^{k-1}$.

Theorem 6.19 provides alternative proofs of some of the results on Dedekind domains in chapter 2, in particular of Proposition 2.17 and its consequences like the multiplicativity of the norm of ideals in the case of number fields.

6.3 Localization at a collection of prime ideals

For \mathfrak{p} a maximal ideal of a Dedekind domain R , the valuation ring of $v_{\mathfrak{p}}$ is the localization of R at the prime ideal \mathfrak{p} . The unique prime ideal of the Dedekind domain $R_{\mathfrak{p}}$ is the ideal $\mathfrak{p}R_{\mathfrak{p}}$. In this section we generalize this to an arbitrary collection P of maximal ideals of a Dedekind domain R : we will extend R inside its field of fractions to a Dedekind domain R_P with $\text{Max}(R_P) = \{\mathfrak{p}R_P \mid \mathfrak{p} \in P\}$.

In this section R is a Dedekind domain, K the field of fractions of R and P is a subset of $\text{Max}(R)$.

6.21 Definition. The subring

$$R_P = \{a \in K \mid v_{\mathfrak{p}}(a) \geq 0 \text{ for all } \mathfrak{p} \in P\}$$

is called the *localization of R at P* .

Note that $R_P \subseteq R_Q$ if $P \supseteq Q$. For any P the ring R is a subring of R_P . Here are some (extreme) examples:

6.22 Examples.

- a) $R_{\emptyset} = K$.
- b) By Proposition 6.4: $R_{\text{Max}(R)} = R$.
- c) Let $\mathfrak{p} \in \text{Max}(R)$. Then $R_{\{\mathfrak{p}\}} = R_{\mathfrak{p}}$, the valuation ring of the discrete valuation $v_{\mathfrak{p}}$.

6 Localization of Dedekind Domains

Note that the localization of R at P is an intersection of discrete valuation rings:

$$R_P = \bigcap_{\mathfrak{p} \in P} R_{\mathfrak{p}}.$$

We will compare ideals of R and ideals of R_P . If \mathfrak{a} is an ideal of R , the ideal of R_P generated by \mathfrak{a} is $\mathfrak{a}R_P$. If \mathfrak{b} is an ideal of R_P , then $\mathfrak{b} \cap R$ is an ideal of R . Thus we have extension and restriction of ideals:

$$\begin{array}{ccc} \mathfrak{a} & \xrightarrow{\quad\quad\quad} & \mathfrak{a}R_P \\ \text{ideals of } R & \begin{array}{c} \xrightarrow{\text{extension}} \\ \xleftarrow{\text{restriction}} \end{array} & \text{ideals of } R_P \\ \mathfrak{b} \cap R & \xleftarrow{\quad\quad\quad} & \mathfrak{b} \end{array}$$

For the extension of the restriction we have:

6.23 Proposition. *Let \mathfrak{b} be an ideal of R_P . Then $(\mathfrak{b} \cap R)R_P = \mathfrak{b}$.*

PROOF. We can assume that \mathfrak{b} is not the zero ideal. The ideal $(\mathfrak{b} \cap R)R_P$ is the ideal of R_P generated by the subset $\mathfrak{b} \cap R$ of the ideal \mathfrak{b} . So $(\mathfrak{b} \cap R)R_P \subseteq \mathfrak{b}$. Let $b \in \mathfrak{b}$. We will prove that $b \in (\mathfrak{b} \cap R)R_P$. The principal fractional ideal bR of R can be written as $\mathfrak{a}_1\mathfrak{a}_2^{-1}$, where \mathfrak{a}_1 and \mathfrak{a}_2 are comaximal ideals of R . Since $\mathfrak{a}_1 = \mathfrak{a}_2 \cdot bR \subseteq R \cdot bR = bR \subseteq \mathfrak{b}$, we have $\mathfrak{a}_1 \subseteq \mathfrak{b} \cap R$. For each $\mathfrak{p} \in P$ we have $v_{\mathfrak{p}}(\mathfrak{a}_1) = v_{\mathfrak{p}}(\mathfrak{a}_2) + v_{\mathfrak{p}}(b) \geq v_{\mathfrak{p}}(\mathfrak{a}_2)$ and so $v_{\mathfrak{p}}(\mathfrak{a}_2) = 0$. It follows that $\mathfrak{a}_2^{-1} \subseteq R_P$. Thus $b \in bR = \mathfrak{a}_1\mathfrak{a}_2^{-1} \subseteq (\mathfrak{b} \cap R)R_P$. \square

This can be used to show that the localization of a Dedekind domain is a Dedekind domain:

6.24 Theorem. *Let P be nonempty. Then R_P is a Dedekind domain.*

PROOF. The ring R_P is not a field since P is nonempty: for $\mathfrak{p} \in P$ and $\pi \in R$ with $v_{\mathfrak{p}}(\pi) = 1$ we have $\pi \in R_P$ and $\frac{1}{\pi} \notin R_P$. Let \mathfrak{b}_1 and \mathfrak{b}_2 be nonzero ideals of R_P such that $\mathfrak{b}_1 \supseteq \mathfrak{b}_2$. We will prove that $\mathfrak{b}_1 \mid \mathfrak{b}_2$. For the ideals $\mathfrak{b}_1 \cap R$ and $\mathfrak{b}_2 \cap R$ of the Dedekind domain R we have $\mathfrak{b}_1 \cap R \supseteq \mathfrak{b}_2 \cap R$. There is an ideal \mathfrak{a} of R such that $(\mathfrak{b}_1 \cap R)\mathfrak{a} = \mathfrak{b}_2 \cap R$. It follows that $(\mathfrak{b}_1 \cap R)R_P \cdot \mathfrak{a}R_P = (\mathfrak{b}_2 \cap R)R_P$ and so by Proposition 6.23: $\mathfrak{b}_1 \cdot \mathfrak{a}R_P = \mathfrak{b}_2$. In particular $\mathfrak{b}_1 \mid \mathfrak{b}_2$. \square

6.25 Proposition. *Let \mathfrak{a} be a nonzero ideal of R . Then*

$$\mathfrak{a}R_P = \{x \in K \mid v_{\mathfrak{p}}(x) \geq v_{\mathfrak{p}}(\mathfrak{a}) \text{ for all } \mathfrak{p} \in P\}.$$

PROOF. For $x \in K$ the following are equivalent:

$$x \in \mathfrak{a}R_P,$$

$$\begin{aligned}
 xR &\subseteq \mathfrak{a}R_P, \\
 x\mathfrak{a}^{-1} &\subseteq R_P, \\
 v_{\mathfrak{p}}(y) &\geq 0 \text{ for all } y \in x\mathfrak{a}^{-1} \text{ and all } \mathfrak{p} \in P, \\
 v_{\mathfrak{p}}(x\mathfrak{a}^{-1}) &\geq 0 \text{ for all } \mathfrak{p} \in P && \text{(Proposition 6.3),} \\
 v_{\mathfrak{p}}(x) &\geq v_{\mathfrak{p}}(\mathfrak{a}) \text{ for all } \mathfrak{p} \in P. && \square
 \end{aligned}$$

So for the restriction of the extension we have:

6.26 Corollary. *Let \mathfrak{a} be a nonzero ideal of R . Then*

$$\mathfrak{a}R_P \cap R = \prod_{\mathfrak{p} \in P} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})}. \quad \square$$

PROOF. By Proposition 6.25

$$\mathfrak{a}R_P \cap R = \{x \in R \mid v_{\mathfrak{p}}(x) \geq v_{\mathfrak{p}}(\mathfrak{a}) \text{ for all } \mathfrak{p} \in P\}. \quad \square$$

Two special cases are worth mentioning:

6.27 Corollary. *Let \mathfrak{a} be a nonzero ideal of R .*

- (i) *If $\mathfrak{p} \in P$ for all $\mathfrak{p} \mid \mathfrak{a}$, then $\mathfrak{a}R_P \cap R = \mathfrak{a}$ and the inclusion $R \rightarrow R_P$ induces an isomorphism $R/\mathfrak{a} \xrightarrow{\sim} R_P/\mathfrak{a}R_P$.*
- (ii) *If $\mathfrak{p} \notin P$ for all $\mathfrak{p} \mid \mathfrak{a}$, then $\mathfrak{a}R_P = R_P$.*

PROOF.

- (i) By Corollary 6.26 $\mathfrak{a}R_P \cap R = \mathfrak{a}$, so the homomorphism $R/\mathfrak{a} \rightarrow R_P/\mathfrak{a}R_P$ is injective. For surjectivity we need $R_P = R + \mathfrak{a}R_P$. Let $b \in R_P$ with $b \neq 0$. It suffices to prove that $bR \subseteq R + \mathfrak{a}R_P$. Write $bR = \mathfrak{a}_1\mathfrak{a}_2^{-1}$ with \mathfrak{a}_1 and \mathfrak{a}_2 comaximal ideals of R . Since $bR \subseteq R_P$, we have $v_{\mathfrak{p}}(\mathfrak{a}_2) = 0$ for all $\mathfrak{p} \in P$. It follows that $\mathfrak{a}_2 + \mathfrak{a} = R$ and from this $bR = b\mathfrak{a}_2 + b\mathfrak{a} = \mathfrak{a}_1 + b\mathfrak{a} \subseteq R + \mathfrak{a}R_P$.
- (ii) By Corollary 6.26 $\mathfrak{a}R_P \cap R = R$, so $R \subseteq \mathfrak{a}R_P$ and hence $1 \in \mathfrak{a}R_P$. □

The following proposition describes the maximal ideals of a localization of a Dedekind domain R at a set P of maximal ideals.

6.28 Proposition. *The map*

$$\text{Max}(R_P) \rightarrow \text{Max}(R), \quad \mathfrak{q} \mapsto \mathfrak{q} \cap R$$

is injective and its image equals P . The maximal ideals of R_P are the ideals $\mathfrak{p}R_P$ with $\mathfrak{p} \in P$.

PROOF. By Proposition 6.23 $(\mathfrak{q} \cap R)R_P = \mathfrak{q}$ for all $\mathfrak{q} \in \text{Max}(R_P)$. In particular $\mathfrak{q} \cap R$ is a nonzero prime ideal of R , that is $\mathfrak{q} \cap R \in \text{Max}(R)$. It also follows that the map $\text{Max}(R_P) \rightarrow \text{Max}(R)$ is injective.

For $\mathfrak{p} \notin P$ by Corollary 6.27 we have $\mathfrak{p}R_P = R_P$. Let $\mathfrak{q} \in \text{Max}(R_P)$. Then $\mathfrak{q} \cap R \in P$, since otherwise $\mathfrak{q} = (\mathfrak{q} \cap R)R_P = R_P$. So the image of the map $\text{Max}(R_P) \rightarrow \text{Max}(R)$ is contained in P . For $\mathfrak{p} \in P$ and a maximal ideal $\mathfrak{q} \supseteq \mathfrak{p}R_P$ of R_P we have by Corollary 6.27 $\mathfrak{q} \cap R \supseteq \mathfrak{p}R_P \cap R = \mathfrak{p}$ and so $\mathfrak{q} \cap R = \mathfrak{p}$, since \mathfrak{p} is maximal. By Proposition 6.23 we have in fact $\mathfrak{q} = \mathfrak{p}R_P$. \square

6.29 Proposition. *Let $x \in K^*$. Then $v_{\mathfrak{q}}(x) = v_{\mathfrak{p}}(x)$ for $\mathfrak{p} \in P$ and $\mathfrak{q} = \mathfrak{p}R_P$.*

PROOF. Since $v_{\mathfrak{p}}$ and $v_{\mathfrak{q}}$ are homomorphisms from K^* to \mathbb{Z} we may assume that $x \in R$. By Corollary 6.26

$$xR_P \cap R = \prod_{\mathfrak{p} \in P} \mathfrak{p}^{v_{\mathfrak{p}}(x)}$$

and so by Proposition 6.23

$$xR_P = (xR_P \cap R)R_P = \prod_{\mathfrak{p} \in P} (\mathfrak{p}R_P)^{v_{\mathfrak{p}}(x)}. \quad \square$$

So the exact sequence (2.2) on page 44 for the Dedekind domain R_P is the sequence

$$1 \longrightarrow R_P^* \longrightarrow K^* \xrightarrow{(v_{\mathfrak{p}})_{\mathfrak{p} \in P}} \bigoplus_{\mathfrak{p} \in P} \mathbb{Z} \longrightarrow \mathcal{C}(R_P) \longrightarrow 1.$$

Therefore, the ker-coker exact sequence of the commutative triangle

$$\begin{array}{ccc} K^* & \xrightarrow{(v_{\mathfrak{p}})} & \bigoplus_{\mathfrak{p} \in \text{Max}(R)} \mathbb{Z} \\ & \searrow (v_{\mathfrak{p}}) & \swarrow \\ & & \bigoplus_{\mathfrak{p} \in P} \mathbb{Z} \end{array}$$

is as follows:

$$1 \longrightarrow R^* \longrightarrow R_P^* \longrightarrow \bigoplus_{\mathfrak{p} \notin P} \mathbb{Z} \longrightarrow \mathcal{C}(R) \longrightarrow \mathcal{C}(R_P) \longrightarrow 1. \quad (6.1)$$

The effect of localizing at P is that the group of units becomes larger and that the ideal class group becomes smaller in the sense that the ideal classes represented by prime ideals outside P are killed.

6.4 Localizations of rings of integers of number fields

For the ring of integers of a number field K we use special notations. We already introduced in section 2.3 the notations $\mathcal{C}(K)$, $\mathbb{I}^+(K)$, $\mathbb{I}(K)$ for $\mathcal{C}(\mathcal{O}_K)$, $\mathbb{I}^+(\mathcal{O}_K)$, $\mathbb{I}(\mathcal{O}_K)$ respectively.

6.30 Notations. Let K be a number field and $P \subseteq \text{Max}(\mathcal{O}_K)$. The following notations are used:

K_P	the localization $(\mathcal{O}_K)_P$,
$\mathbb{I}_P(K)$	the subgroup of $\mathbb{I}(K)$ generated by all $\mathfrak{p} \in P$.

By Proposition 6.28 the map $\mathbb{I}_P(K) \rightarrow \mathbb{I}(K_P)$ given by $\mathfrak{p} \mapsto \mathfrak{p}K_P$ on base elements, is an isomorphism. The exact sequence (6.1) on page 140 becomes

$$1 \longrightarrow \mathcal{O}_K^* \longrightarrow K_P^* \longrightarrow \bigoplus_{\mathfrak{p} \notin P} \mathbb{Z} \longrightarrow \mathcal{C}(K) \longrightarrow \mathcal{C}(K_P) \longrightarrow 1.$$

The group $\mathcal{C}(K)$ is finite and \mathcal{O}_K^* is an abelian group of finite rank. So the group K_P^* is of finite rank if and only if the group $\bigoplus_{\mathfrak{p} \notin P} \mathbb{Z}$ is, that is if the complement of P in $\text{Max}(\mathcal{O}_K)$ is finite. Dirichlet's Unit Theorem leads to the following theorem on the structure of K_P^* .

6.31 Theorem. *Let K be a number field and $P \subseteq \text{max}(\mathcal{O}_K)$ such that the complement of P in $\text{Max}(\mathcal{O}_K)$ is finite. Then K_P^* is a finitely generated abelian group of rank $r + s + \#(\text{Max}(\mathcal{O}_K) \setminus P) - 1$. \square*

In this chapter our starting point was a Dedekind domain R . The maximal ideals of R correspond to discrete valuations of the field of fractions K of R . The localizations of R correspond to subsets of this set of discrete valuations. In chapter 10 we will see that for a number field there are no more discrete valuations than those coming from maximal ideals of the ring of integers. In this case its ring of integers is a convenient starting point because a maximal collection of discrete valuations of the number field is involved.

EXERCISES

- Let K be a number field, $\mathfrak{p} \in \text{Max}(\mathcal{O}_K)$ and $k \in \mathbb{N}^*$.
 - Prove that $N(\mathfrak{p}^k) = N(\mathfrak{p})^k$ using Theorem 6.19. Show that this implies that N is multiplicative: $N(\mathfrak{a})N(\mathfrak{b}) = N(\mathfrak{ab})$ for nonzero ideals \mathfrak{a} and \mathfrak{b} of \mathcal{O}_K .
 - Prove that $\#((\mathcal{O}_K/\mathfrak{p}^k)^*) = N(\mathfrak{p})^k \left(1 - \frac{1}{N(\mathfrak{p})}\right)$.

6 Localization of Dedekind Domains

(iii) Let \mathfrak{a} be a nonzero ideal of \mathcal{O}_K . Show that

$$\#((\mathcal{O}_K/\mathfrak{a})^*) = N(\mathfrak{a}) \cdot \prod_{\mathfrak{p}|\mathfrak{a}} \left(1 - \frac{1}{N(\mathfrak{p})}\right).$$

2. Let k be a field. The polynomial ring $k[T]$ is a Euclidean domain and the rational function field $k(T)$ is the field of fractions of $k[T]$. For $f \in k(T)^*$ the *degree* $\deg(f)$ of f and the *leading coefficient* $\text{lc}(f)$ are defined as follows: put $f = g/h$ with $g, h \in k[T]$, then

$$\deg(f) = \deg(g) - \deg(h) \quad \text{and} \quad \text{lc}(f) = \text{lc}(g)/\text{lc}(h).$$

(i) Show that the map

$$v_\infty: k(T)^* \rightarrow \mathbb{Z}, \quad f \mapsto -\deg(f)$$

is a discrete valuation on $k(T)$.

(ii) Let R be the valuation ring of v_∞ , \mathfrak{m} its maximal ideal and $f \in R \setminus \{0\}$. Show that $f \equiv \text{lc}(f) \pmod{\mathfrak{m}}$.

(iii) Prove that the inclusion $k \subseteq R$ induces an isomorphism $k \xrightarrow{\sim} R/\mathfrak{m}$.

3. Let K be a number field. Show that there is a subset P of $\text{Max}(\mathcal{O}_K)$ such that $\text{Max}(\mathcal{O}_K) \setminus P$ is finite and the localization \mathcal{O}_P is a principal ideal domain.

4. In Example 4.32 it was shown that structure of the ideal class group of $K = \mathbb{Q}(\sqrt{-222})$ is $C_6 \times C_2$. Let S be a finite set of maximal ideals of $\mathbb{Z}[\sqrt{-222}]$ such that for $P = \text{Max}(\mathbb{Z}[\sqrt{-222}]) \setminus S$ the ideal class group $\mathcal{C}_P(K)$ is trivial.

(i) Show that $\#(S) \geq 2$.

(ii) Find two prime ideals \mathfrak{p} and \mathfrak{q} such that for $S = \{\mathfrak{p}, \mathfrak{q}\}$ the ideal class group $\mathcal{C}(K_P)$ is trivial. (Use exercise 12 of chapter 4.)

5. Let \mathfrak{p} be the maximal ideal $(3, 1 + \sqrt{-5})$ of $K = \mathbb{Q}(\sqrt{-5})$.

(i) Show that $K_{\mathfrak{p}}$ is a principal ideal domain.

(ii) Show that $K_{\mathfrak{p}}^* = \langle -1, 2 - \sqrt{-5} \rangle$.

6. Let \mathfrak{p} be the maximal ideal $(6 + \sqrt{-5})$ of $K = \mathbb{Q}(\sqrt{-5})$.

(i) Show that $K_{\mathfrak{p}}$ is not a principal ideal domain.

(ii) Show that $K_{\mathfrak{p}}^* = \langle -1, 6 + \sqrt{-5} \rangle$.

(iii) Prove that the Dedekind domain $K_{\mathfrak{p}}$ is not the integral closure of a principal ideal domain.

7. Show that there are Dedekind domains with all maximal ideals nonprincipal.

8. Let R be a Dedekind domains which is not a principal ideal domain. Show that there are infinitely many nonprincipal prime ideals of R .

9. Let R be a Dedekind domain such that each ideal class of R contains a prime ideal. Show that for any nonempty $P \subseteq \text{Max}(R)$ nonprincipal ideal classes of R_P contain prime ideals.

10. Let K be a number field. An element $\alpha \in \mathcal{O}_K$ is called *totally positive* if $\sigma(\alpha) > 0$ for every embedding $\sigma: K \rightarrow \mathbb{R}$. Let K^+ denote the subgroup of K^* of all totally positive elements of K . Let $\mathbb{P}^+(K)$ be the subgroup of $\mathbb{I}(K)$ of all principal fractional ideals $\alpha\mathcal{O}_K$ with α totally positive. The factor group $\mathcal{C}^+(K) := \mathbb{I}(K)/\mathbb{P}^+(K)$ is called the *narrow ideal class group* of K . So we have an exact sequence

$$1 \longrightarrow \mathcal{O}_K^* \cap K^+ \longrightarrow K^+ \longrightarrow \mathbb{I}(K) \longrightarrow \mathcal{C}^+(K) \longrightarrow 1.$$

Let $[\mathfrak{a}]^+$ denote the class of $\mathfrak{a} \in \mathbb{I}(K)$ in $\mathcal{C}^+(K)$ and $[\mathfrak{a}]$ its class in $\mathcal{C}(K)$.

- (i) Show that the group homomorphism

$$\mathcal{C}^+(K) \rightarrow \mathcal{C}(K), \quad [\mathfrak{a}]^+ \mapsto [\mathfrak{a}]$$

is surjective and that its kernel is an elementary abelian 2-group.

- (ii) Show that $\mathcal{O}_K^* \cap K^+$ is a free abelian group of rank $r + s - 1$ if K has at least one real embedding.

11. Let K be a real quadratic number field and ε the fundamental unit of K . Show that

$$\#(\mathcal{C}^+(K)) = \begin{cases} 2 \cdot \#(\mathcal{C}(K)) & \text{if } \varepsilon \text{ is totally positive,} \\ \#(\mathcal{C}(K)) & \text{otherwise.} \end{cases}$$

In the following exercises the localization of a Dedekind domain in the sense of commutative algebra is compared with the localization as defined in this chapter (Definition 6.21).

12. Let R be a Dedekind domain with field of fractions K and S a multiplicative system of R with $0 \notin S$. Let P be the collection of maximal ideals of R disjoint from S :

$$P = \{ \mathfrak{p} \mid \mathfrak{p} \cap S = \emptyset \}.$$

- (i) Show that $S^{-1}R \subseteq R_P$.
- (ii) Let \mathfrak{b} an ideal of R satisfying $\mathfrak{p} \nmid \mathfrak{b}$ for all $\mathfrak{p} \in P$. Prove that there exists a $b \in \mathfrak{b}$ such that $b \notin \mathfrak{p}$ for all $\mathfrak{p} \in P$.
- (iii) Show that $R_P \subseteq S^{-1}R$.
13. Let R be a Dedekind domain, P a finite nonempty collection of maximal ideals of R and $S = R \setminus \bigcup_{\mathfrak{p} \in P} \mathfrak{p}$. Prove that S is a multiplicative system in the ring R and that $R_P = S^{-1}R$.
14. Let R be a Dedekind domain, P a nonempty collection of maximal ideals of R and $S = R \setminus \bigcup_{\mathfrak{p} \in P} \mathfrak{p}$. Assume that $\mathcal{C}(R)$ is a torsion group. Prove that $R_P = S^{-1}R$.
15. Let R be a Dedekind domain such that $\mathcal{C}(R)$ contains elements of infinite order.
- (i) Show that there exists a $\mathfrak{p} \in \text{Max}(R)$ such that $[\mathfrak{p}] \in \mathcal{C}(R)$ is of infinite order.
- (ii) Let $P = \text{Max}(R) \setminus \{\mathfrak{p}\}$, where \mathfrak{p} is as in (i). Assume there exists a multiplicative system S in R such that $S^{-1}R = R_P$. Show that $\mathfrak{q} \cap S = \emptyset$ for all maximal ideals $\mathfrak{q} \neq \mathfrak{p}$ of R .
- (iii) Show that $\mathfrak{p} \cap S = \emptyset$.
- (iv) Show that there is no multiplicative set S such that $S^{-1}R = R_P$.

7 Extensions of Dedekind Domains

In chapter 3 the splitting behavior of prime numbers in the ring of integers of a number field K was studied. This ring \mathcal{O}_K is the integral closure of \mathbb{Z} in K . More generally we can consider extensions $L : K$ of number fields, the so-called *relative* extensions, extensions $K : \mathbb{Q}$ being called *absolute*. In the relative case the ring \mathcal{O}_L is the integral closure of \mathcal{O}_K in L . Our point of view in this chapter is even more general: we start with just a Dedekind domain R and consider the splitting behavior of prime ideals of R in the integral closure of R in a finite separable extension of the field of fractions of R . Results of chapter 3 will be generalized, using more general notions of norm and discriminant. Many examples are given, most of them concern number field extensions.

Particularly important are the Galois extensions. The action of the Galois group on the set of prime ideals above a given prime ideal of the base field determines subgroups of the Galois group and hence, by the Galois correspondence, intermediate fields of the extension. This is studied in the sections 7.3 and 7.5. In this last section a chain of subgroups of the Galois group related to a ramifying prime is considered. This will be used in chapter 9 in a proof of the Kronecker-Weber Theorem. Further on, in chapter 17, these groups are of fundamental importance. In section 7.7 the Frobenius automorphism of a prime ideal is introduced. This is a first step towards class field theory: in the abelian case it connects an ideal to an automorphism of the extension.

7.1 Ramification index, residue class degree

Our aim is to generalize Theorem 3.4 to the relative case: for $L : K$ an extension of number fields an analogous theorem on the splitting of a $\mathfrak{p} \in \text{Max}(\mathcal{O}_K)$ in L . In fact, we will consider the even more general situation of an extension of a Dedekind domain.

For this section we fix the following:

R	a Dedekind domain,
K	the field of fractions of R ,
$L : K$	a finite separable field extension,

n	the degree of $L : K$,
S	the integral closure of R in L .

By Theorem 2.43 the ring S is a Dedekind domain. So for each $\mathfrak{p} \in \text{Max}(R)$ the ideal $\mathfrak{p}S$ of S has a unique decomposition as a product of prime ideals of S .

7.1 Lemma. *Let $\mathfrak{q} \in \text{Max}(S)$ and $\mathfrak{p} = \mathfrak{q} \cap R$. Then $\mathfrak{p} \in \text{Max}(R)$ and $\mathfrak{q} \mid \mathfrak{p}S$.*

PROOF. Since \mathfrak{q} is a prime ideal of S , the ideal \mathfrak{p} is a prime ideal of R . It is not the zero ideal: for $0 \neq \alpha \in \mathfrak{q}$ we have $N_K^L(\alpha) \in \mathfrak{q} \cap K^*$. Because $\mathfrak{q} \supseteq \mathfrak{p}$ we have $\mathfrak{q} \supseteq \mathfrak{p}S$ and so, since S is a Dedekind domain, $\mathfrak{q} \mid \mathfrak{p}S$. \square

7.2 Definitions. A $\mathfrak{q} \in \text{Max}(S)$ is said to be *above* \mathfrak{p} if $\mathfrak{q} \cap K = \mathfrak{p}$. It is then also said that \mathfrak{p} is *below* \mathfrak{q} . For $\mathfrak{q} \in \text{Max}(S)$ above $\mathfrak{p} \in \text{Max}(R)$ the number $v_{\mathfrak{q}}(\mathfrak{p}S)$ is called the *ramification index* of \mathfrak{q} over K . By Proposition 1.36 and Lemma 2.44 S is a finitely generated R -module, so the field extension $S/\mathfrak{q} : R/\mathfrak{p}$ is finite. Its degree is called the *residue class degree* of \mathfrak{q} over K . Notations: $e_K(\mathfrak{q}) = v_{\mathfrak{q}}(\mathfrak{p}S)$ and $f_K(\mathfrak{q}) = [S/\mathfrak{q} : R/\mathfrak{p}]$.

Thus the ideal $\mathfrak{p}S$ of the Dedekind domain S has a factorization

$$\mathfrak{p}S = \prod_{\mathfrak{q} \mid \mathfrak{p}S} \mathfrak{q}^{e_K(\mathfrak{q})}, \tag{7.1}$$

where the product is taken over the $\mathfrak{q} \in \text{Max}(S)$ above \mathfrak{p} .

For a tower of field extensions it follows directly from the definitions that we have the following (exercise 3).

7.3 Proposition. *Let also $M : L$ be a finite separable field extension and T the integral closure of R in M . Then $M : K$ is a finite separable field extension and T is the integral closure of S in M . Let $\mathfrak{q} \in \text{Max}(T)$. Then*

$$e_K(\mathfrak{q}) = e_L(\mathfrak{q})e_K(\mathfrak{q} \cap S) \quad \text{and} \quad f_K(\mathfrak{q}) = f_L(\mathfrak{q})f_K(\mathfrak{q} \cap S). \quad \square$$

For P a collection of maximal ideals of R , the ring R_P is a Dedekind domain and so is its integral closure in L . For the collection Q of all maximal ideals of S above the maximal ideals in P the ring S_Q is a Dedekind domain and is the obvious candidate to be the integral closure of R_P in L , but this still requires a proof. First some lemmas.

7.4 Lemma. *Let \mathfrak{p} be a maximal ideal of R and $\gamma \in S$ such that $\gamma \notin \mathfrak{q}$ for all maximal ideals \mathfrak{q} of S above \mathfrak{p} . Then $N_K^L(\gamma) \notin \mathfrak{p}$.*

PROOF. Let $M : K$ be the normal closure of $L : K$ and T the integral closure of S in M . Then γ is not in any of the maximal ideals of T above \mathfrak{p} . Because $N_K^M(\gamma) = N_K^L(\gamma)^{[M:L]}$, we may assume that $L : K$ is a Galois extension. In that case we have $N_K^L(\gamma) = \prod_{\sigma} \sigma(\gamma)$, where the product is over all $\sigma \in \text{Gal}(L : K)$.

Suppose $N_K^L(\gamma) \in \mathfrak{p}$. Then for any \mathfrak{q} above \mathfrak{p} we have $N_K^L(\gamma) \in \mathfrak{q}$. This implies that $\sigma(\gamma) \in \mathfrak{q}$ for some σ . But then $\gamma \in \sigma^{-1}(\mathfrak{q})$. Contradiction. \square

7.5 Lemma. *Let \mathfrak{p} be a maximal ideal of R and Q the collection of primes of S above \mathfrak{p} . Then $S_Q = R_{\mathfrak{p}}S$.*

PROOF. From $R_{\mathfrak{p}}, S \subseteq S_Q$ follows that $R_{\mathfrak{p}}S \subseteq S_Q$. Let $\gamma \in S_Q$. Then $\gamma S = \frac{\mathfrak{a}}{\mathfrak{b}}$ for ideals $\mathfrak{a}, \mathfrak{b}$ of S such that $v_{\mathfrak{q}}(\mathfrak{b}) = 0$ for all $\mathfrak{q} \in Q$. By Lemma 2.28 there exists an ideal \mathfrak{c} of R such that \mathfrak{c} is in the inverse ideal class of \mathfrak{b} and $v_{\mathfrak{q}}(\mathfrak{c}) = 0$ for the finitely many \mathfrak{q} in Q . Then \mathfrak{ac} and \mathfrak{bc} are principal ideals, say $\mathfrak{ac} = \alpha S$ and $\mathfrak{bc} = \beta S$ with $\alpha, \beta \in S$. Then $\gamma S = \frac{\mathfrak{a}}{\mathfrak{b}} = \frac{\alpha \mathfrak{c}}{\beta \mathfrak{c}} = \frac{\alpha}{\beta} S$ and $v_{\mathfrak{q}}(\beta) = 0$ for all $\mathfrak{q} \in Q$. Hence $\gamma = \frac{\alpha \nu}{\beta}$ with $\nu \in S^*$. Let $\sigma_1, \dots, \sigma_n$ be the K -embeddings of L in a normal closure of $L : K$ and take σ_1 to be the identity on L . Then $N_K^L(\beta) = \beta \delta$, where $\delta = \sigma_2(\beta) \cdots \sigma_n(\beta)$. So

$$\gamma = \frac{\alpha \nu}{\beta} = \frac{\alpha \nu \delta}{N_K^L(\beta)}.$$

Then $\alpha \nu \delta \in S$ and by Lemma 7.4 $N_K^L(\beta) \notin \mathfrak{p}$. Hence $\gamma \in R_{\mathfrak{p}}S$. \square

7.6 Lemma. *Let A and B be R -submodules of L such that $R_{\mathfrak{p}}A \subseteq R_{\mathfrak{p}}B$ for all $\mathfrak{p} \in \text{Max}(R)$. Then $A \subseteq B$.*

PROOF. Let $\alpha \in A$. For each $\mathfrak{p} \in \text{Max}(R)$ there exists an $r_{\mathfrak{p}} \in R \setminus \mathfrak{p}$ such that $r_{\mathfrak{p}}\alpha \in B$. The ideal of R generated by all $r_{\mathfrak{p}}$ is the unit ideal. So there are $x_{\mathfrak{p}} \in R$ such that all but a finite number of them $\neq 0$ and $1 = \sum_{\mathfrak{p}} x_{\mathfrak{p}} r_{\mathfrak{p}}$. Multiplying by α yields

$$\alpha = \sum_{\mathfrak{p}} x_{\mathfrak{p}} r_{\mathfrak{p}} \alpha \in B. \quad \square$$

7.7 Theorem. *Let P be a collection of maximal ideals of R and Q the collection of all maximal ideals of S above the maximal ideals in P . Then $S_Q = R_P S$. Moreover, S_Q is the integral closure of R_P in L .*

PROOF. We apply Lemma 7.6, using the Dedekind domain R_P instead of R . Both S_Q and $R_P S$ are R_P -submodules of L . The maximal ideals of R_P are the ideals $\mathfrak{p}R_P$ with $\mathfrak{p} \in P$. Note that the localization of R_P at $\mathfrak{p}R_P$ coincides with the localization of R at \mathfrak{p} . Denote the collection of maximal ideals of S above \mathfrak{p} by $Q_{\mathfrak{p}}$. By Lemma 7.5 we have $R_{\mathfrak{p}}S = S_{Q_{\mathfrak{p}}}$. Let $\mathfrak{p} \in P$. Then

$$R_{\mathfrak{p}}S_Q = R_{\mathfrak{p}}SS_Q = S_{Q_{\mathfrak{p}}}S_Q = S_{Q_{\mathfrak{p}}} = R_{\mathfrak{p}}S = R_{\mathfrak{p}}R_P S.$$

The ring S_Q is integrally closed and the elements of $R_P S$ are integral over R_P . So S_Q is the integral closure of R_P in L . \square

A generalization of Theorem 3.4:

7.8 Theorem.

$$\sum_{\mathfrak{q}|\mathfrak{p}S} e_K(\mathfrak{q})f_K(\mathfrak{q}) = [L : K],$$

the sum being taken over all maximal ideals \mathfrak{q} of S above \mathfrak{p} .

PROOF. Let Q be the set of maximal ideals of S above \mathfrak{p} . By Theorem 7.7 (or Lemma 7.5) the ring S_Q is the integral closure of $R_{\mathfrak{p}}$ in L . The factorization (7.1) becomes

$$\mathfrak{p}S_Q = \prod_{\mathfrak{q}|\mathfrak{p}S} (\mathfrak{q}S_Q)^{e_K(\mathfrak{q})}. \tag{7.2}$$

By Corollary 6.27(i) we have commutative squares with horizontal ring isomorphisms

$$\begin{array}{ccc} S/\mathfrak{q} & \xrightarrow{\sim} & S_Q/\mathfrak{q}S_Q \\ \uparrow & & \uparrow \\ R/\mathfrak{p} & \xrightarrow{\sim} & R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}} \end{array} \qquad \begin{array}{ccc} S/\mathfrak{p}S & \xrightarrow{\sim} & S_Q/\mathfrak{p}S_Q \\ \uparrow & & \uparrow \\ R/\mathfrak{p} & \xrightarrow{\sim} & R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}} \end{array}$$

From the first square it follows that the dimension of the $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$ -vector space $S_Q/\mathfrak{q}S_Q$ is equal to the dimension of the R/\mathfrak{p} -vector space S/\mathfrak{q} . The second square tells us that the dimension of the $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$ -vector space $S_Q/\mathfrak{p}S_Q$ is equal to the dimension of the R/\mathfrak{p} -vector space $S/\mathfrak{p}S$. The ring $R_{\mathfrak{p}}$ is a discrete valuation ring and in particular a principal ideal domain, so by Corollary 1.38 the latter dimension equals n .

For every ideal $\mathfrak{a} \mid \mathfrak{p}S_Q$ the ring S_Q/\mathfrak{a} is an $R_{\mathfrak{p}}$ -module and also a homomorphic image of the $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$ -vector space $S_Q/\mathfrak{p}S_Q$. Therefore, S_Q/\mathfrak{a} is an $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$ -vector space as well. The theorem follows by repeated application of Proposition 2.17 using the identity (7.2). \square

7.9 Definitions.

- \mathfrak{p} is said to *remain prime* in L if $f_K(\mathfrak{q}) = n$ for some $\mathfrak{q} \in \text{Max}(S)$ above \mathfrak{p} . By Theorem 7.8 \mathfrak{q} is the unique prime ideal of S above \mathfrak{p} .
- \mathfrak{p} is said to *ramify* in L if $e_K(\mathfrak{q}) > 1$ for some $\mathfrak{q} \in \text{Max}(S)$ above \mathfrak{p} . It *totally ramifies* in L if $e_K(\mathfrak{q}) = n$ for some $\mathfrak{q} \in \text{Max}(S)$ above \mathfrak{p} . If this is the case, then by Theorem 7.8 \mathfrak{q} is the unique prime ideal of S above \mathfrak{p} .
- \mathfrak{p} *splits completely* in L if $e_K(\mathfrak{q}) = f_K(\mathfrak{q}) = 1$ for all $\mathfrak{q} \in \text{Max}(S)$ above \mathfrak{p} . By Theorem 7.8 there are exactly n such prime ideals \mathfrak{q} .

- For R/\mathfrak{p} of characteristic $p \neq 0$: a $\mathfrak{q} \in \text{Max}(S)$ above \mathfrak{p} is said to be *wildly ramified* over K if $p \mid e_K(\mathfrak{q})$. Otherwise \mathfrak{q} is called *tamely ramified* over K .

Note that with this definition unramified implies tamely ramified. As this terminology suggests, wild ramification is much more difficult to handle than tame ramification.

Next we derive a generalization (Theorem 7.12) of the Kummer-Dedekind Theorem (Theorem 3.6).

7.10 Lemma. *Let R be a discrete valuation ring. Suppose there is a $\vartheta \in S$ such that $S = R[\vartheta]$ and let $f \in R[X]$ be the minimal polynomial of ϑ over K . Let $g \in R[X]$ be a monic polynomial such that $\bar{g} \in (R/\mathfrak{p})[X]$ is an over R/\mathfrak{p} irreducible divisor of $\bar{f} \in (R/\mathfrak{p})[X]$. Then $\mathfrak{q} = \mathfrak{p}S + g(\vartheta)S$ is a maximal ideal of S above \mathfrak{p} .*

PROOF. The surjective ring homomorphisms

$$\begin{array}{ccc} (R/\mathfrak{p})[X] & \longleftarrow R[X] & \longrightarrow S \\ \bar{h} & \longleftarrow h & \longrightarrow h(\vartheta) \end{array}$$

induce isomorphisms

$$(R/\mathfrak{p})[X]/(\bar{g}) \xleftarrow{\sim} R[X]/(\mathfrak{p}R[X] + gR[X]) \xrightarrow{\sim} S/\mathfrak{q}.$$

Since \bar{g} is irreducible over R/\mathfrak{p} , the ring on the left is a field. It follows that S/\mathfrak{q} is a field and hence \mathfrak{q} is a maximal ideal of S . \square

7.11 Proposition. *Under the assumptions and in the notations of Lemma 7.10: let $\bar{f} = \bar{g}_1^{e_1} \cdots \bar{g}_r^{e_r}$ be the factorization of \bar{f} , where the polynomials $g_i \in R[X]$ are monic such that \bar{g}_i is irreducible over R/\mathfrak{p} . Then the factorization of $\mathfrak{p}S$ into maximal ideals of S is*

$$\mathfrak{p}S = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r},$$

where $\mathfrak{q}_i = \mathfrak{p}S + g_i(\vartheta)S$. The residue class degree of \mathfrak{q}_i over R equals $\deg(g_i)$.

PROOF. By Lemma 7.10 the \mathfrak{q}_i are maximal ideals of S . Their residue class degree equals $[(R/\mathfrak{p})[X]/(\bar{g}_i) : R/\mathfrak{p}] = \deg(\bar{g}_i)$. We have

$$\begin{aligned} \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r} &= (\mathfrak{p}S + g_1(\vartheta)S)^{e_1} \cdots (\mathfrak{p}S + g_r(\vartheta)S)^{e_r} \\ &\subseteq \mathfrak{p}S + g_1(\vartheta)^{e_1} \cdots g_r(\vartheta)^{e_r} S = \mathfrak{p}S + f(\vartheta)S = \mathfrak{p}S. \end{aligned}$$

For $i \neq j$ the maximal ideals \mathfrak{q}_i and \mathfrak{q}_j are different: take $a(X), b(X) \in R[X]$ such that $\bar{a}(X)\bar{g}_i(X) + \bar{b}(X)\bar{g}_j(X) = \bar{1} \in (R/\mathfrak{p})[X]$. Then $a(\vartheta)g_i(\vartheta) + b(\vartheta)g_j(\vartheta) \in 1 + \mathfrak{p}S$ and so $1 \in \mathfrak{q}_i + \mathfrak{q}_j$. Since $e_1 f_1 + \cdots + e_r f_r = e_1 \deg(g_1) + \cdots + e_r \deg(g_r) = \deg(f) = [L : K]$, by Theorem 7.8 we actually have an equality: $\mathfrak{p}S = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}$. \square

7.12 Theorem. *Let $\vartheta \in S$ be such that $L = K(\vartheta)$ and $\mathfrak{p} \in \text{Max}(R)$ such that $R_{\mathfrak{p}}[\vartheta]$ is the integral closure of $R_{\mathfrak{p}}$ in L . Let f be the minimal polynomial of ϑ over K and $\bar{f} = \bar{g}_1^{e_1} \cdots \bar{g}_r^{e_r}$ the factorization of $\bar{f} \in (R/\mathfrak{p})[X]$ with g_1, \dots, g_r monic polynomials over R . Put $\mathfrak{q}_i = \mathfrak{p}S + g_i(\vartheta)S$ for $i = 1, \dots, r$. Then the ideals $\mathfrak{q}_1, \dots, \mathfrak{q}_r$ are different maximal ideals of S and the factorization of the ideal $\mathfrak{p}S$ in the Dedekind domain S is*

$$\mathfrak{p}S = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r}.$$

The residue class degree of \mathfrak{q}_i over R is equal to $\deg(g_i)$.

PROOF. Let Q be the set of maximal ideals of S above \mathfrak{p} . Then $S_Q = R_{\mathfrak{p}}[\vartheta]$. By Proposition 7.11 the factorization of $\mathfrak{p}S_Q$ is

$$\mathfrak{p}S_Q = (\mathfrak{p}S_Q + g_1(\vartheta)S_Q)^{e_1} \cdots (\mathfrak{p}S_Q + g_r(\vartheta)S_Q)^{e_r}.$$

Restriction of the ideals to the ring S yields

$$\mathfrak{p}S = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r},$$

where $\mathfrak{q}_i = (\mathfrak{p}S_Q + g_i(\vartheta)S_Q) \cap S = (\mathfrak{p}S + g_i(\vartheta)S)S_Q \cap S = \mathfrak{p}S + g_i(\vartheta)S$. \square

Of course it depends on the element $\vartheta \in S$ to which of the maximal ideals \mathfrak{p} of R the theorem is applicable. In any case the theorem is applicable to all but a finite number: for $d = \text{disc}(f) \in R$ we have by Proposition 1.36 that $d \cdot R[\vartheta] \subseteq S$, so the theorem applies to all $\mathfrak{p} \in \text{Max}(R)$ with $d \notin \mathfrak{p}$, i.e. all \mathfrak{p} for which $\bar{f} \in R/\mathfrak{p}[X]$ has no multiple roots. It is possible that there is no $\vartheta \in S$ such that $S = R[\vartheta]$, or even for a given \mathfrak{p} that there is no $\vartheta \in S$ such that $S_Q = R_{\mathfrak{p}}[\vartheta]$ (exercise 5).

For $L : K$ a Galois extension the following generalizes Theorem 3.11. The proof is a straightforward generalization.

7.13 Theorem. *Let $L : K$ be a Galois extension. Then the group $\text{Gal}(L : K)$ operates transitively on the set of prime ideals of S above \mathfrak{p} .*

PROOF. Put $G = \text{Gal}(L : K)$. Let \mathfrak{q} and \mathfrak{q}' be a prime ideals of S above \mathfrak{p} . Suppose $\sigma(\mathfrak{q}) \neq \mathfrak{q}'$ for all $\sigma \in G$. By the Chinese Remainder Theorem there is an $\alpha \in S$ such that

$$\alpha \equiv \begin{cases} 0 \pmod{\mathfrak{q}'}, \\ 1 \pmod{\sigma(\mathfrak{q})} \end{cases} \text{ for all } \sigma \in G.$$

Then $\alpha \notin \sigma(\mathfrak{q})$, that is $\sigma^{-1}(\alpha) \notin \mathfrak{q}$, for all $\sigma \in G$. So $N_K^L(\alpha) = \prod_{\sigma \in G} \sigma(\alpha) \notin \mathfrak{q} \supseteq \mathfrak{p}$. However, $N_K^L(\alpha) \in \mathfrak{q}' \cap K = \mathfrak{p}$. \square

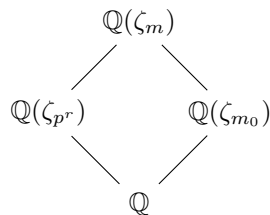
Again we have:

7.14 Corollary. *Let $L : K$ be a Galois extension. Then all prime ideals of S above \mathfrak{p} have the same ramification index over K and they also have the same residue class degree over K .* \square

For Galois extensions the following terminology will be used.

7.15 Definitions and notations. Let $L : K$ be a Galois extension. The *ramification index* of \mathfrak{p} in L is the ramification index $e_K(\mathfrak{q})$ of any of the $\mathfrak{q} \in \text{Max}(S)$ above \mathfrak{p} . Notation: $e_{\mathfrak{p}}^{(L)} = e_K(\mathfrak{q})$. Similarly we have the *residue class degree* $f_{\mathfrak{p}}^{(L)}$ of \mathfrak{p} in L . The number of \mathfrak{q} above \mathfrak{p} is often denoted by $r_{\mathfrak{p}}^{(L)}$. Then Theorem 7.8 reads $r_{\mathfrak{p}}^{(L)} e_{\mathfrak{p}}^{(L)} f_{\mathfrak{p}}^{(L)} = [L : K]$.

7.16 Example. In chapter 3 the splitting behavior of prime numbers in cyclotomic fields was studied (Theorem 3.16). Proposition 7.4 provides an alternative way for this. Let $m \in \mathbb{N}^*$ with $m > 2$, p a prime number and $m = p^r m_0$ with $p \nmid m_0$. The prime p totally ramifies in $\mathbb{Q}(\zeta_{p^r})$, so $e_p^{(\mathbb{Q}(\zeta_{p^r}))} = [\mathbb{Q}(\zeta_{p^r}) : \mathbb{Q}] = \varphi(p^r)$. By Proposition 3.14 $f_p^{(\mathbb{Q}(\zeta_{m_0}))} = f$, where f is the order of \bar{p} in $(\mathbb{Z}/m_0)^*$. The prime number p does not ramify in this subfield and the number of prime ideals of $\mathbb{Z}[\zeta_{m_0}]$ above p is $\varphi(m_0)/f$. By Proposition 7.4 and Corollary 7.14



$$r_p^{(\mathbb{Q}(\zeta_{m_0}))} \mid r_p^{(\mathbb{Q}(\zeta_m))} \quad f_p^{(\mathbb{Q}(\zeta_{m_0}))} \mid f_p^{(\mathbb{Q}(\zeta_m))} \quad \text{and} \quad e_p^{(\mathbb{Q}(\zeta_{p^r}))} \mid e_p^{(\mathbb{Q}(\zeta_m))},$$

and because

$$\varphi(m) = \frac{\varphi(m_0)}{f} \cdot \varphi(p^r) \cdot f \mid r_p^{(\mathbb{Q}(\zeta_m))} e_p^{(\mathbb{Q}(\zeta_m))} f_p^{(\mathbb{Q}(\zeta_m))} = [\mathbb{Q}(\zeta_m) : \mathbb{Q}]$$

we have equality in all three cases.

7.17 Example. Let $L = \mathbb{Q}(\alpha, \zeta_3)$, where $\alpha = \sqrt[3]{2}$. Then $\text{Gal}(L : \mathbb{Q}) \cong S_3$. It is generated by σ and τ defined by

$$\begin{cases} \sigma(\alpha) = \zeta_3 \alpha, \\ \sigma(\zeta_3) = \zeta_3 \end{cases} \quad \text{and} \quad \begin{cases} \tau(\alpha) = \alpha, \\ \tau(\zeta_3) = \zeta_3^2. \end{cases}$$

By the Galois correspondence L has a unique quadratic subfield and three (pure) cubic subfields:

$$L^\sigma = \mathbb{Q}(\zeta_3), \quad L^\tau = \mathbb{Q}(\alpha), \quad L^{\sigma\tau} = \mathbb{Q}(\zeta_3^2 \alpha) \quad \text{and} \quad L^{\sigma^2\tau} = \mathbb{Q}(\zeta_3 \alpha).$$

Application of relative traces to a $\gamma \in \mathcal{O}_L$ yields:

$$\begin{aligned} \gamma + \sigma(\gamma) + \sigma^2(\gamma) &\in \mathbb{Z}[\zeta_3], \\ \gamma + \tau(\gamma) &\in \mathbb{Z}[\alpha], \\ \gamma + \sigma\tau(\gamma) &\in \mathbb{Z}[\zeta_3^2 \alpha], \\ \gamma + \sigma^2\tau(\gamma) &\in \mathbb{Z}[\zeta_3 \alpha]. \end{aligned}$$

So $3\gamma + N_{\mathbb{Q}}^L(\gamma) \in \mathbb{Z}[\zeta_3] + \mathbb{Z}[\alpha] + \mathbb{Z}[\zeta_3\alpha] + \mathbb{Z}[\zeta_3^2\alpha]$ and hence $3\gamma \in \mathbb{Z}[\zeta_3, \alpha]$. The prime number 3 totally ramifies in both $\mathbb{Q}(\zeta_3)$ and $\mathbb{Q}(\alpha)$. Since the degrees of these fields are relatively prime, the prime number 3 totally ramifies in $\mathbb{Q}(\zeta_3, \alpha) = L$, say $(3) = \mathfrak{p}^6$, where \mathfrak{p} is the unique prime ideal of \mathcal{O}_L above 3. From $\mathfrak{p}^3 = (1 + 2\zeta_3)$ and $\mathfrak{p}^2 = (\alpha + 1)$ follows that \mathfrak{p} is the principal ideal generated by $\delta := \frac{1+2\zeta_3}{\alpha+1}$.

We compute \mathcal{O}_L . Let $\beta = \frac{\beta_0}{3} + \frac{\beta_1}{3}\zeta_3$ with $\beta_0, \beta_1 \in \mathbb{Z}[\alpha]$. From

$$\beta \in \mathcal{O}_L \iff \text{Tr}_{\mathbb{Q}(\alpha)}^L(\beta), N_{\mathbb{Q}(\alpha)}^L(\beta) \in \mathbb{Z}[\alpha]$$

follows that $\beta \in \mathcal{O}_L$ if and only if

$$2\beta_0 - \beta_1 \in 3\mathbb{Z}[\alpha] \quad \text{and} \quad \beta_0^2 - \beta_0\beta_1 + \beta_1^2 \in 9\mathbb{Z}[\alpha].$$

Let $\beta_1 = 2\beta_0 - 3\gamma$ with $\gamma \in \mathbb{Z}[\alpha]$. Then

$$\beta_0^2 - \beta_0\beta_1 + \beta_1^2 = 3\beta_0^2 - 9\beta_0\gamma + 9\gamma^2.$$

So $3\beta_0^2 \in 9\mathbb{Z}[\alpha]$ and hence $\beta_0 \in (\alpha + 1)^2\mathbb{Z}[\alpha]$ and $\beta_1 = 2\beta_0 - 3\gamma \in (\alpha + 1)^2\mathbb{Z}[\alpha]$. Put $\frac{\beta_0}{3} = \frac{\gamma_0}{\alpha+1}$ and $\frac{\beta_1}{3} = \frac{\gamma_1}{\alpha+1}$ with $\gamma_0, \gamma_1 \in \mathbb{Z}[\alpha]$. Then

$$\beta = \frac{\gamma_0}{\alpha+1} + \frac{\gamma_1}{\alpha+1}\zeta_3 = \frac{\gamma_0}{\alpha+1} + \frac{2\gamma_0}{\alpha+1}\zeta_3 - \gamma_1\zeta_3 = \gamma_0\delta - \gamma_1\zeta_3.$$

Hence, $(\delta, \alpha\delta, \alpha^2\delta, \zeta_3, \alpha\zeta_3, \alpha^2\zeta_3)$ is an integral basis of L . The identities

$$\alpha\delta = 1 + 2\zeta_3 - \delta \quad \text{and} \quad \alpha^2\delta = \alpha + 2\alpha\zeta_3 - \alpha\delta$$

imply that also $(1, \alpha, \delta, \zeta_3, \alpha\zeta_3, \alpha^2\zeta_3)$ is an integral basis. Since

$$3\delta = (\alpha^2 - \alpha + 1)(1 + 2\zeta_3) = 1 - \alpha + 2\zeta_3 - 2\zeta_3\alpha + 2\zeta_3\alpha^2,$$

we have for the discriminant of L (using Proposition 1.33):

$$\begin{aligned} \text{disc}(L) &= \text{disc}(1, \alpha, \delta, \zeta_3, \alpha\zeta_3, \alpha^2\zeta_3) = \frac{1}{9} \text{disc}(1, \alpha, \alpha^2, \zeta_3, \alpha\zeta_3, \alpha^2\zeta_3) \\ &= \frac{1}{9} \text{disc}(\mathbb{Q}(\alpha))^2 \text{disc}(\mathbb{Q}(\zeta_3))^3 = \frac{1}{9}(-4 \cdot 27)^2(-3)^3 = -2^4 \cdot 3^7. \end{aligned}$$

Because the discriminant of this field of degree 6 is small, the Minkowski bound is (very) small, i.e. less than 6. The only prime ideal of norm ≤ 5 is the principal ideal \mathfrak{p} , so the ring \mathcal{O}_L is a principal ideal domain.

Let's compute \mathcal{O}_L^* . Taking relative norms instead of relative traces yields:

$$(\mathcal{O}_L^*)^3 \subseteq \mathbb{Z}^* \cdot \mathbb{Z}[\zeta_3]^* \cdot \mathbb{Z}[\alpha]^* \cdot \mathbb{Z}[\zeta_3\alpha]^* \cdot \mathbb{Z}[\zeta_3^2\alpha]^* = \langle -\zeta_3, \alpha - 1, \zeta_3\alpha - 1 \rangle.$$

Let $\nu \in \mathcal{O}_L^*$. Then

$$\nu^3 = (-\zeta_3)^{k_0} (\alpha - 1)^{k_1} (\zeta_3\alpha - 1)^{k_2}$$

with $k_0, k_1, k_2 \in \mathbb{Z}$. We look for units $\nu \notin \langle -\zeta_3, \alpha - 1, \zeta_3\alpha - 1 \rangle$. So we can assume that $k_0, k_1, k_2 \in \{-1, 0, 1\}$. Clearly $\mu(L) = \langle -\zeta_3 \rangle$, so k_1 and k_2 are not both 0. Using the action of the Galois group on \mathcal{O}_L^* together with $x \mapsto x^{-1}$ it suffices to consider four cases:

- (1) $\nu^3 = \alpha - 1$. There is no such ν , since otherwise $\alpha - 1$ would not be a fundamental unit of $\mathbb{Q}(\alpha)$.
- (2) $\nu^3 = \zeta_3(\alpha - 1)$. Then $(\nu\tau(\nu))^3 = (\alpha - 1)^2$ and this also contradicts the fact that $\alpha - 1$ is a fundamental unit of L .
- (3) $\nu^3 = \frac{\alpha-1}{\zeta_3\alpha-1}$. The elements $\alpha + 1$ and $\zeta_3\alpha + 1$ both generate the ideal \mathfrak{p}^2 of \mathcal{O}_L . So $\frac{\zeta_3\alpha+1}{\alpha+1} \in \mathcal{O}_L^*$. We compute its cube:

$$\left(\frac{\zeta_3\alpha + 1}{\alpha + 1}\right)^3 = \frac{3\zeta_3^2\alpha^2 + 3\zeta_3\alpha + 3}{3\alpha^2 + 3\alpha + 3} = \frac{\alpha - 1}{\zeta_3\alpha - 1}.$$

- (4) $\nu^3 = \zeta_3\frac{\alpha-1}{\zeta_3\alpha-1}$. This is not possible in L , since in combination with (3) it would lead to the existence of a primitive 9-th root of unity in L .

So the group generated by the units of proper subfields is of index 3 in \mathcal{O}_L^* and

$$\mathcal{O}_L^* = \left\langle -\zeta_3, \alpha - 1, \frac{\zeta_3\alpha + 1}{\alpha + 1} \right\rangle.$$

In this example the prime 3 totally ramifies in L : $(3) = \mathfrak{p}^6$. For δ we have $v_{\mathfrak{p}}(\delta) = 1$ (and even $\mathfrak{p} = (\delta)$). Its minimal polynomial over \mathbb{Q} is easily computed:

$$\begin{aligned} \delta^2 &= \frac{(1 + 2\zeta_3)^2}{(\alpha + 1)^2} = -\frac{3}{(\alpha + 1)^2} = -3\frac{\alpha + 1}{(\alpha + 1)^3} = -\frac{\alpha + 1}{\alpha^2 + \alpha + 1} \\ &= -(\alpha + 1)(\alpha - 1) = -\alpha^2 + 1 \end{aligned}$$

and so

$$(\delta^2 - 1)^3 = -\alpha^6 = -4.$$

Hence the minimal polynomial of δ over \mathbb{Q} is

$$X^6 - 3X^4 + 3X^2 + 3.$$

It is an Eisenstein polynomial:

7.18 Definition. A polynomial

$$f(X) = X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n \in R[X]$$

is called a \mathfrak{p} -polynomial if $a_1, \dots, a_n \in \mathfrak{p}$ and an *Eisenstein \mathfrak{p} -polynomial* if, moreover, $a_n \notin \mathfrak{p}^2$.

Eisenstein polynomials are irreducible. More precisely:

7.19 Lemma. *Let f be an Eisenstein \mathfrak{p} -polynomial. Then f is irreducible over K .*

PROOF. Let L be a splitting field of f over K . The zeros of f in L are integral and so they are elements of S . It follows that monic divisors in $K[X]$ of f have coefficients in R . By reduction modulo \mathfrak{p} it is easily seen that divisors of \mathfrak{p} -polynomials are \mathfrak{p} -polynomials as well. The constant term of a product of two \mathfrak{p} -polynomials is divisible by \mathfrak{p}^2 and is, therefore, not an Eisenstein \mathfrak{p} -polynomial. \square

For total ramification we have the following characterization in terms of a minimal polynomial:

7.20 Theorem. *The maximal ideal \mathfrak{p} totally ramifies in L if and only if there exists a $\vartheta \in S$ such that $L = K(\vartheta)$ and the minimal polynomial of ϑ over K is an Eisenstein \mathfrak{p} -polynomial.*

PROOF. Assume that \mathfrak{p} totally ramifies in L , say $\mathfrak{p}S = \mathfrak{q}^n$ with $\mathfrak{q} \in \text{Max}(S)$. Take $\vartheta \in S$ such that $v_{\mathfrak{q}}(\vartheta) = 1$ and let

$$f(X) = X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n \in R[X]$$

be the characteristic polynomial of ϑ over K . Then

$$\vartheta^n = -(a_1\vartheta^{n-1} + \cdots + a_{n-1}\vartheta + a_n)$$

and for $1 \leq j \leq n$ with $a_j \neq 0$ we have

$$v_{\mathfrak{q}}(a_j\vartheta^{n-j}) = n \cdot v_{\mathfrak{p}}(a_j) + n - j \equiv -j \pmod{n},$$

all different modulo n . So by Corollary 6.6

$$v_{\mathfrak{q}}(a_1\vartheta^{n-1} + \cdots + a_{n-1}\vartheta + a_n) = \min_{1 \leq j \leq n} n \cdot v_{\mathfrak{p}}(a_j) + n - j.$$

If $v_{\mathfrak{p}}(a_j) = 0$ for some j , then $v_{\mathfrak{q}}(a_1\vartheta^{n-1} + \cdots + a_n) < n - j < n$. However, $v_{\mathfrak{q}}(\vartheta^n) = n$. It follows that $v_{\mathfrak{p}}(a_j) > 0$ for all j , that is f is a \mathfrak{p} -polynomial. Since

$$v_{\mathfrak{q}}(\vartheta^n + a_n) = v_{\mathfrak{q}}(a_1\vartheta^{n-1} + \cdots + a_{n-1}\vartheta) = \min_{1 \leq j < n} n \cdot v_{\mathfrak{p}}(a_j) + n - j > n$$

we have $v_{\mathfrak{q}}(a_n) = n$, that is $v_{\mathfrak{p}}(a_n) = 1$. So f is an Eisenstein \mathfrak{p} -polynomial.

Conversely, let $L = K(\vartheta)$ with $\vartheta \in S$ and let the minimal polynomial

$$f(X) = X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n \in R[X]$$

of ϑ over K be an Eisenstein \mathfrak{p} -polynomial. Let \mathfrak{q} be a prime ideal of S above \mathfrak{p} . Then $\vartheta \in \mathfrak{q}$ because

$$\vartheta^n = -(a_1\vartheta^{n-1} + \cdots + a_{n-1}\vartheta + a_n) \in \mathfrak{p}S.$$

Put $e = e_K(\mathfrak{q})$. We have to prove that $e = n$. Since $v_{\mathfrak{q}}(\vartheta) \geq 1$, we have $v_{\mathfrak{q}}(a_j\vartheta^{n-j}) \geq e + 1$ for $1 \leq j < n$. The identity

$$\vartheta^n + a_n = -(a_1\vartheta^{n-1} + \cdots + a_{n-1}\vartheta)$$

yields $v_{\mathfrak{q}}(\vartheta^n + a_n) \geq e + 1$ and since $v_{\mathfrak{q}}(a_n) = e$, because f is an Eisenstein \mathfrak{p} -polynomial, it follows that $v_{\mathfrak{q}}(\vartheta^n) = e$. So $n \mid e$ and, therefore, $e = n$. \square

Note that the ϑ in the Theorem can be any element of S with $v_{\mathfrak{q}}(\vartheta) = 1$, where \mathfrak{q} is the prime ideal above \mathfrak{p} .

Locally we have:

7.21 Theorem. *Let R be a discrete valuation ring. Suppose that \mathfrak{p} totally ramifies in L . Then $S = R[\vartheta]$ for any $\vartheta \in S$ with $v_{\mathfrak{q}}(\vartheta) = 1$ for \mathfrak{q} the prime ideal of S above \mathfrak{p} .*

PROOF. By (the proof of) Theorem 7.20: $L = K(\vartheta)$. Clearly $R[\vartheta] \subseteq S$. Let $c_0, \dots, c_{n-1} \in K$ such that

$$c_0 + c_1\vartheta + \dots + c_{n-1}\vartheta^{n-1} \in S.$$

Then to prove that $v_{\mathfrak{p}}(c_i) \geq 0$ for $i = 0, \dots, n-1$. Suppose that $v_{\mathfrak{p}}(c_i) < 0$ for some i . Let i be the least such that $v_{\mathfrak{p}}(c_i) < 0$. Then

$$c_i\vartheta^i + \dots + c_{n-1}\vartheta^{n-1} \in S.$$

Since $i < n$, we have $\frac{\pi}{\vartheta^{i+1}} \in S$ and multiplication by this element yields

$$c_i \frac{\pi}{\vartheta} + c_{i+1}\pi + c_{i+2}\pi\vartheta + \dots \in S$$

and so $c_i \frac{\pi}{\vartheta} \in S$. However,

$$v_{\mathfrak{q}}\left(c_i \frac{\pi}{\vartheta}\right) = v_{\mathfrak{q}}(a_i) + n - 1 \leq -n + n - 1 = -1. \quad \square$$

7.2 Ramification and discriminant

This section is about a generalization of Theorem 3.30. In this section

R	is a Dedekind domain,
K	the field of fractions of R ,
$L : K$	a finite separable field extension,
S	the integral closure of R in L .

Since R is in general not a principal ideal domain we need a more general notion of discriminant. The discriminant of S over R will not be an element of R , but an ideal of R :

7.22 Definition. The *discriminant* of S over R (or the *R -discriminant* of L) is the ideal of R generated by all $\text{disc}(\alpha_1, \dots, \alpha_n)$, where $(\alpha_1, \dots, \alpha_n)$ is a K -basis of L with $\alpha_1, \dots, \alpha_n \in S$. Notation: $\mathfrak{d}_R(L)$.

Note that the ring S is determined by R and L . This is reflected in the notation $\mathfrak{d}_R(L)$. The discriminant of a number field K is $\text{disc}(\alpha_1, \dots, \alpha_n)$, where $(\alpha_1, \dots, \alpha_n)$ is an integral basis of K . The \mathbb{Z} -discriminant of K is the ideal $(\text{disc}(\alpha_1, \dots, \alpha_n))$ of \mathbb{Z} . In the terminology for number fields, as will be explained in Terminology 7.31: $\mathfrak{d}_{\mathbb{Q}}(K) = (\text{disc}(K))$.

Under localization the discriminant behaves as expected:

7.23 Proposition. *Let $P \subseteq \text{Max}(R)$ Then*

$$\mathfrak{d}_R(L)R_P = \mathfrak{d}_{R_P}(L).$$

PROOF. Let Q be the set of maximal ideals of S above maximal ideals in P . The ring S_Q is the integral closure of R_P in L (Theorem 7.7). If the elements of a K -basis of L are in the subring S , then they are in S_Q , so the generators of the ideal $\mathfrak{d}_R(S)$ of R form a subset of the generators of the ideal $\mathfrak{d}_{R_P}(L)$ of R_P . Hence $\mathfrak{d}_R(L)R_P \subseteq \mathfrak{d}_{R_P}(L)$. Let $\alpha_1, \dots, \alpha_n$ be a K -basis of L with $\alpha_1, \dots, \alpha_n \in S_Q$. We have to show that $\text{disc}(\alpha_1, \dots, \alpha_n) \in \mathfrak{d}_R(L)R_P$. By Proposition 6.25 this is equivalent to $v_{\mathfrak{p}}(\text{disc}(\alpha_1, \dots, \alpha_n)) \geq v_{\mathfrak{p}}(\mathfrak{d}_R(L))$ for all $\mathfrak{p} \in P$. For a given $\mathfrak{p} \in P$ take $t \in R$ such that $v_{\mathfrak{p}}(t) = 0$ and $t\alpha_1, \dots, t\alpha_n \in S$. Then $\text{disc}(t\alpha_1, \dots, t\alpha_n) = t^{2n} \text{disc}(\alpha_1, \dots, \alpha_n)$ and, therefore, $v_{\mathfrak{p}}(\text{disc}(\alpha_1, \dots, \alpha_n)) = v_{\mathfrak{p}}(\text{disc}(t\alpha_1, \dots, t\alpha_n)) \geq v_{\mathfrak{p}}(\mathfrak{d}_R(L))$. \square

It follows that the discriminant is determined locally:

7.24 Corollary. $\mathfrak{d}_R(L) = \prod_{\mathfrak{p} \in \text{Max}(R)} \mathfrak{d}_{R_{\mathfrak{p}}}(L) \cap R$.

PROOF. For $\mathfrak{p} \in \text{Max}(R)$ denote $\mathfrak{p}R_{\mathfrak{p}}$ by \mathfrak{p}' . By Proposition 6.23, Corollary 6.26 and Proposition 7.23 we have for all $\mathfrak{p} \in \text{Max}(R)$:

$$\begin{aligned} v_{\mathfrak{p}}(\mathfrak{d}_{R_{\mathfrak{p}}}(L) \cap R) &= v_{\mathfrak{p}'}((\mathfrak{d}_{R_{\mathfrak{p}}}(L) \cap (R)r_{\mathfrak{p}})) = v_{\mathfrak{p}'}(\mathfrak{d}_{R_{\mathfrak{p}}}(L)) = v_{\mathfrak{p}'}(\mathfrak{d}_R(L)R_{\mathfrak{p}}) \\ &= v_{\mathfrak{p}}(\mathfrak{d}_R(L)). \end{aligned} \quad \square$$

7.25 Theorem. *Let $(\alpha_1, \dots, \alpha_n)$ be a K -basis of L with $\alpha_1, \dots, \alpha_n \in S$. Then $(\alpha_1, \dots, \alpha_n)$ is an R -basis of S if and only if $\mathfrak{d}_R(L) = \text{disc}(\alpha_1, \dots, \alpha_n)R$.*

PROOF. Suppose $(\alpha_1, \dots, \alpha_n)$ is an R -basis of S . The ideal $\mathfrak{d}_R(L)$ is generated by all $\text{disc}(\beta_1, \dots, \beta_n)$ such that $(\beta_1, \dots, \beta_n)$ is a K -basis of L and $\beta_1, \dots, \beta_n \in S$. Let $(\beta_1, \dots, \beta_n)$ be such a basis. Then by Proposition 1.27

$$\text{disc}(\beta_1, \dots, \beta_n) = \det(M)^2 \text{disc}(\alpha_1, \dots, \alpha_n),$$

where M is the transition matrix from $(\beta_1, \dots, \beta_n)$ to $(\alpha_1, \dots, \alpha_n)$. Because $(\alpha_1, \dots, \alpha_n)$ is an R -basis of S , the entries of M are in R . It follows that $\text{disc}(\beta_1, \dots, \beta_n) \in \text{disc}(\alpha_1, \dots, \alpha_n)R$. Hence $\mathfrak{d}_R(L) = \text{disc}(\alpha_1, \dots, \alpha_n)R$.

For the converse suppose that $\mathfrak{d}_R(L) = \text{disc}(\alpha_1, \dots, \alpha_n)R$. Let $\mathfrak{p} \in \text{Max}(R)$ and Q the set of prime ideals of S above \mathfrak{p} . Then by Proposition 7.23 $\mathfrak{d}_{R_{\mathfrak{p}}}(L) = \mathfrak{d}_R(L)R_{\mathfrak{p}} = \text{disc}(\alpha_1, \dots, \alpha_n)R_{\mathfrak{p}}$. Since $R_{\mathfrak{p}}$ is a discrete valuation ring, S_Q has an $R_{\mathfrak{p}}$ -basis, say $(\beta_1, \dots, \beta_n)$ and for this basis we have $\text{disc}(\beta_1, \dots, \beta_n)R_{\mathfrak{p}} = \mathfrak{d}_{R_{\mathfrak{p}}}(L)$. Hence $\text{disc}(\alpha_1, \dots, \alpha_n)R_{\mathfrak{p}} = \text{disc}(\beta_1, \dots, \beta_n)R_{\mathfrak{p}}$. Again by Proposition 1.27

$$\text{disc}(\alpha_1, \dots, \alpha_n) = \det(M)^2 \text{disc}(\beta_1, \dots, \beta_n),$$

where M is the transition matrix from $(\alpha_1, \dots, \alpha_n)$ to $(\beta_1, \dots, \beta_n)$. It follows that $\det(M) \in R_{\mathfrak{p}}^*$. This implies that $(\alpha_1, \dots, \alpha_n)$ is an $R_{\mathfrak{p}}$ -basis of S_Q . Let $x \in S$. Then there are unique $b_1, \dots, b_n \in K$ such that $x = b_1\alpha_1 + \dots + b_n\alpha_n$. Since $(\alpha_1, \dots, \alpha_n)$ is an $R_{\mathfrak{p}}$ -basis of S_Q , we have $b_1, \dots, b_n \in R_{\mathfrak{p}}$. This holds for all $\mathfrak{p} \in \text{Max}(R)$. Hence $b_1, \dots, b_n \in R$ and so $(\alpha_1, \dots, \alpha_n)$ is an R -basis of S . \square

In particular we have the following.

7.26 Corollary. *Let $\vartheta \in S$ be a primitive element of $L : K$ and $f \in R[X]$ the minimal polynomial of ϑ over K . Then $\mathfrak{d}_R(L) = \text{disc}(f)R$ if and only if $S = R[\vartheta]$. \square*

The following generalizes Lemma 3.29.

7.27 Lemma. *Let $\mathfrak{p} \in \text{Max}(R)$ and $\alpha_1, \dots, \alpha_n \in S$ such that $(\overline{\alpha_1}, \dots, \overline{\alpha_n})$ is an R/\mathfrak{p} -basis of $S/\mathfrak{p}S$. Then $\mathfrak{p} \mid \mathfrak{d}_R(L)$ if and only if $\text{disc}(\alpha_1, \dots, \alpha_n) \in \mathfrak{p}$.*

PROOF. Put $v_{\mathfrak{p}}(\mathfrak{d}_R(L)) = k$. Then $\mathfrak{d}_R(L)R_{\mathfrak{p}} = \mathfrak{p}^k R_{\mathfrak{p}}$. Proposition 7.23, with $P = \{\mathfrak{p}\}$ gives

$$\mathfrak{p} \mid \mathfrak{d}_R(L) \iff \mathfrak{p}R_{\mathfrak{p}} \mid \mathfrak{d}_R(L)R_{\mathfrak{p}} \iff \mathfrak{p}R_{\mathfrak{p}} \mid \mathfrak{d}_{R_{\mathfrak{p}}}(L).$$

Let Q be the set of maximal ideals of S above \mathfrak{p} . The ring $R_{\mathfrak{p}}$ is a principal ideal domain. So L has a K -basis $(\beta_1, \dots, \beta_n)$ which is an $R_{\mathfrak{p}}$ -basis of S_Q and by Theorem 7.25 we have

$$\mathfrak{d}_{R_{\mathfrak{p}}}(L) = \text{disc}(\beta_1, \dots, \beta_n)R_{\mathfrak{p}}.$$

Let T be the transition matrix from $(\alpha_1, \dots, \alpha_n)$ to $(\beta_1, \dots, \beta_n)$. Then $T \in M_n(R_{\mathfrak{p}})$ and

$$\text{disc}(\alpha_1, \dots, \alpha_n) = \det(T)^2 \text{disc}(\beta_1, \dots, \beta_n).$$

Since $(\overline{\alpha_1}, \dots, \overline{\alpha_n})$ and $(\overline{\beta_1}, \dots, \overline{\beta_n})$ both are $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$ -bases of $S_Q/\mathfrak{p}S_Q$, we have $\det(T) \in R_{\mathfrak{p}}^*$. So we have

$$\mathfrak{d}_{R_{\mathfrak{p}}}(L) = \text{disc}(\beta_1, \dots, \beta_n)R_{\mathfrak{p}} = \text{disc}(\alpha_1, \dots, \alpha_n)R_{\mathfrak{p}}.$$

Therefore,

$$\mathfrak{p} \mid \mathfrak{d}_R(L) \iff \mathfrak{p}R_{\mathfrak{p}} \mid \mathfrak{d}_{R_{\mathfrak{p}}}(L) \iff \text{disc}(\alpha_1, \dots, \alpha_n) \in \mathfrak{p}R_{\mathfrak{p}} \cap R = \mathfrak{p}. \quad \square$$

The proof of Theorem 3.30 now easily generalizes to a proof of the following theorem using Lemma 7.27.

7.28 Theorem. *Let $\mathfrak{p} \in \text{Max}(R)$. Then*

$$\mathfrak{p} \text{ ramifies in } L \iff \mathfrak{p} \mid \mathfrak{d}_R(L).$$

PROOF. First assume that \mathfrak{p} does not ramify in S , say $\mathfrak{p}S = \mathfrak{q}_1 \cdots \mathfrak{q}_r$ with $\mathfrak{q}_1, \dots, \mathfrak{q}_r$ the different maximal ideals of S above \mathfrak{p} . Put $f_i = f_R(\mathfrak{q}_i)$ for $i = 1, \dots, r$. As in the proof of Theorem 3.30 one constructs a K -basis

$$(\alpha_{11}, \dots, \alpha_{1f_1}, \alpha_{21}, \dots, \alpha_{2f_2}, \dots, \dots, \alpha_{r1}, \dots, \alpha_{rf_r})$$

of L consisting of elements of S such that $(\overline{\alpha_{i1}}, \dots, \overline{\alpha_{if_i}})$ is an R/\mathfrak{p} -basis of S/\mathfrak{q}_i for $i = 1, \dots, r$; moreover, $\alpha_{ij}\alpha_{kj} \in \mathfrak{p}S$, and so $\text{Tr}_K^L(\alpha_{ij}\alpha_{kl}) \in \mathfrak{p}$. Then again for the matrix $A = (\text{Tr}_K^L(\alpha_{ij}\alpha_{kl}))$ we have $\det(A) \equiv \det(A_1) \cdot \det(A_2) \cdots \det(A_r) \pmod{\mathfrak{p}}$, where the A_i are the $f_i \times f_i$ -matrices $(\text{Tr}_K^L(\alpha_{ij}\alpha_{il}))$. Since the $\alpha_{i1}, \dots, \alpha_{if_i}$ form modulo \mathfrak{p} a basis of S/\mathfrak{q}_i , we have in R/\mathfrak{p} :

$$\overline{\text{Tr}_K^L(\alpha_{ij}\alpha_{ik})} = \overline{\text{Tr}(M_{\alpha_{ij}\alpha_{ik}})} = \text{Tr}(M_{\overline{\alpha_{ij}\alpha_{ik}}}).$$

So $\overline{\det(A_i)}$ is the discriminant of the R/\mathfrak{p} -basis of S/\mathfrak{q}_i . By Corollary 1.30 it follows that $\overline{\det(A_i)} \neq 0$, that is $\det(A_i) \notin \mathfrak{p}$. By Lemma 7.27 we have $\mathfrak{p} \nmid \mathfrak{d}_R(L)$.

Assume now that \mathfrak{p} ramifies in S . Then there is a $\mathfrak{q} \in \text{Max}(S)$ above \mathfrak{p} such that $\mathfrak{p}S = \mathfrak{q}\mathfrak{a}$, where \mathfrak{a} is an ideal of S with $\mathfrak{q} \mid \mathfrak{a}$. Choose an $\alpha \in \mathfrak{a} \setminus \mathfrak{p}S$. The ring $S/\mathfrak{p}S$ is an R/\mathfrak{p} -vector space of dimension $n = [L : K]$. The image $\overline{\alpha}$ of α in $S/\mathfrak{p}S$ is not 0, so there are $\alpha_1, \dots, \alpha_n \in S$ such that $(\overline{\alpha_1}, \dots, \overline{\alpha_n})$ is a basis of the R/\mathfrak{p} -vector space $S/\mathfrak{q}S$ and $\alpha_1 = \alpha$. The discriminant of $(\alpha_1, \dots, \alpha_n)$ is the determinant of the matrix $(\text{Tr}_K^L(\alpha_i\alpha_j))$. As in the proof of Theorem 3.30 the entries in the first row of this matrix are all in \mathfrak{p} . Therefore,

$$\text{disc}(\alpha_1, \dots, \alpha_n) = \det(\text{Tr}(\alpha_i\alpha_j)) \in \mathfrak{p}.$$

From Lemma 7.27 follows that $\mathfrak{p} \mid \mathfrak{d}_R(L)$. □

7.29 Proposition. *Let R be a principal ideal domain, L_1 and L_2 intermediate fields of $L : K$ such that $L = L_1L_2$ and $[L : K] = [L_1 : K][L_2 : K]$. Then*

$$(\mathfrak{d}_R(L_1) + \mathfrak{d}_R(L_2))S \subseteq S_1S_2.$$

PROOF. Let S_1 and S_2 be the integral closures of R in L_1 and L_2 respectively. By Corollary 1.38 there are K -bases $\alpha_1, \dots, \alpha_{n_1}$ and $\beta_1, \dots, \beta_{n_2}$ of L_1 and L_2 respectively such that $S_1 = R\alpha_1 + \cdots + R\alpha_{n_1}$ and $S_2 = R\beta_1 + \cdots + R\beta_{n_2}$. Put $d_1 = \text{disc}(\alpha_1, \dots, \alpha_{n_1})$ and $d_2 = \text{disc}(\beta_1, \dots, \beta_{n_2})$. By Theorem 7.25 $\mathfrak{d}_R(L_1) = Rd_1$ and $\mathfrak{d}_R(L_2) = Rd_2$. As in the proof of Theorem 1.50 we have

$$d_1S \subseteq S_1S_2 \quad \text{and} \quad d_2S \subseteq S_1S_2. \quad \square$$

7.30 Theorem. Let L_1 and L_2 intermediate fields of $L : K$ such that $L = L_1L_2$ and $[L : K] = [L_1 : K][L_2 : K]$. Suppose that $\mathfrak{p} \in \text{Max}(R)$ ramifies in L_1 and does not ramify in L_2 . Then

$$v_{\mathfrak{p}}(\mathfrak{d}_R(L)) = v_{\mathfrak{p}}(\mathfrak{d}_R(L_1))^{[L_2:K]}.$$

PROOF. Let S_1 and S_2 be the integral closures of R in L_1 and L_2 respectively. First we prove the theorem under the extra assumption that R is a discrete valuation ring and use the notations in the proof of Proposition 7.29. By Proposition 1.33 the discriminant d of the K -basis of the products $\alpha_i\beta_j$ equals $d_1^{n_2}d_2^{n_1}$. By Theorem 7.28 $\mathfrak{d}_R(L_2) = (1)$, so Proposition 7.29 implies that $S = S_1S_2$ and it follows that the elements $\alpha_i\beta_j$ form an R -basis of S . We have

$$\mathfrak{d}_R(L) = Rd = (Rd_1)^{n_2}(Rd_2)^{n_1} = (\mathfrak{d}_R(L_1))^{n_2}(\mathfrak{d}_R(L_2))^{n_1} = (\mathfrak{d}_R(L_1))^{n_2}.$$

The general case is done by localization. Let $P = \{\mathfrak{p}\}$ and Q, Q_1 and Q_2 the sets of prime ideals of respectively S, S_1 and S_2 above \mathfrak{p} . Then $\mathfrak{d}_{R_{\mathfrak{p}}}(L_2) = \mathfrak{d}_R(L_2)R_{\mathfrak{p}} = R_{\mathfrak{p}}$. The ring $R_{\mathfrak{p}}$ is a discrete valuation ring, so we have

$$\mathfrak{d}_R(L)R_{\mathfrak{p}} = (\mathfrak{d}_R(L_1))^{n_2}R_{\mathfrak{p}}.$$

The theorem follows from Proposition 6.29. \square

7.31 Terminology for number fields. For a number field extension $L : K$ the *discriminant* of L over K is the discriminant $\mathfrak{d}_{\mathcal{O}_K}(L)$. Notation: $\mathfrak{d}_K(L)$. So we have: $\mathfrak{p} \in \text{Max}(\mathcal{O}_K)$ ramifies in L if and only if $\mathfrak{p} \mid \mathfrak{d}_K(L)$.

7.32 Example. In Example 7.17 it is shown that the prime number 3 totally ramifies in $L = \mathbb{Q}(\alpha, \zeta_3)$, where $\alpha = \sqrt[3]{2}$. The prime ideal of \mathcal{O}_L above 3 is the principal ideal $\mathfrak{p} = (\delta)$. On page 153 the minimal polynomial f of δ over \mathbb{Q} has been computed: $f = X^6 - 3X^4 + 3X^2 + 3$. By Theorem 7.21, Proposition 7.23 and Corollary 7.26 we have

$$v_3(\text{disc}(L)) = v_3(\text{disc}(f)).$$

Indeed, by the computation in Example 7.17: $v_3(\text{disc}(L)) = 7$ and

$$\begin{aligned} \text{disc}(f) &= -N_{\mathbb{Q}}^L(6\delta^5 - 12\delta^3 + 6\delta) = 6^6 \cdot N_{\mathbb{Q}}^L(\delta) \cdot N_{\mathbb{Q}}^L(\delta^4 - 2\delta^2 + 1) \\ &= 6^6 \cdot 3 \cdot N_{\mathbb{Q}}^L(\delta^2 - 1)^2 = 2^6 \cdot 3^7 \cdot N_{\mathbb{Q}}^L(\delta - 1)^2 \cdot N_{\mathbb{Q}}^L(\delta + 1)^2 = 2^{14} \cdot 3^7. \end{aligned}$$

(Of course $3 \nmid N_{\mathbb{Q}}^L(\delta^4 - 2\delta^2 + 1)$, because $\delta^4 - 2\delta^2 + 1 \notin \mathfrak{p}$.)

In Example 7.17 the discriminant of L was computed using the computation of an integral basis. For a computation of the discriminant it is not necessary to have an explicit integral basis. One can argue as follows. Since 2 and 3 are the only prime numbers ramifying in L , the discriminant is of type $\pm 2^k 3^l$. The sign is -1 by Proposition 1.46, the above computation shows that $l = 7$ and by Theorem 7.30 we have $k = 2 \cdot v_2(\text{disc}(K)) = 4$.

7.3 Decomposition groups and inertia groups

We consider the splitting of a prime ideal in a Galois extension. For this section we fix the following notations:

R	a Dedekind domain with the property that <i>all its residue class fields are finite,</i>
K	the field of fractions of R ,
$L : K$	a Galois extension,
$G = \text{Gal}(L : K)$	the Galois group,
S	the integral closure of R in L ,
$\mathfrak{q} \in \text{Max}(S)$	a maximal ideal of S ,
$\mathfrak{p} = \mathfrak{q} \cap K$	the prime ideal of R under \mathfrak{q} ,
Q	the set of prime ideals of S above \mathfrak{p} ,
$f = f_{\mathfrak{p}}^{(L)}$	the residue class degree of \mathfrak{p} in L ,
$e = e_{\mathfrak{p}}^{(L)}$	the ramification index of \mathfrak{p} in L ,
$r = r_{\mathfrak{p}}^{(L)}$	the number of prime ideals of S above \mathfrak{p} ,
$\overline{G} = \text{Gal}(S/\mathfrak{q} : R/\mathfrak{p})$	the Galois group of the residue class field extension.

The extension $S/\mathfrak{q} : R/\mathfrak{p}$ is a Galois extension since it is an extension of finite fields. For R the ring of integers of a number field the condition of residue class fields being finite is satisfied. Without this condition it still follows that this extension is normal (exercise 1). Therefore, most of the results in this section hold under the weaker condition of residue class fields being perfect. In section 7.7, however, it is essential that the residue class fields are finite.

By Theorem 7.13 the group G operates transitively on Q . Consequently, we have the equality of ramification indices and of residue class degrees of the prime ideals in Q over K (Corollary 7.14).

7.33 Definition. The stabilizer of \mathfrak{q} under the action of G on the set Q is called the *decomposition group* of \mathfrak{q} over K . Notation: $Z = Z_K(\mathfrak{q})$. So,

$$Z_K(\mathfrak{q}) = \text{Stab}_G(\mathfrak{q}).$$

The intermediate field L^Z is called the *decomposition field* of \mathfrak{q} over K . (The Z stands for Zerlegung, which is German for decomposition.)

7.34 Proposition. $\#(Z_K(\mathfrak{q})) = ef$.

PROOF. The map

$$G \rightarrow Q, \quad \sigma \mapsto \sigma(\mathfrak{q})$$

is surjective by the transitivity of the action of G . It induces a bijection from the set of left cosets of $Z_K(\mathfrak{q})$ in G to the set of primes above \mathfrak{p} . Hence,

$$(G : Z) = r.$$

From $n = ref$ it follows that $\#(Z_K(\mathfrak{q})) = ef$. □

7.35 Proposition. $r_{\mathfrak{q}^Z}^{(L)} = 1$, $e_{\mathfrak{q}^Z}^{(L)} = e_{\mathfrak{p}}^{(L)}$ and $f_{\mathfrak{q}^Z}^{(L)} = f_{\mathfrak{p}}^{(L)}$. In a diagram:

$$\begin{array}{ccc}
 L & \mathfrak{q} & \\
 ef \downarrow & \downarrow & \text{ramification index} = e \\
 L^Z & \mathfrak{q}^Z & \text{residue class degree} = f \\
 r \downarrow & \downarrow & \\
 K & \mathfrak{p} & \text{ramification index} = 1 \\
 & & \text{residue class degree} = 1
 \end{array}$$

PROOF. For all $\sigma \in Z$ we have $\sigma(\mathfrak{q}) = \mathfrak{q}$. Since Z acts transitively on the set of primes of L above \mathfrak{q}^Z , it follows that $r_{\mathfrak{q}^Z}^{(L)} = 1$. The proposition follows from

$$[L : L^Z] = \#(Z) = ef, \quad [L : L^Z] = e_{\mathfrak{q}^Z}^{(L)} f_{\mathfrak{q}^Z}^{(L)}, \quad e_{\mathfrak{q}^Z}^{(L)} \mid e \quad \text{and} \quad f_{\mathfrak{q}^Z}^{(L)} \mid f. \quad \square$$

The elements of $Z_K(\mathfrak{q})$ are the automorphisms $\sigma \in G$ which induce an automorphism of S/\mathfrak{q} . The map

$$Z_K(\mathfrak{q}) \rightarrow \overline{G}, \quad \sigma \mapsto \overline{\sigma}$$

clearly is a group homomorphism. Its kernel consists of all $\sigma \in Z$ with $\overline{\sigma} = 1$, that is $\sigma(\alpha) \equiv \alpha \pmod{\mathfrak{q}}$ for all $\alpha \in S$.

7.36 Definition. The subgroup of Z of all $\sigma \in Z$ with

$$\sigma(\alpha) \equiv \alpha \pmod{\mathfrak{q}} \quad \text{for all } \alpha \in S$$

is called the *inertia group* of \mathfrak{q} over K . Notation: $T = T_K(\mathfrak{q})$. (Trägheit is German for inertia.)

Since T is the kernel of the group homomorphism $Z \rightarrow \overline{G}$, it is a normal subgroup of Z . In Theorem 7.40 we will see that the homomorphism is surjective. Decomposition groups and inertia groups of prime ideals above the same prime ideal of the base field are related as follows.

7.37 Proposition. Let $\sigma \in G$. Then $Z_K(\sigma(\mathfrak{q})) = \sigma Z_K(\mathfrak{q}) \sigma^{-1}$ and $T_K(\sigma(\mathfrak{q})) = \sigma T_K(\mathfrak{q}) \sigma^{-1}$.

PROOF. For all $\tau \in G$:

$$\begin{aligned} \tau \in Z_K(\sigma(\mathfrak{q})) &\iff \tau\sigma(\mathfrak{q}) = \sigma(\mathfrak{q}) \iff \sigma^{-1}\tau\sigma(\mathfrak{q}) = \mathfrak{q} \\ &\iff \sigma^{-1}\tau\sigma \in Z_K(\mathfrak{q}) \iff \tau \in \sigma Z_K(\mathfrak{q})\sigma^{-1} \end{aligned}$$

and

$$\begin{aligned} \tau \in T_K(\sigma(\mathfrak{q})) &\iff \tau(\alpha) \equiv \alpha \pmod{\sigma(\mathfrak{q})} \text{ for all } \alpha \in S \\ &\iff \sigma^{-1}\tau(\alpha) \equiv \sigma^{-1}(\alpha) \pmod{\mathfrak{q}} \text{ for all } \alpha \in S \\ &\iff \sigma^{-1}\tau\sigma(\alpha) \equiv \alpha \pmod{\mathfrak{q}} \text{ for all } \alpha \in S \\ &\iff \sigma^{-1}\tau\sigma \in T_K(\mathfrak{q}) \iff \tau \in \sigma T_K(\mathfrak{q})\sigma^{-1}. \quad \square \end{aligned}$$

It follows that the decomposition group only depends on the prime ideal \mathfrak{p} if this group is a normal subgroup of the Galois group. Similarly for the inertia group.

7.38 Definition and notations. If $Z_K(\mathfrak{q}) \trianglelefteq G$, the group $Z_K(\mathfrak{q})$ is also called the *decomposition group of \mathfrak{p} in L* . Notation $Z_{\mathfrak{p}}^{(L)}$. Similarly, if $T_K(\mathfrak{q}) \trianglelefteq G$, the group $T_K(\mathfrak{q})$ is also called the *inertia group of \mathfrak{p} in L* . Notation $T_{\mathfrak{p}}^{(L)}$.

7.39 Lemma. *The prime \mathfrak{q}^T of L^T totally ramifies in L .*

PROOF. Since $r_{\mathfrak{q}^T}^{(L)} = 1$ (Proposition 7.35), it remains to show that $f_{\mathfrak{q}^T}^{(L)} = 1$, that is $[S/\mathfrak{q} : S^T/\mathfrak{q}^T] = 1$. Let $\alpha \in S$ and consider

$$\Delta_{\alpha}(X) = \prod_{\sigma \in T} (X - \sigma(\alpha)),$$

the characteristic polynomial of α over L^T . From $\sigma(\alpha) \equiv \alpha \pmod{\mathfrak{q}}$ for all $\sigma \in T$ it follows that

$$\overline{\Delta_{\alpha}}(X) = (X - \overline{\alpha})^{\#(T)} \in (S/\mathfrak{q})[X].$$

Since $\Delta_{\alpha}(X) \in S^T[X]$ we have in fact

$$(X - \overline{\alpha})^{\#(T)} \in (S^T/\mathfrak{q}^T)[X].$$

The extension $S/\mathfrak{q} : S^T/\mathfrak{q}^T$, being an extension of finite fields, is separable. Therefore, $X - \overline{\alpha}$ is the minimal polynomial of $\overline{\alpha}$ over S^T/\mathfrak{q}^T . Hence $\overline{\alpha} \in S^T/\mathfrak{q}^T$ for all $\alpha \in S$. \square

7.40 Theorem. *The group homomorphism $Z \rightarrow \overline{G}$ induces an isomorphism*

$$Z/T \xrightarrow{\sim} \overline{G}.$$

PROOF. The homomorphism $Z/T \rightarrow \overline{G}$ is injective by definition of T . By Lemma 7.39 and Proposition 7.35 we have $f_{\mathfrak{q}^Z}^{(L^T)} = f$, and so $\#(Z/T) = [L^T : L^Z] \geq f$. \square

Summarizing:

7.41 Theorem. For the primes \mathfrak{p} , \mathfrak{q}^Z , \mathfrak{q}^T and \mathfrak{q} we have:

L	\mathfrak{q}	ramification index = e	(\mathfrak{q}^T totally ramifies in L)
$e \mid$	\mid	residue class degree = 1	
L^T	\mathfrak{q}^T	ramification index = 1	(\mathfrak{q}^Z remains prime in L^T)
$f \mid$	\mid	residue class degree = f	
L^Z	\mathfrak{q}^Z	ramification index = 1	
$r \mid$	\mid	residue class degree = 1	
K	\mathfrak{p}		

□

7.42 Example. Let $L = \mathbb{Q}(\alpha, \zeta_3)$ and $K = \mathbb{Q}$, where $\alpha = \sqrt[3]{2}$, see also Example 7.17. There \mathcal{O}_L , $\text{disc}(L)$ and \mathcal{O}_L^* have been computed. Only the primes 2 and 3 ramify in L . Since $G = \text{Gal}(L : \mathbb{Q})$ is not cyclic no prime number remains prime in L . Let's look at the factorization of the primes 2, 3, 5 and 7.

$p = 2$: 2 totally ramifies in $\mathbb{Q}(\alpha)$: $(2) = (\alpha)^3$. So $3 \mid e_2^{(L)}$. On the other hand 2 remains prime in $\mathbb{Q}(\zeta_3)$. Hence the prime ideal factorization in L is $(2) = \mathfrak{p}_2^3$, where $\mathfrak{p}_2 = (\alpha)$. Since $\#(T) = e_2^{(L)} = 3$, we have $L^T = \mathbb{Q}(\zeta_3)$. Clearly $Z = G$ and so $L^Z = \mathbb{Q}$. The prime 2 remains prime in $\mathbb{Q}(\zeta_3)$ and subsequently totally ramifies in L .

$p = 3$: In Example 7.16 it was shown that 3 totally ramifies in L : $(3) = (\delta)^6$. In this case $G = Z = T$ and so $L^T = L^Z = \mathbb{Q}$.

$p = 5$: The prime ideal factorization of (5) in $\mathbb{Q}(\alpha)$ is:

$$(5) = (5, \alpha + 2)(5, \alpha^2 - 2\alpha - 1).$$

This implies that $2 \mid f_5^{(L)}$ and $f_5^{(L)} \neq 6$. So $f_5^{(L)} = 2$. Take a prime \mathfrak{q} above the prime $(5, \alpha + 2)$ of $\mathbb{Q}(\alpha)$. Then $\#(T) = e_5^{(L)} = 1$, $\#(Z) = \#(Z/T) = f_5^{(L)} = 2$. Therefore, $L^T = L$ and, since $\tau \in G$ with $\tau(\alpha) = \alpha$ and $\tau \neq 1$ satisfies $\tau(\mathfrak{q}) = \mathfrak{q}$, we have $Z = \langle \tau \rangle$, that is $L^Z = \mathbb{Q}(\alpha)$. So the prime $(5, \alpha + 2)$ of $\mathbb{Q}(\alpha)$ remains prime in L . Note that, however, 5 does not split completely in L^Z .

$p = 7$: 7 remains prime in $\mathbb{Q}(\alpha)$ and splits completely in $\mathbb{Q}(\zeta_3)$. So for any of the two prime ideals of \mathcal{O}_L above 7 we have $L^T = L$ and $L^Z = \mathbb{Q}(\zeta_3)$.

7.43 Example. Let $L = \mathbb{Q}(\zeta_m)$, p a prime number and $m = p^r m_0$ with $p \nmid m_0$. According to Theorem 3.16 (or Example 7.16) we have $e_p^{(L)} = \varphi(p^r)$. Since p does not ramify in $\mathbb{Q}(\zeta_{m_0})$, prime ideals of $\mathbb{Z}[\zeta_{m_0}]$ above p totally ramify in L and it follows that $L^T = \mathbb{Q}(\zeta_{m_0})$.

For K' an intermediate field of $L : K$, the decomposition group and the inertia group of \mathfrak{q} over K' are the intersections of respectively Z and T with $\text{Gal}(L : K')$:

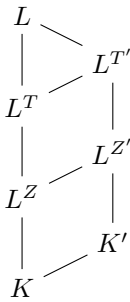
7.44 Proposition. *Let H be a subgroup of G . Then $Z_{L^H}(\mathfrak{q}) = H \cap Z_K(\mathfrak{q})$ and $T_{L^H}(\mathfrak{q}) = H \cap T_K(\mathfrak{q})$.*

PROOF. For a $\sigma \in G$ we have:

$$\sigma \in Z_{L^H}(\mathfrak{q}) \iff \sigma \in H \text{ and } \sigma(\mathfrak{q}) = \mathfrak{q} \iff \sigma \in H \text{ and } \sigma \in Z_K(\mathfrak{q})$$

and

$$\begin{aligned} \sigma \in T_{L^H}(\mathfrak{q}) &\iff \sigma \in H \text{ and } \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{q}} \text{ for all } \alpha \in S \\ &\iff \sigma \in H \text{ and } \sigma \in T_K(\mathfrak{q}). \end{aligned} \quad \square$$



7.45 Corollary. *Let K' be an intermediate field of $L : K$. Then for $Z' = Z_{K'}(\mathfrak{q})$ and $T' = T_{K'}(\mathfrak{q})$ we have*

$$L^{Z'} = L^Z K' \quad \text{and} \quad L^{T'} = L^T K'.$$

PROOF. Apply Proposition 7.44 for $H = \text{Gal}(L : K')$ and use the Galois correspondence. \square

For L' an intermediate field of $L : K$ such that $L' : K$ is a Galois extension, the decomposition group and the inertia group of $\mathfrak{q} \cap L'$ over K are the images of respectively Z and T in $\text{Gal}(L' : K)$. More precisely:

7.46 Proposition. *Let N be a normal subgroup of G . Then the isomorphism*

$$G/N \xrightarrow{\sim} \text{Gal}(L^N : K), \quad \sigma N \mapsto \sigma|_{L^N}$$

induces isomorphisms

$$Z_K(\mathfrak{q})/(N \cap Z_K(\mathfrak{q})) \xrightarrow{\sim} Z_K(\mathfrak{q}^N) \quad \text{and} \quad T_K(\mathfrak{q})/(N \cap T_K(\mathfrak{q})) \xrightarrow{\sim} T_K(\mathfrak{q}^N).$$

PROOF. Under the group homomorphism

$$f: G \rightarrow \text{Gal}(L^N : K), \quad \sigma \mapsto \sigma|_{L^N}$$

the subgroups $Z_K(\mathfrak{q})$ and $T_K(\mathfrak{q})$ are mapped to $Z_K(\mathfrak{q}^N)$ and $T_K(\mathfrak{q}^N)$ respectively. Indeed, if $\sigma \in Z_K(\mathfrak{q})$, then $\sigma(\mathfrak{q}) = \mathfrak{q}$ and hence $\sigma(\mathfrak{q}^N) = \sigma(\mathfrak{q}) \cap \sigma(L^N) = \mathfrak{q} \cap L^N = \mathfrak{q}^N$, that is $f(\sigma) \in Z_K(\mathfrak{q}^N)$, and similarly, if $\sigma \in T_K(\mathfrak{q})$, then $\sigma(\alpha) \equiv \alpha \pmod{\mathfrak{q}}$ for all $\alpha \in S$, and so also $\sigma(\alpha) \equiv \alpha \pmod{\mathfrak{q}^N}$ for all $\alpha \in S^N$, that is $f(\sigma) \in T_K(\mathfrak{q}^N)$.

It suffices to show that the induced homomorphisms

$$\begin{aligned} Z_K(\mathfrak{q}) &\rightarrow Z_K(\mathfrak{q}^N), & \sigma &\mapsto \sigma|_{L^N} \\ T_K(\mathfrak{q}) &\rightarrow T_K(\mathfrak{q}^N), & \sigma &\mapsto \sigma|_{L^N} \end{aligned}$$

are surjective.

Surjectivity for the decomposition groups. Let $\tau \in Z_K(\mathfrak{q}^N)$. Then there is a $\sigma \in G$ such that $\sigma|_{L^N} = \tau$. Choose $\sigma' \in \text{Gal}(L : L^N) = N$ such that $\sigma'(\mathfrak{q}) = \sigma(\mathfrak{q})$. Then

$$(\sigma')^{-1}\sigma(\mathfrak{q}) = \mathfrak{q} \quad \text{and} \quad (\sigma')^{-1}\sigma|_{L^N} = \tau.$$

Surjectivity for the inertia groups. Let $\tau \in T_K(\mathfrak{q}^N)$. Since we have surjectivity for the decomposition groups, there is a $\sigma \in Z_K(\mathfrak{q})$ such that $\sigma|_{L^N} = \tau$. This automorphism σ induces a $\bar{\sigma} \in \bar{G}$ with $\bar{\sigma}|_{S^N/\mathfrak{q}^N} = \bar{\tau} = 1$. It follows that $\bar{\sigma} \in \text{Gal}(S/\mathfrak{q} : S^N/\mathfrak{q}^N)$. Choose a $\sigma' \in N$ such that $\bar{\sigma}' = \bar{\sigma}$. Then

$$(\sigma')^{-1}\sigma \in T_K(\mathfrak{q}) \quad \text{and} \quad (\sigma')^{-1}\sigma|_{L^N} = \tau. \quad \square$$

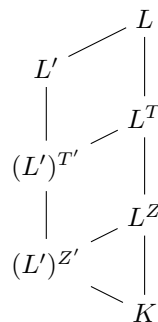
7.47 Corollary. *Let L' be an intermediate field of $L : K$ such that $L' : K$ is a Galois extension. Then for $Z' = Z_K(\mathfrak{q} \cap L')$ and $T' = T_K(\mathfrak{q} \cap L')$ we have*

$$(L')^{Z'} = L^Z \cap L' \quad \text{and} \quad (L')^{T'} = L^T \cap L'.$$

PROOF. For $N = \text{Gal}(L : L')$ we have

$$(L')^{Z'} = (L^N)^{Z'} = L^{NZ'} = L^Z \cap L^N = L^Z \cap L',$$

and similarly for the inertia groups. □



Decomposition groups and inertia groups are convenient tools when studying the splitting behavior of a prime ideal in an extension.

7.48 Theorem. *Suppose $Z \trianglelefteq G$. Let K' be an intermediate field of $L : K$. Then*

$$\mathfrak{p} \text{ splits completely in } K' \iff K' \subseteq L^Z.$$

PROOF. $L^Z : K$ is a Galois extension. By Theorem 7.41 we have $e_{\mathfrak{p}}^{(L^Z)} = f_{\mathfrak{p}}^{(L^Z)} = 1$. Hence $r_{\mathfrak{p}}^{(L^Z)} = [L^Z : K]$. So \mathfrak{p} splits completely in L^Z and it does so in any intermediate field of $L^Z : K$.

Conversely, suppose \mathfrak{p} splits completely in K' . Put $H = \text{Gal}(L : K')$. Then

$$e_{\mathfrak{q}^H}^{(L)} = e \quad \text{and} \quad f_{\mathfrak{q}^H}^{(L)} = f.$$

Hence,

$$\#(Z_{L^H}(\mathfrak{q})) = \#(Z).$$

By Proposition 7.44 we have $H \supseteq Z$, that is $K' \subseteq L^Z$. □

7.49 Corollary. *Suppose $Z \trianglelefteq G$ and $T \trianglelefteq G$. Then \mathfrak{p} splits completely in L^Z into primes that remain prime in L^T and which subsequently totally ramify in L . \square*

7.50 Theorem. *Let L_1 and L_2 be intermediate fields of $L : K$. Then:*

- a) *If \mathfrak{p} does not ramify in both L_1 and L_2 , then \mathfrak{p} does not ramify in L_1L_2 .*
- b) *If \mathfrak{p} splits completely in both L_1 and L_2 , then \mathfrak{p} splits completely in L_1L_2 .*

PROOF.

- a) Put $H_1 = \text{Gal}(L : L_1)$ and $H_2 = \text{Gal}(L : L_2)$. Then $\text{Gal}(L : L_1L_2) = H_1 \cap H_2$. Let $\mathfrak{p}' \in \text{Max}(S^{H_1 \cap H_2})$ be any prime ideal above \mathfrak{p} and choose $\mathfrak{q} \in \text{Max}(S)$ above \mathfrak{p}' . Then $e_K(\mathfrak{q}^{H_1}) = 1$ and $e_K(\mathfrak{q}^{H_2}) = 1$. Hence $e_{\mathfrak{q}^{H_1}}^{(L)} = e$ and $e_{\mathfrak{q}^{H_2}}^{(L)} = e$. Therefore,

$$\#(T_{L^{H_1}}(\mathfrak{q})) = \#(T) \quad \text{and} \quad \#(T_{L^{H_2}}(\mathfrak{q})) = \#(T).$$

By Proposition 7.44 we have $H_1 \supseteq T$ and $H_2 \supseteq T$. Hence $H_1 \cap H_2 \supseteq T$. It follows that $T_{L_1L_2}(\mathfrak{q}) = T$ and so $e_K(\mathfrak{p}') = 1$.

- b) As (i) with Z instead of T . \square

7.51 Corollary. *Let $L : K$ be the normal closure of a field extension $K' : K$. Then*

- a) *\mathfrak{p} does not ramify in $K' \iff \mathfrak{p}$ does not ramify in L ,*
- b) *\mathfrak{p} splits completely in $K' \iff \mathfrak{p}$ splits completely in L .*

PROOF. The field L is the composition of the fields $\sigma(K')$, where $\sigma \in G$. \square

7.4 The splitting of a prime ideal in an extension

In this section we consider the splitting of a prime ideal in a finite *separable* extension. The results will be used in the chapters 8, 15 and 18. A finite separable extension is a subextension of a Galois extension. So let's fix for this section the following notations:

R	a Dedekind domain,
K	the field of fractions of R ,
$L : K$	a Galois extension,
$K' : K$	an intermediate field of $L : K$,
S	the integral closure of R in L ,
$G = \text{Gal}(L : K)$	the Galois group,
$H = \text{Gal}(L : K')$	the subgroup of G corresponding to K' ,
$R' = S^H$	the integral closure of R in K' ,

7.4 The splitting of a prime ideal in an extension

$\mathfrak{q} \in \text{Max}(S)$	a prime ideal of S ,
$Z = Z_K(\mathfrak{q})$	the decomposition group of \mathfrak{q} over K ,
$T = T_K(\mathfrak{q})$	the inertia group of \mathfrak{q} over K ,
$\mathfrak{p} = \mathfrak{q} \cap K$	the prime ideal of R under \mathfrak{q} .

The splitting behavior of \mathfrak{p} in K' will be described in terms of the subgroups H and Z of G . The group G acts on the right on the set $\{H\sigma \mid \sigma \in G\}$ of right cosets of H in G by

$$(H\sigma, \tau) \mapsto H\sigma\tau.$$

A group homomorphism $f: G \rightarrow S(X)$ from a group G to the group $S(X)$ of permutations of a set X corresponds to a left action of G on X : define $g \cdot x = f(g)(x)$. A left action is a map

$$G \times X \rightarrow X, \quad (g, x) \mapsto g \cdot x$$

such that $g \cdot (h \cdot x) = (gh) \cdot x$ and $1 \cdot x = x$ for all $g, h \in G$ and $x \in X$. A *right action* of G on X is a map

$$X \times G \rightarrow X, \quad (x, g) \mapsto x \cdot g$$

such that $(x \cdot g) \cdot h = x \cdot (gh)$ and $x \cdot 1 = x$ for all $g, h \in G$ and $x \in X$. A right action of a group can be seen as a left action of the opposite group. When we say that a group acts (or operates) on a set, we will mean, unless indicated otherwise, that it acts on the left.

The group Z , being a subgroup of G , acts on the right on the right cosets of H in the same way. Let $\{H\sigma \mid \sigma \in G\}_Z$ denote the set of orbits of this action of Z . The orbit of $H\sigma$ is denoted by $[H\sigma]$.

7.52 Lemma. $\#[[H\sigma]] = (Z : (Z \cap \sigma^{-1}H\sigma))$.

PROOF. The map $Z \rightarrow [H\sigma]$, which sends ρ to $H\sigma\rho$, is surjective and for $\rho_1, \rho_2 \in Z$ we have $H\sigma\rho_1 = H\sigma\rho_2$ if and only if $\sigma^{-1}H\sigma\rho_1 = \sigma^{-1}H\sigma\rho_2$. So the number of elements in the orbit of $H\sigma$ under Z equals the number of left cosets of $Z \cap \sigma^{-1}H\sigma$ in Z . \square

7.53 Theorem. *The map*

$$G \longrightarrow \text{Max}(R'), \quad \sigma \mapsto \sigma(\mathfrak{q}) \cap K'$$

induces a bijection

$$\{H\sigma \mid \sigma \in G\}_Z \xrightarrow{\sim} \{\mathfrak{q}' \in \text{Max}(R') \mid \mathfrak{q}' \cap K = \mathfrak{p}\}$$

and for each $\sigma \in G$ we have

$$e_K(\sigma(\mathfrak{q}) \cap K') f_K(\sigma(\mathfrak{q}) \cap K') = (Z : (Z \cap \sigma^{-1}H\sigma)) = \#[[H\sigma]]$$

and

$$e_K(\sigma(\mathfrak{q}) \cap K') = (T : (T \cap \sigma^{-1}H\sigma)).$$

PROOF. The map defined on G factors through $\{H\sigma \mid \sigma \in G\}_Z$: for $\tau \in H$ and $\rho \in Z$ we have

$$\tau\sigma\rho(\mathfrak{q}) \cap K' = \tau\sigma(\mathfrak{q}) \cap K' = \tau(\sigma(\mathfrak{q}) \cap K') = \sigma(\mathfrak{q}) \cap K'.$$

Surjectivity of the induced map follows from the transitivity of the action of G on the set of prime ideals of S above \mathfrak{p} . For the proof of injectivity, let $\sigma_1, \sigma_2 \in G$ satisfy $\sigma_1(\mathfrak{q}) \cap K' = \sigma_2(\mathfrak{q}) \cap K'$. The prime ideals $\sigma_1(\mathfrak{q})$ and $\sigma_2(\mathfrak{q})$ of S are above the same prime ideal of R' , so there is a $\tau \in H$ such that $\tau\sigma_1(\mathfrak{q}) = \sigma_2(\mathfrak{q})$. Then $\sigma_2^{-1}\tau\sigma_1 \in Z$. So $\tau\sigma_1 = \sigma_2\rho$ with $\rho \in Z$. Therefore, $H\sigma_1 = H\sigma_2\rho$, which implies that $[H\sigma_1] = [H\sigma_2]$.

Finally we compute $e_K(\sigma(\mathfrak{q}) \cap K')f_K(\sigma(\mathfrak{q}) \cap K')$. It is equal to the quotient $e_K(\sigma(\mathfrak{q})f_K(\sigma(\mathfrak{q}))/e_{K'}(\sigma(\mathfrak{q}))f_{K'}(\sigma(\mathfrak{q}))$. By Proposition 7.44 we have

$$\begin{aligned} e_{K'}(\sigma(\mathfrak{q}))f_{K'}(\sigma(\mathfrak{q})) &= \#Z_{K'}(\sigma(\mathfrak{q})) = \#(Z_K(\sigma(\mathfrak{q})) \cap H) = \#(\sigma Z\sigma^{-1} \cap H) \\ &= \#(Z \cap \sigma^{-1}H\sigma) \end{aligned}$$

and similarly

$$e_{K'}(\sigma(\mathfrak{q})) = \#(T \cap \sigma^{-1}H\sigma).$$

So by Lemma 7.52

$$\begin{aligned} e_K(\sigma(\mathfrak{q}) \cap K')f_K(\sigma(\mathfrak{q}) \cap K') &= \frac{e_K(\sigma(\mathfrak{q}))f_K(\sigma(\mathfrak{q}))}{e_{K'}(\sigma(\mathfrak{q}))f_{K'}(\sigma(\mathfrak{q}))} = \frac{\#(Z)}{\#(Z \cap \sigma^{-1}H\sigma)} \\ &= \#([H\sigma]) \end{aligned}$$

and

$$e_K(\sigma(\mathfrak{q}) \cap K') = \frac{e_K(\sigma(\mathfrak{q}))}{e_{K'}(\sigma(\mathfrak{q}))} = \frac{\#(T)}{\#(T \cap \sigma^{-1}H\sigma)} \quad \square$$

The prime ideal \mathfrak{q}^Z of S^Z has residue class degree 1 over K . If $L^Z : K$ is a Galois extension, that is if Z is a normal subgroup of G , then \mathfrak{p} splits completely in L^Z . So in that case the number of prime ideals of S^Z above \mathfrak{p} with residue class degree 1 is equal to $[L^Z : K] = \#(G/Z) = (G : Z)$. In the following proposition this is generalized.

7.54 Proposition. *The number of prime ideals of S^Z above \mathfrak{p} with residue class degree 1 is equal to $(N_G(Z) : Z)$.*

The group $N_G(Z)$ is the *normalizer* of Z in G :

$$N_G(Z) = \{\sigma \in G \mid \sigma Z\sigma^{-1} = Z\},$$

the largest subgroup of G having Z as a normal subgroup.

PROOF. By Theorem 7.53 the splitting behavior of \mathfrak{p} in L^Z is given by the action of Z from the right on the right cosets of Z in G . The primes of L^Z above \mathfrak{p} of residue class degree 1 over K correspond to right cosets $Z\sigma$ fixed by the action of Z on the right. By Theorem 7.53 and Lemma 7.52 this is precisely the case when $\sigma Z\sigma^{-1} = Z$. So this number of right cosets is $(N_G(Z) : Z)$. \square

7.5 Ramification groups

Ramification groups are subgroups of the inertia group and provide information on the structure of the inertia group. They will be used in chapter 9 and also in chapter 17. In chapter 9 in the proof of the Kronecker-Weber Theorem, which states that abelian number fields are subfields of cyclotomic fields; in chapter 17 for the proof of the Conductor-Discriminant Formula of class field theory. The notations used in this section are the same as in section 7.3. In this section the residue class fields are assumed to be *finite*.

7.55 Definition. Let $\mathfrak{q} \in \text{Max}(S)$ be above $\mathfrak{p} \in \text{Max}(R)$ and let $i \in \mathbb{N}$. The subgroup

$$V_i = V_i(\mathfrak{q}) = V_{K,i}(\mathfrak{q}) = \{ \sigma \in Z_K(\mathfrak{q}) \mid \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{q}^{i+1}} \text{ for all } \alpha \in S \}$$

is called the i -th *ramification group* of \mathfrak{q} over K . (Note that V_0 is the inertia group.)

7.56 Proposition. For all $i \in \mathbb{N}$ we have $V_i(\mathfrak{q}) \trianglelefteq Z_K(\mathfrak{q})$ and $V_{i+1} \trianglelefteq V_i$. There is an $i_0 \in \mathbb{N}$ such that $V_{i_0} = \{1\}$.

PROOF. Clearly $V_i \trianglelefteq Z$, since V_i is the kernel of a homomorphism:

$$V_i = \text{Ker}(Z \rightarrow \text{Aut}(S/\mathfrak{q}^{i+1})).$$

The inclusion $V_{i+1} \subseteq V_i$ follows directly from the definition. Since G is finite, there is an $i_0 \in \mathbb{N}$ such that $V_i = V_{i_0}$ for all $i \geq i_0$. Let $\sigma \in Z$ with $\sigma \neq 1$. Then there is an $\alpha \in S$ such that $\sigma(\alpha) \neq \alpha$. Let $k = v_{\mathfrak{q}}(\sigma(\alpha) - \alpha)$. Then $\sigma(\alpha) - \alpha \notin \mathfrak{q}^{k+1}$, which implies that $\sigma \notin V_k$. Therefore, $\sigma \notin V_{i_0}$. Hence $V_{i_0} = \{1\}$. \square

So we have a chain of groups

$$Z \supseteq T \supseteq V_1 \supseteq V_2 \supseteq \cdots \supseteq V_{i_0} = \{1\}.$$

We will study the factor groups V_{i-1}/V_i for $i \in \mathbb{N}^*$. Theorem 6.19 on the unique representation of residue classes modulo powers of \mathfrak{q} will be used. Let $\pi \in S$ with $v_{\mathfrak{q}}(\pi) = 1$ and let X be a system of representatives of S^T/\mathfrak{q}^T . Since the inclusion $S^T \rightarrow S$ induces an isomorphism $S^T/\mathfrak{q}^T \xrightarrow{\sim} S/\mathfrak{q}$, the set X is a system of representatives of S/\mathfrak{q} as well. For each $\alpha \in S$ and each $i \in \mathbb{N}$ there are unique a_0, \dots, a_i in X such that

$$\alpha \equiv a_0 + a_1\pi + \cdots + a_i\pi^i \pmod{\mathfrak{q}^{i+1}}.$$

Furthermore we assume that $0 \in X$, that is 0 is the representative of \mathfrak{q} . Then for k with $0 \leq k \leq i$ and $\alpha \in S$ we have

$$v_{\mathfrak{q}}(\alpha) = k \iff a_0 = \cdots = a_{k-1} = 0 \text{ and } a_k \neq 0.$$

For $\sigma \in T$ the element $\sigma(\pi)$ alone determines to which ramification group σ belongs:

7.57 Proposition. *Let $\sigma \in T$. Then*

$$\sigma \in V_i \iff \sigma(\pi) \equiv \pi \pmod{\mathfrak{q}^{i+1}}.$$

PROOF. Suppose $\sigma(\pi) \equiv \pi \pmod{\mathfrak{q}^{i+1}}$ and let $\alpha \in S$. Then there are unique $a_0, \dots, a_i \in X$ such that

$$\alpha \equiv a_0 + a_1\pi + \cdots + a_i\pi^i \pmod{\mathfrak{q}^{i+1}}.$$

We have

$$\begin{aligned} \sigma(\alpha) &\equiv \sigma(a_0 + a_1\pi + \cdots + a_i\pi^i) \pmod{\mathfrak{q}^{i+1}} && \text{(since } \sigma(\mathfrak{q}) = \mathfrak{q}) \\ &\equiv a_0 + a_1\sigma(\pi) + \cdots + a_i\sigma(\pi)^i \pmod{\mathfrak{q}^{i+1}} && \text{(since } a_i \in X \subseteq S^T) \\ &\equiv a_0 + a_1\pi + \cdots + a_i\pi^i \pmod{\mathfrak{q}^{i+1}} && \text{(since } \sigma(\pi) \equiv \pi) \end{aligned}$$

So $\sigma(\alpha) \equiv \alpha \pmod{\mathfrak{q}^{i+1}}$ for all $\alpha \in S$, that is $\sigma \in V_i$. □

7.58 Proposition. *T/V_1 is isomorphic to a subgroup of $(S/\mathfrak{q})^*$.*

PROOF. Let $\sigma \in T$. Then $\sigma(\pi) \in \mathfrak{q}$ and there is a unique $a \in X \setminus \{0\}$ such that

$$\sigma(\pi) \equiv a\pi \pmod{\mathfrak{q}^2}.$$

So we have a map

$$f: T \rightarrow (S/\mathfrak{q})^*, \quad \sigma \mapsto \bar{a}.$$

We will show that f is a group homomorphism. Suppose $f(\sigma) = \bar{a}$ and $f(\tau) = \bar{b}$ with $a, b \in X$. Then

$$\begin{aligned} \tau(\pi) &\equiv b\pi \pmod{\mathfrak{q}^2} \\ \sigma\tau(\pi) &\equiv \sigma(b\pi) \pmod{\mathfrak{q}^2} && \text{(since } \sigma(\mathfrak{q}) = \mathfrak{q}) \\ &\equiv b\sigma(\pi) \pmod{\mathfrak{q}^2} && \text{(since } b \in S^T) \\ &\equiv ba\pi \pmod{\mathfrak{q}^2} && \text{(since } f(\sigma) = \bar{a}). \end{aligned}$$

If $c \in X$ with $\sigma\tau(\pi) \equiv c\pi \pmod{\mathfrak{q}^2}$, then $\overline{ab} = \bar{c}$ and so $f(\sigma\tau) = f(\sigma)f(\tau)$. Furthermore $\text{Ker}(f) = V_1$, since $\sigma \in \text{Ker}(f) \iff \sigma(\pi) \equiv \pi \pmod{\mathfrak{q}^2}$. □

7.59 Proposition. *Let $i \geq 2$. Then V_{i-1}/V_i is isomorphic to a subgroup of the additive group S/\mathfrak{q} .*

PROOF. Let $\sigma \in V_{i-1}$. Then $\sigma(\pi) \equiv \pi \pmod{\mathfrak{q}^i}$. There is a unique $a \in X$ such that

$$\sigma(\pi) - \pi \equiv a\pi^i \pmod{\mathfrak{q}^{i+1}}.$$

So we have a map

$$g: V_{i-1} \rightarrow S/\mathfrak{q}, \quad \sigma \mapsto \bar{a}.$$

We will show that it is a group homomorphism. Suppose $f(\sigma) = \bar{a}$ and $f(\tau) = \bar{b}$ with $a, b \in X$. Then

$$\begin{aligned} \tau(\pi) - \pi &\equiv b\pi^i \pmod{\mathfrak{q}^{i+1}}, \\ \sigma\tau(\pi) - \sigma(\pi) &\equiv \sigma(b\pi^i) \pmod{\mathfrak{q}^{i+1}} && \text{(since } \sigma(\mathfrak{q}) = \mathfrak{q}) \\ &\equiv b\sigma(\pi)^i \pmod{\mathfrak{q}^{i+1}} && \text{(since } b \in S^T) \\ \sigma\tau(\pi) - \pi - a\pi^i &\equiv b(\pi + a\pi^i)^i \pmod{\mathfrak{q}^{i+1}} \\ &\equiv b\pi^i \pmod{\mathfrak{q}^{i+1}} && \text{(since } i \geq 2). \end{aligned}$$

If $c \in S$ with $\sigma\tau(\pi) \equiv \pi + c\pi^i \pmod{\mathfrak{q}^{i+1}}$, then $\overline{a+b} = \bar{c}$ and so $f(\sigma\tau) = f(\sigma) + f(\tau)$. Furthermore $\text{Ker}(f) = V_i$, since $\sigma \in \text{Ker}(f) \iff \sigma(\pi) \equiv \pi \pmod{\mathfrak{q}^{i+1}}$. \square

The maps f and g in the proofs of the propositions 7.58 and 7.59 can also be defined by mapping σ to the residue classes of respectively $\frac{\sigma(\pi)}{\pi}$ and $\frac{\sigma(\pi) - \pi}{\pi^i}$ in the discrete valuation ring $S_{\mathfrak{q}}$ modulo its maximal ideal $\mathfrak{q}S_{\mathfrak{q}}$.

In case the group Z/V_1 is abelian, Proposition 7.58 can be strengthened to the following.

7.60 Proposition. *Let Z/V_1 be abelian. Then T/V_1 is isomorphic to a subgroup of $(R/\mathfrak{p})^*$.*

PROOF. We will prove that the image of the map $f: T \rightarrow (S/\mathfrak{q})^*$ constructed in the proof of Proposition 7.58 is contained in the subgroup $(R/\mathfrak{p})^*$. Let $\sigma \in T$ and put $N = \#(R/\mathfrak{p})$. Then to prove that $f(\sigma)^N = f(\sigma)$, that is $a^N \equiv a \pmod{\mathfrak{p}}$, where $a \in X$ is such that $\sigma(\pi) \equiv a\pi \pmod{\mathfrak{q}^2}$.

For all $\beta \in \mathfrak{q}$ we have $\sigma(\beta) \equiv a\beta \pmod{\mathfrak{q}^2}$: if $\beta \equiv b\pi \pmod{\mathfrak{q}^2}$ for a $b \in X$, then

$$\sigma(\beta) \equiv \sigma(b\pi) = b\sigma(\pi) \equiv ab\pi \equiv a\beta \pmod{\mathfrak{q}^2}.$$

The map $Z \rightarrow \overline{G}$ is surjective. Take $\varphi \in Z$ such that its image in \overline{G} is the generator $x \mapsto x^N$ of \overline{G} . Since $\varphi \in Z$, we have $\varphi^{-1}(\pi) \in \mathfrak{q}$ and therefore

$$\sigma(\varphi^{-1}(\pi)) \equiv a \cdot \varphi^{-1}(\pi) \pmod{\mathfrak{q}^2}.$$

Application of φ yields

$$(\varphi\sigma\varphi^{-1})(\pi) \equiv \varphi(a)\pi \equiv a^N\pi \pmod{\mathfrak{q}^2}.$$

Since Z/V_1 is abelian we have $(\varphi\sigma\varphi^{-1})(\pi) \equiv \sigma(\pi) \pmod{\mathfrak{q}^2}$ and so

$$a^N \equiv a \pmod{\mathfrak{p}}. \quad \square$$

The propositions in this section have consequences for the structure of the groups Z , T and V_1 :

7.61 Theorem. *Let p be the characteristic of R/\mathfrak{p} . Then*

- (i) *The group V_1 is a p -group.*
- (ii) *The group V_1 is the Sylow p -subgroup of T .*
- (iii) *The group Z is solvable.*

PROOF.

- (i) This follows from Proposition 7.59: the group S/\mathfrak{q} is a p -group.
- (ii) By (i) and Proposition 7.58: $p \nmid \#(S/\mathfrak{q})^*$.
- (iii) The factor groups of the chain

$$Z \trianglerighteq T \trianglerighteq V_1 \trianglerighteq V_2 \trianglerighteq \cdots \trianglerighteq V_{i_0} = \{1\}$$

are all abelian. □

In particular we have:

7.62 Corollary. *The prime ideal \mathfrak{q} of S is wildly ramified over K if and only if the group V_1 is nontrivial. □*

The group V_1 is also known as the *wild inertia group* of \mathfrak{q} over K .

For K' an intermediate field of $L : K$, the ramification groups of \mathfrak{q} over K' are simply the intersections of the ramification groups over K with $\text{Gal}(L : K')$:

7.63 Proposition. *Let H be a subgroup of $\text{Gal}(L : K)$ and $i \in \mathbb{N}$. Then $V_{L^H, i}(\mathfrak{q}) = V_{K, i}(\mathfrak{q}) \cap H$.*

PROOF. For $\sigma \in Z_K(\mathfrak{q})$ we have

$$\begin{aligned} \sigma \in V_{L^H, i}(\mathfrak{q}) &\iff \sigma \in H \text{ and } \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{q}^{i+1}} \text{ for all } \alpha \in S \\ &\iff \sigma \in H \text{ and } \sigma \in V_{K, i}(\mathfrak{q}). \end{aligned} \quad \square$$

7.64 Example. Let p be an odd prime and $r \in \mathbb{N}^*$. The prime p is the unique prime which ramifies in the cyclotomic field $L = \mathbb{Q}(\zeta_{p^r})$. In fact, p totally ramifies in L and the unique prime ideal of $\mathcal{O}_L = \mathbb{Z}[\zeta_{p^r}]$ is the ideal $\mathfrak{p} = (1 - \zeta_{p^r})$. We compute the ramification groups of \mathfrak{p} over \mathbb{Q} . The group $G = \text{Gal}(L : \mathbb{Q})$ is isomorphic to the cyclic group $(\mathbb{Z}/p^r)^*$ of order $\varphi(p^r) = p^{r-1}(p-1)$. Let $a \in \mathbb{Z}$ be such that $\bar{a} \in (\mathbb{Z}/p^r)^*$ is of order $p-1$. The element $\bar{1+p} \in (\mathbb{Z}/p^r)^*$ is of order p^{r-1} . It generates the subgroup $1 + (\bar{p})$. A descending chain of subgroups is

$$(\mathbb{Z}/p^r)^* \triangleright 1 + (\bar{p}) \triangleright 1 + (\bar{p})^2 \triangleright \cdots \triangleright 1 + (\bar{p})^{r-1} \triangleright 1 + (\bar{p})^r (= \{1\}).$$

The corresponding chain of subgroups of the Galois group G is

$$G \triangleright \text{Gal}(L : \mathbb{Q}(\zeta_p)) \triangleright \text{Gal}(L : \mathbb{Q}(\zeta_{p^2})) \triangleright \cdots \triangleright \text{Gal}(L : \mathbb{Q}(\zeta_{p^{r-1}})) \triangleright \{1\}.$$

For $m \in \mathbb{N}^*$ the kernel of the ring homomorphism $\mathbb{Z}/p^{m+1} \rightarrow \mathbb{Z}/p^m$ is the ideal $(p^m)/(p^{m+1})$. For the multiplicative groups of these local rings we have the short exact sequence

$$1 \longrightarrow (1 + (p)^m)/(1 + (p)^{m+1}) \longrightarrow (\mathbb{Z}/p^{m+1})^* \longrightarrow (\mathbb{Z}/p^m)^* \longrightarrow 1.$$

The group $(1 + (p)^m)/(1 + (p)^{m+1})$ is of order p and is generated by $\overline{1 + p^m}$. Put $V_j = V_{\mathbb{Q},j}(\mathfrak{p})$. Since p totally ramifies, we have $V_0 = G$. The Propositions 7.58 and 7.59 imply that $V_1 = \text{Gal}(L : \mathbb{Q}(\zeta_p))$ and that for $j \geq 2$ the indices $(V_{j-1} : V_j)$ are either 1 or p . Let $m < r$. The group $\text{Gal}(L : \mathbb{Q}(\zeta_{p^m}))$ is generated by the automorphism $\sigma_{1+p^m} : \zeta_{p^r} \mapsto \zeta_{p^r}^{1+p^m}$. We have

$$\sigma_{1+p^m}(\zeta_{p^r}) - \zeta_{p^r} = \zeta_{p^r}^{1+p^m} - \zeta_{p^r} = \zeta_{p^r}(\zeta_{p^r}^{p^m} - 1) = \zeta_{p^r}(\zeta_{p^{r-m}} - 1).$$

It follows that $v_{\mathfrak{p}}(\sigma_{1+p^r}(1 - \zeta_{p^r}) - (1 - \zeta_{p^r})) = v_{\mathfrak{p}}(\sigma_{1+p^r}(\zeta_{p^r}) - \zeta_{p^r}) = p^m$. By Proposition 7.57

$$\sigma_{1+p^m} \in V_{p^m-1} \setminus V_{p^m}.$$

This implies

$$V_j = \text{Gal}(L : \mathbb{Q}(\zeta_{p^m})) \quad \text{if} \quad p^{m-1} \leq j \leq p^m - 1.$$

So the jumps in the descending chain of ramification groups are at $p^m - 1$ for $m = 0, \dots, r - 1$. (A jump at j meaning that $V_{j+1} \neq V_j$.)

7.6 Norms of fractional ideals

For rings of integers of number fields we have the notion of norm of a nonzero ideal. This easily generalizes to a notion of norm of a fractional ideal. It will take values in the group of positive rational numbers. This group is isomorphic to the group of fractional ideals of \mathbb{Z} . We generalize this further. In this section

R	is a Dedekind domain,
K	the field of fractions of R ,
$L : K$	a finite separable field extension,
S	the integral closure of R in L .

7.65 Definitions and notations. We have homomorphisms

$$j_S^R: \mathbb{I}(R) \rightarrow \mathbb{I}(S) \quad \text{and} \quad N_R^S: \mathbb{I}(S) \rightarrow \mathbb{I}(R).$$

The first one is defined by $j_S^R(\mathfrak{a}) = \mathfrak{a}S$, the second one is called a *norm map* and is defined on basis elements $\mathfrak{q} \in \text{Max}(S)$ by $N_R^S(\mathfrak{q}) = (\mathfrak{q} \cap K)^f$, where $f = f_K(\mathfrak{q})$, the residue class degree of \mathfrak{q} over K . The inclusion $K^* \rightarrow L^*$ will be denoted by j_L^K .

Clearly, the map j_S^R is injective, because for each $\mathfrak{p} \in \text{Max}(R)$ the homomorphism $\langle \mathfrak{p} \rangle \rightarrow \langle \mathfrak{q} \mid \mathfrak{q} \text{ above } \mathfrak{p} \rangle$, $\mathfrak{p} \mapsto \mathfrak{p}S$ is injective:

$$\begin{array}{ccc} \langle \mathfrak{p} \rangle & \longrightarrow & \langle \mathfrak{q} \mid \mathfrak{q} \text{ above } \mathfrak{p} \rangle \\ \sim \downarrow & & \downarrow \sim \\ \mathbb{Z} & \longrightarrow & \bigoplus_{\mathfrak{q} \mid \mathfrak{p}S} \mathbb{Z} \end{array}$$

For a tower of extensions we have:

7.66 Lemma. *Let also $M : L$ be a finite separable field extension and T the integral closure of R in M . Then*

$$j_T^S j_S^R = j_T^R: \mathbb{I}(R) \rightarrow \mathbb{I}(T) \quad \text{and} \quad N_R^S N_S^T = N_R^T: \mathbb{I}(T) \rightarrow \mathbb{I}(R). \quad \square$$

7.67 Proposition. *The following diagrams commute:*

$$\begin{array}{ccc} L^* & \longrightarrow & \mathbb{I}(S) \\ j_L^K \uparrow & & \uparrow j_S^R \\ K^* & \longrightarrow & \mathbb{I}(R) \end{array} \qquad \begin{array}{ccc} L^* & \longrightarrow & \mathbb{I}(S) \\ N_K^L \downarrow & & \downarrow N_R^S \\ K^* & \longrightarrow & \mathbb{I}(R) \end{array}$$

The horizontal maps are the homomorphisms which map an element to the principal fractional ideal it generates.

PROOF. It is obvious from the definition that the first square commutes. For the second let's assume first that $L : K$ is a Galois extension. Let $\alpha \in L^*$. Then to prove that $N_R^S(\alpha S) = N_K^L(\alpha)R$. This means that $v_{\mathfrak{p}}(N_R^S(\alpha S)) = v_{\mathfrak{p}}(N_K^L(\alpha))$ for all $\mathfrak{p} \in \text{Max}(R)$. So let $\mathfrak{p} \in \text{Max}(R)$. We have

$$v_{\mathfrak{p}}(N_R^S(\alpha S)) = v_{\mathfrak{p}}\left(N_R^S\left(\prod_{\mathfrak{q}} \mathfrak{q}^{v_{\mathfrak{q}}(\alpha)}\right)\right) = v_{\mathfrak{p}}\left(\prod_{\mathfrak{q}} (\mathfrak{q} \cap K)^{f_K(\mathfrak{q})v_{\mathfrak{q}}(\alpha)}\right)$$

$$= v_{\mathfrak{p}} \left(\prod_{\mathfrak{q}|\mathfrak{p}S} \mathfrak{p}^{f_{\mathfrak{p}}^{(L)} v_{\mathfrak{q}}(\alpha)} \right) = \sum_{\mathfrak{q}|\mathfrak{p}S} f_{\mathfrak{p}}^{(L)} v_{\mathfrak{q}}(\alpha) = f_{\mathfrak{p}}^{(L)} \sum_{\mathfrak{q}|\mathfrak{p}S} v_{\mathfrak{q}}(\alpha).$$

Let $\mathfrak{q} \in \text{Max}(S)$ above \mathfrak{p} . Put $G = \text{Gal}(L : K)$ and $Z = \{\sigma \in G \mid \sigma(\mathfrak{q}) = \mathfrak{q}\}$. Then $\sigma(\mathfrak{q}) = \tau(\mathfrak{q})$ if and only if σ and τ are in the same left coset of Z in G . Therefore,

$$\begin{aligned} v_{\mathfrak{q}}(N_K^L(\alpha)) &= v_{\mathfrak{q}} \left(\prod_{\sigma \in G} \sigma(\alpha) \right) = \sum_{\sigma \in G} v_{\mathfrak{q}}(\sigma(\alpha)) = \sum_{\sigma \in G} v_{\sigma^{-1}(\mathfrak{q})}(\alpha) = \sum_{\sigma \in G} v_{\sigma(\mathfrak{q})}(\alpha) \\ &= \sum_{C \in G/Z} \sum_{\sigma \in C} v_{\sigma(\mathfrak{q})}(\alpha) = \sum_{\mathfrak{q}|\mathfrak{p}S} \#(C) \cdot v_{\mathfrak{q}}(\alpha) = e_{\mathfrak{p}}^{(L)} f_{\mathfrak{p}}^{(L)} \sum_{\mathfrak{q}|\mathfrak{p}S} v_{\mathfrak{q}}(\alpha). \end{aligned}$$

Hence, $v_{\mathfrak{p}}(N_K^L(\alpha)) = f_{\mathfrak{p}}^{(L)} \sum_{\mathfrak{q}|\mathfrak{p}S} v_{\mathfrak{q}}(\alpha)$. So indeed $v_{\mathfrak{p}}(N_K^L(\alpha S)) = v_{\mathfrak{p}}(N_K^L(\alpha))$.

In general, let $M : K$ be the normal closure of $L : K$. Put $t = [M : L]$ and let T be the integral closure of R in M . Since $M : K$ is a Galois extension, by the above we have $N_R^T(\alpha T) = N_K^M(\alpha)R$ for all $\alpha \in M^*$. So in particular for $\alpha \in L^*$:

$$N_R^T(\alpha T) = N_R^S(N_S^T(\alpha T)) = N_R^S(N_L^M(\alpha)S) = N_R^S(\alpha^t S) = N_R^S(\alpha S)^t$$

and

$$N_K^M(\alpha)R = N_K^L(\alpha^t)R = (N_K^L(\alpha)R)^t.$$

Since the group $\mathbb{I}(R)$ is torsion free, it follows that $N_R^S(\alpha S) = N_K^L(\alpha)R$. \square

7.68 Definition and notations. In the notation of Proposition 7.67: the map N_R^S induces a homomorphism $\mathcal{C}(S) \rightarrow \mathcal{C}(R)$, $[\mathfrak{b}] \mapsto [N_R^S(\mathfrak{b})]$. It is called the *transfer* from $\mathcal{C}(S)$ to $\mathcal{C}(R)$ and is denoted by tr_R^S . The inclusion map j_S^R induces a homomorphism $\mathcal{C}(R) \rightarrow \mathcal{C}(S)$, $[\mathfrak{a}] \mapsto [\mathfrak{a}S]$. It is denoted by j_S^R as well.

For $a \in K^*$ we have $N_K^L(a) = a^{[L:K]}$. In other words the composition $N_K^L j_L^K$ is raising to the power $[L : K]$. For fractional ideals we have:

7.69 Proposition. Let $\mathfrak{a} \in \mathbb{I}(R)$. Then $N_R^S j_S^R(\mathfrak{a}) = \mathfrak{a}^{[L:K]}$. If $L : K$ is a Galois extension with Galois group G , then $j_S^R N_R^S(\mathfrak{b}) = \prod_{\sigma \in G} \sigma(\mathfrak{b})$ for all $\mathfrak{b} \in \mathbb{I}(S)$.

PROOF. It suffices to prove that the composition $N_R^S j_S^R$ raises base elements $\mathfrak{p} \in \text{Max}(R)$ to the power $[L : K]$. For such \mathfrak{p} we have by Theorem 7.8

$$N_R^S j_S^R(\mathfrak{p}) = N_R^S \left(\prod_{\mathfrak{q}|\mathfrak{p}S} \mathfrak{q}^{e_{\mathfrak{K}}(\mathfrak{q})} \right) = \prod_{\mathfrak{q}|\mathfrak{p}S} \mathfrak{p}^{e_{\mathfrak{K}}(\mathfrak{q}) f_{\mathfrak{K}}(\mathfrak{q})} = \mathfrak{p}^{[L:K]}.$$

The second assertion follows directly from the splitting behavior of prime ideals in case of a Galois extension: for $\mathfrak{q} \in \text{Max}(S)$, $\mathfrak{p} \in \text{Max}(R)$ under \mathfrak{q} and $f = f_{\mathfrak{p}}^{(L)}$ we have

$$j_S^R N_R^S(\mathfrak{q}) = j_S^R(\mathfrak{p}^f) = (\mathfrak{p}S)^f = \prod_{\sigma \in G} \sigma(\mathfrak{q}). \quad \square$$

7.70 Corollary. $\text{tr}_R^S j_S^R([\mathfrak{a}]) = [\mathfrak{a}]^{[L:K]}$ for all $\mathfrak{a} \in \mathbb{I}^+(R)$. □

Number fields are the fields of fractions of their rings of integers. This is reflected in the terminology and notation in the number field case.

7.71 Notations. Let $L : K$ be a number field extension. The maps $j_{\mathcal{O}_L}^{\mathcal{O}_K}$ and $N_{\mathcal{O}_K}^{\mathcal{O}_L}$ are denoted by j_L^K and N_K^L respectively. Thus we have homomorphisms

$$j_L^K : \mathbb{I}(K) \rightarrow \mathbb{I}(L) \quad \text{and} \quad N_K^L : \mathbb{I}(L) \rightarrow \mathbb{I}(K)$$

and similarly

$$j_L^K : \mathcal{C}(K) \rightarrow \mathcal{C}(L) \quad \text{and} \quad \text{tr}_K^L : \mathcal{C}(L) \rightarrow \mathcal{C}(K).$$

Though the maps $j_L^K : K^* \rightarrow L^*$ and $j_S^R : \mathbb{I}(R) \rightarrow \mathbb{I}(S)$ are injective, the induced map $j_S^R : \mathcal{C}(R) \rightarrow \mathcal{C}(S)$ need not to be so. The following theorem gives a class of extensions for which this map is injective.

7.72 Theorem. Let $m \in \mathbb{N}^*$ with $m > 2$, $L = \mathbb{Q}(\zeta_m)$ and $K = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$. Then the map

$$j_L^K : \mathcal{C}(K) \rightarrow \mathcal{C}(L), \quad [\mathfrak{a}] \rightarrow [\mathfrak{a}\mathcal{O}_L]$$

is injective.

PROOF. We may assume that $m \not\equiv 2 \pmod{4}$. Let $\mathfrak{a} \in \mathbb{I}^+(K)$ such that $\mathfrak{a}\mathcal{O}_L$ is principal. Then to show that \mathfrak{a} is a principal ideal of \mathcal{O}_K . Complex conjugation induces an automorphism τ of L and we have $L^\tau = K$. Let $\alpha \in \mathcal{O}_L$ generate $\mathfrak{a}\mathcal{O}_L$. Then

$$\alpha\mathcal{O}_L = \mathfrak{a}\mathcal{O}_L = \tau(\mathfrak{a})\mathcal{O}_L = \tau(\mathfrak{a}\mathcal{O}_L) = \tau(\alpha\mathcal{O}_L) = \tau(\alpha)\mathcal{O}_L.$$

Hence $\frac{\alpha}{\tau(\alpha)} \in \mathcal{O}_L^*$. For each $\sigma \in \text{Gal}(L : \mathbb{Q})$ we have

$$\left| \sigma\left(\frac{\alpha}{\tau(\alpha)}\right) \right| = \left| \frac{\sigma(\alpha)}{\sigma\tau(\alpha)} \right| = \frac{|\sigma(\alpha)|}{|\tau\sigma(\alpha)|} = 1.$$

So by Lemma 5.45 $\frac{\alpha}{\tau(\alpha)} \in \mu(L)$. We distinguish two cases.

Case 1: m is not a prime power. The proof of Theorem 5.51 shows that in this case the map $\mathcal{O}_L^* \rightarrow \mu(L)$, $\nu \mapsto \frac{\nu}{\tau(\nu)}$ is surjective. So there is a $\nu \in \mathcal{O}_L^*$ such that $\frac{\alpha}{\tau(\alpha)} = \frac{\nu}{\tau(\nu)}$. For $\beta = \alpha\tau(\nu)$ we have $\tau(\beta) = \tau(\alpha)\nu = \alpha\tau(\nu) = \beta$. Therefore, $\beta \in \mathcal{O}_K$. So

$$j_L^K(\mathfrak{a}) = \alpha\mathcal{O}_L = \beta\mathcal{O}_L = j_L^K(\beta\mathcal{O}_K).$$

Since $j_L^K : \mathbb{I}(K) \rightarrow \mathbb{I}(L)$ is injective, it follows that $\mathfrak{a} = \beta\mathcal{O}_K$.

Case 2: m is a prime power, say $m = p^r$. From $\tau(1 - \zeta_m) = -\zeta_m^{-1}(1 - \zeta_m)$ follows that $\frac{1 - \zeta_m}{\tau(1 - \zeta_m)}$ generates $\mu(L)$. Since $\frac{\alpha}{\tau(\alpha)}$ is a root of unity, there is a $k \in \mathbb{Z}$ such that

$$\frac{\alpha}{\tau(\alpha)} = \frac{(1 - \zeta_m)^k}{\tau(1 - \zeta_m)^k}.$$

So $\alpha\tau(1 - \zeta_m)^k \in \mathcal{O}_K$. The prime p totally ramifies in L . Put $\mathfrak{q} = (1 - \zeta_m)\mathcal{O}_L$ and let \mathfrak{p} be the prime of K under \mathfrak{q} . Then $p\mathcal{O}_L = (1 - \zeta_m)^n\mathcal{O}_L = \mathfrak{q}^n$ and $\mathfrak{p}\mathcal{O}_L = \mathfrak{q}^2$, where $n = [L : \mathbb{Q}] = \varphi(m)$. Because $\alpha\tau(1 - \zeta_m)^k \in \mathcal{O}_K$, we have

$$v_{\mathfrak{q}}(\alpha\tau(1 - \zeta_m)^k) = 2 \cdot v_{\mathfrak{p}}(\alpha\tau(1 - \zeta_m)^k)$$

and

$$v_{\mathfrak{q}}(\alpha) = v_{\mathfrak{q}}(\mathfrak{a}\mathcal{O}_L) = 2 \cdot v_{\mathfrak{p}}(\mathfrak{a}).$$

hence $2 \mid v_{\mathfrak{q}}(\tau(1 - \zeta_m)^k) = k \cdot v_{\mathfrak{q}}(1 - \zeta_m) = k$. We have

$$j_L^K(\alpha\tau(1 - \zeta_m)^k\mathcal{O}_K) = \alpha\tau(1 - \zeta_m)^k\mathcal{O}_L = \alpha\mathcal{O}_L \cdot \mathfrak{q}^k = j_L^K(\mathfrak{a})j_L^K(\mathfrak{p}^{k/2}) = j_L^K(\mathfrak{a}\mathfrak{p}^{k/2}).$$

Hence, by injectivity of j_L^K , $\alpha(1 - \zeta_m)^k\mathcal{O}_K = \mathfrak{a}\mathfrak{p}^{k/2}$. Because \mathfrak{q} is a principal ideal, so is \mathfrak{p} :

$$\mathfrak{p} = N_K^L(\mathfrak{q}) = N_K^L((1 - \zeta_m)\mathcal{O}_L) = N_K^L(1 - \zeta_m)\mathcal{O}_K.$$

So also in this case \mathfrak{a} is a principal ideal of \mathcal{O}_K . □

For an arbitrary quadratic extension of number fields by Corollary 7.70 the composition $\text{tr}_K^L j_L^K: \mathcal{C}(K) \rightarrow \mathcal{C}(K)$ sends each class to its square, so the kernel of $j_L^K: \mathcal{C}(K) \rightarrow \mathcal{C}(L)$ is contained in the subgroup ${}_2\mathcal{C}(K)$ of classes having trivial squares. On the ‘odd parts’ of the ideal class groups the map j_L^K is injective. So the extra information in the theorem is that ideal classes of order 2 of $\mathbb{Q}(\zeta_m + \zeta_m^{-1})$ do not vanish in $\mathcal{C}(\mathbb{Q}(\zeta_m))$.

7.7 The Frobenius automorphism of a prime ideal

We will use the notations of section 7.3. Note that in particular *the residue class fields are finite*. In this section there is the *extra assumption*:

\mathfrak{q} is unramified over K .

This means that the map $Z_K(\mathfrak{q}) \rightarrow \overline{G}$ is an isomorphism. Because the residue class field R/\mathfrak{p} is finite, the group \overline{G} is generated by the automorphism $x \mapsto x^{\#(R/\mathfrak{p})}$ of S/\mathfrak{q} . In other words:

7.73 Proposition. *There is a unique $\varphi \in \text{Gal}(L : K)$ such that*

$$\varphi(\alpha) \equiv \alpha^N \pmod{\mathfrak{q}} \quad \text{for all } \alpha \in S,$$

where $N = \#(R/\mathfrak{p})$. This φ generates $Z_K(\mathfrak{q})$. □

7.74 Definition. The unique φ in Proposition 7.73 is called the *Frobenius automorphism* of \mathfrak{q} over K . Notation: $\varphi_K(\mathfrak{q})$. (So we have $Z_K(\mathfrak{q}) = \langle \varphi_K(\mathfrak{q}) \rangle$.)

Let $\sigma: L \xrightarrow{\sim} L'$ be a field isomorphism and put $S' = \sigma(S)$. Then L' is the field of fractions of the Dedekind domain S' and the following are equivalent:

7 Extensions of Dedekind Domains

$$\begin{aligned}\varphi_K(\mathfrak{q})(\alpha) &\equiv \alpha^N \pmod{\mathfrak{q}} \text{ for all } \alpha \in S, \\ (\sigma\varphi_K(\mathfrak{q}))(\alpha) &\equiv \sigma(\alpha)^N \pmod{\sigma(\mathfrak{q})} \text{ for all } \alpha \in S, \\ (\sigma\varphi_K(\mathfrak{q})\sigma^{-1})(\beta) &\equiv \beta^N \pmod{\sigma(\mathfrak{q})} \text{ for all } \beta \in S'.\end{aligned}$$

So we have:

7.75 Proposition. *Let $\sigma : L \xrightarrow{\sim} L'$ be an isomorphism of fields. Then*

$$\varphi_{\sigma(K)}(\sigma(\mathfrak{q})) = \sigma\varphi_K(\mathfrak{q})\sigma^{-1}.$$

In particular if $\sigma \in \text{Gal}(L : K)$, then

$$\varphi_K(\sigma(\mathfrak{q})) = \sigma\varphi_K(\mathfrak{q})\sigma^{-1}. \quad \square$$

7.76 Corollary. *If, moreover, $L : K$ is abelian, then $\varphi_K(\mathfrak{q})$ satisfies*

$$\varphi_K(\mathfrak{q})(\alpha) \equiv \alpha^N \pmod{\mathfrak{p}S} \text{ for all } \alpha \in S.$$

PROOF. By Proposition 7.75 and the transitivity of the action of $\text{Gal}(L : K)$ on the set of prime ideals of S above \mathfrak{p} :

$$\varphi_K(\mathfrak{q}') = \varphi_K(\mathfrak{q}) \text{ for all } \mathfrak{q}' \in \text{Max}(S) \text{ above } \mathfrak{p}.$$

Since \mathfrak{p} does not ramify in L , the ideal $\mathfrak{p}S$ is the product of the prime ideals above \mathfrak{p} . \square

For abelian extensions a Frobenius automorphism of a prime ideal \mathfrak{q} depends only on the prime ideal below \mathfrak{q} in the base field. In this case we use a special notation.

7.77 Definition and notation. For $L : K$ abelian and $\mathfrak{p} \in \text{Max}(R)$ unramified in L put $\varphi_{\mathfrak{p}}^{(L)} = \varphi_K(\mathfrak{q})$. The automorphism $\varphi_{\mathfrak{p}}^{(L)} \in \text{Gal}(L : K)$ is called the *Frobenius automorphism of \mathfrak{p} in $\text{Gal}(L : K)$* .

7.78 Example. Let $m \in \mathbb{N}^*$ and p a prime number with $p \nmid m$. Then p does not ramify in the cyclotomic field $\mathbb{Q}(\zeta_m)$. The automorphism of $\mathbb{Q}(\zeta_m)$ with $\zeta_m \mapsto \zeta_m^p$ is the Frobenius automorphism of p in $\text{Gal}(\mathbb{Q}(\zeta_m) : \mathbb{Q})$, since

$$\sum a_i \zeta_m^i \mapsto \sum a_i \zeta_m^{pi} \equiv \left(\sum a_i \zeta_m^i \right)^p \pmod{p\mathbb{Z}[\zeta_m]}.$$

In particular $f_p^{(L)}$ is equal to the order of \bar{p} in $(\mathbb{Z}/m)^*$.

7.79 Quadratic Reciprocity Law. The splitting behavior of primes in a cyclotomic field leads to another proof of the Quadratic Reciprocity Law. Let p be an odd prime number. Put $p^* = (-1)^{p-1/2}p$. Then $K = \mathbb{Q}(\sqrt{p^*})$ is the unique quadratic

subfield of $\mathbb{Q}(\zeta_p)$. Let q be a prime number $\neq p$ and let f be the order of \bar{q} in \mathbb{F}_p^* . Let Z be the decomposition group of q in $\mathbb{Q}(\zeta_p)$. Then

$$\begin{aligned} \left(\frac{q}{p}\right) = 1 &\iff q \text{ is a square modulo } p \iff f \mid \frac{p-1}{2} \iff 2 \mid \frac{p-1}{f} \\ &\iff K \subseteq \mathbb{Q}(\zeta_p)^Z \iff q \text{ splits completely in } K. \end{aligned}$$

For $q \neq 2$ this is equivalent to $\left(\frac{p^*}{q}\right) = 1$. Hence, for odd q

$$\left(\frac{p^*}{q}\right)\left(\frac{q}{p}\right) = 1 \quad \text{and so} \quad \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \left(\frac{-1}{q}\right)^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

For $q = 2$ we get:

$$\begin{aligned} \left(\frac{2}{p}\right) = 1 &\iff 2 \text{ splits completely in } K \iff p^* \equiv 1 \pmod{8} \\ &\iff p \equiv 1, 7 \pmod{8} \iff \frac{p^2-1}{8} \text{ is even.} \end{aligned}$$

$$\text{So } \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Finally, for future reference we consider the behavior of Frobenius automorphisms under a change of the base field. We do so only in the number field case.

7.80 Proposition. *Let $L : K$ be a Galois extension of number fields and $K' : K$ a number field extension. Let \mathfrak{q} be an over K unramified prime ideal of \mathcal{O}_L and \mathfrak{q}' a prime ideal of $\mathcal{O}_{LK'}$ above \mathfrak{q} . Then \mathfrak{q}' is unramified over K' and $\varphi_{K'}(\mathfrak{q}')|_L = \varphi_K(\mathfrak{q})^f$, where $f = f_K(\mathfrak{q}' \cap K')$.*

PROOF. By Galois theory restriction of automorphisms in $\text{Gal}(LK' : K')$ to L yields an isomorphism

$$\text{Gal}(LK' : K') \xrightarrow{\sim} \text{Gal}(L : L \cap K') \subseteq \text{Gal}(L : K).$$

By definition of inertia and decomposition groups this restricts to isomorphisms

$$Z_{K'}(\mathfrak{q}') \xrightarrow{\sim} Z_{L \cap K'}(\mathfrak{q}) \subseteq Z_K(\mathfrak{q}) \quad \text{and} \quad T_{K'}(\mathfrak{q}') \xrightarrow{\sim} T_{L \cap K'}(\mathfrak{q}) \subseteq T_K(\mathfrak{q}).$$

Since $T_K(\mathfrak{q})$ is trivial, so is $T_{K'}(\mathfrak{q}')$, that is \mathfrak{q}' is unramified over K' . Put $\mathfrak{p}' = \mathfrak{q}' \cap K'$ and $\mathfrak{p} = \mathfrak{q}' \cap K (= \mathfrak{q} \cap K)$. The Frobenius automorphism of \mathfrak{q}' over K' satisfies

$$\varphi_{K'}(\mathfrak{q}')(\alpha) \equiv \alpha^{N(\mathfrak{p}')} \pmod{\mathfrak{q}'} \quad \text{for all } \alpha \in \mathcal{O}_{LK'}.$$

In particular this holds for all $\alpha \in \mathcal{O}_L$. The Frobenius automorphism of \mathfrak{q} over K is characterized by

$$\varphi_K(\mathfrak{q})(\alpha) \equiv \alpha^{N(\mathfrak{p})} \pmod{\mathfrak{q}} \quad \text{for all } \alpha \in \mathcal{O}_L.$$

The proposition follows from $N(\mathfrak{p}') = N(\mathfrak{p})^f$. □

In particular for abelian extensions we have the following.

7.81 Corollary. *Let $K' : K$ be a number field extension, $L : K$ an abelian extension of number fields, \mathfrak{p} a prime ideal of \mathcal{O}_K which does not ramify in L and \mathfrak{p}' a prime ideal of $\mathcal{O}_{K'}$ above \mathfrak{p} . Then $\varphi_{\mathfrak{p}'}^{(LK')}|_L = (\varphi_{\mathfrak{p}}^{(L)})^f$, where $f = f_K(\mathfrak{p}')$. \square*

7.8 Galois groups of polynomials and reduction modulo a prime ideal

In chapter 5 it was shown that in every number field there is a prime ideal which is ramified over \mathbb{Q} , or in other words: there are no unramified extensions of \mathbb{Q} . In this section we show that for other base fields the situation can be quite different: in Example 7.82 an unramified extension of a quadratic number field will be constructed with Galois group A_5 , the symmetric group on 5 elements.

Let K be a number field and $f \in \mathcal{O}_K[X]$ a monic polynomial of degree n without multiple roots. Then $\text{disc}(f)$ is a nonzero element of \mathcal{O}_K . Let L be the splitting field of f over K , say $f = (X - \alpha_1) \cdots (X - \alpha_n)$ with $\alpha_1, \dots, \alpha_n \in \mathcal{O}_L$. Then $L = K(\alpha_1, \dots, \alpha_n)$ and $L : K$ is a Galois extension of number fields. The Galois group $G = \text{Gal}(L : K)$ acts by restriction on the set $A = \{\alpha_1, \dots, \alpha_n\}$ and since an automorphism of $L : K$ is determined by its action on A , this restriction is an injective group homomorphism

$$\kappa : G \rightarrow S(A), \quad \sigma \mapsto \sigma|_A,$$

where $S(A)$ is the full permutation group of A . The subgroup $\kappa(G)$ of $S(A)$ is by definition the Galois group $\text{Gal}_K(f)$ over K of the polynomial f .

Let $\mathfrak{p} \in \text{Max}(\mathcal{O}_K)$ and assume that $\text{disc}(f) \notin \mathfrak{p}$. Choose $\mathfrak{q} \in \text{Max}(\mathcal{O}_L)$ above \mathfrak{p} . For $\alpha \in \mathcal{O}_L$ its class in the residue field $\mathcal{O}_L/\mathfrak{q}$ is denoted by $\bar{\alpha}$. In $(\mathcal{O}_L/\mathfrak{q})[X]$ we have

$$\bar{f} = (X - \bar{\alpha}_1) \cdots (X - \bar{\alpha}_n),$$

and since $\text{disc}(\bar{f}) = \overline{\text{disc}(f)} \neq 0$, the polynomial \bar{f} has no multiple roots as well. The subfield $F = (\mathcal{O}_K/\mathfrak{p})(\bar{\alpha}_1, \dots, \bar{\alpha}_n)$ of $\mathcal{O}_L/\mathfrak{q}$ is a splitting field of \bar{f} over $\mathcal{O}_K/\mathfrak{p}$. The composition

$$Z_K(\mathfrak{q}) \rightarrow \bar{G} \rightarrow \text{Gal}(F : \mathcal{O}_K/\mathfrak{p})$$

of surjective homomorphisms is injective: if $\sigma \in Z_K(\mathfrak{q})$ induces the identity on $\bar{A} = \{\bar{\alpha}_1, \dots, \bar{\alpha}_n\}$, then also on A . Therefore, both homomorphisms are isomorphisms and this implies that \mathfrak{q} is unramified over K (and since $L : K$ is a Galois extension, \mathfrak{p} doesn't ramify in L) and that $\mathcal{O}_L/\mathfrak{q}$ is a splitting field of \bar{f} over $\mathcal{O}_K/\mathfrak{p}$.

The group \bar{G} is generated by the automorphism $x \mapsto x^{N(\mathfrak{p})}$. It induces a permutation of \bar{A} and the Frobenius automorphism of \mathfrak{q} over K induces the 'same' permutation of A : if $\bar{\alpha}_i^{N(\mathfrak{p})} = \bar{\alpha}_j$, then $\varphi_K(\mathfrak{q}) : \alpha_i \mapsto \alpha_j$.

7.82 Example. Let $f = X^5 - X + 1$ and let F be a splitting field of \bar{f} over \mathbb{F}_5 . Then $F : \mathbb{F}_5$ is a Galois extension and $\text{Gal}(F : \mathbb{F}_5)$ is generated by the automorphism $x \mapsto x^5$. A root $x \in F$ of \bar{f} is mapped to $x^5 = x - 1$. So the automorphism is of order 5. This means that \bar{f} is irreducible over \mathbb{F}_5 . From this it follows that f is irreducible over \mathbb{Q} . Let $A = \{\alpha_1, \dots, \alpha_5\}$ be the set of roots in \mathbb{C} and put $K = \mathbb{Q}(\alpha)$, where $\alpha = \alpha_1$. Let $L : \mathbb{Q}$ be the normal closure of $K : \mathbb{Q}$, that is L is the splitting field of f over K . The group $\text{Gal}(L : \mathbb{Q})$ is isomorphic to $\text{Gal}_{\mathbb{Q}}(f)$, a subgroup of $S(A)$. Since $[L : \mathbb{Q}]$ is a multiple of $[K : \mathbb{Q}] = 5$, the group $\text{Gal}_{\mathbb{Q}}(f)$ contains an element of order 5, which must be a 5-cycle of the set A . For instance, the Frobenius automorphism of a $\mathfrak{q} \in \text{Max}(\mathcal{O}_L)$ above 5 induces such a 5-cycle.

We have

$$\begin{aligned} \text{disc}(f) &= N_{\mathbb{Q}}^K(5\alpha^4 - 1) = -N_{\mathbb{Q}}^K(5\alpha^5 - \alpha) = -N_{\mathbb{Q}}^K(4\alpha - 5) = -4^5 N_{\mathbb{Q}}^K(\alpha - \frac{5}{4}) \\ &= 4^5 \cdot ((\frac{5}{4})^5 - \frac{5}{4} + 1) = 5^5 - 4^4 = 2869 = 19 \cdot 151. \end{aligned}$$

Since $\text{disc}(f)$ is squarefree, it follows that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Only the primes 19 and 151 ramify in K . The factorization of $\bar{f} \in \mathbb{F}_2[X]$ is

$$\bar{f} = (X^2 + X + 1)(X^3 + X^2 + 1).$$

So $\text{Gal}_{\mathbb{Q}}(f)$ contains a permutation which is the disjoint product of a 2-cycle and a 3-cycle. The third power of this permutation is a 2-cycle (a transposition). Because the subgroup $\text{Gal}(f)$ of $S(A)$ contains a 5-cycle and a 2-cycle, we have $\text{Gal}(f) = S(A) \cong S_5$, in particular $[L : \mathbb{Q}] = 5! = 120$. The group S_5 has a unique subgroup of index 2, the group A_5 of even permutations. So L has a unique quadratic subfield, and since $\sqrt{\text{disc}(f)} \in L$, it is the field $K' = \mathbb{Q}(\sqrt{19 \cdot 151})$. The extension $L : K'$ is a Galois extension of number fields and its Galois group is isomorphic to A_5 . We show that it is an unramified extension. Since only the primes 19 and 151 ramify in K , these are also the only primes which ramify in the normal closure L . It follows that prime ideals of $\mathcal{O}_{K'}$ different from $(19, \sqrt{19 \cdot 151})$ and $(151, \sqrt{19 \cdot 151})$ do not ramify in L . We have to show that $e_{19}^{(L)} = e_{151}^{(L)} = 2$. Since $\mathcal{O}_K = \mathbb{Z}[\alpha]$, the factorization of 19 and 151 in \mathcal{O}_K can be computed by factorizing f modulo 19 and 151 respectively. The factorization as product of maximal ideals is as follows:

$$\begin{aligned} (19) &= (19, \alpha - 6)^2(19, \alpha^3 - 7\alpha^2 - 6\alpha + 9) \\ (151) &= (151, \alpha - 39)^2(151, \alpha - 9)(151, \alpha^2 - 64\alpha + 61). \end{aligned}$$

The prime ideals $\mathfrak{p} = (19, \alpha - 6)$ and $\mathfrak{q} = (151, \alpha - 39)$ have ramification index 2 over \mathbb{Q} . We will show that they do not ramify in L . The field L is a splitting field of f over K and also a splitting field of $f_2 = \frac{f}{X - \alpha} \in \mathcal{O}_K[X]$ over K . This polynomial has no multiple roots. The discriminant of f_2 is the product of all $(\alpha_i - \alpha_j)^2$ with $i, j \in \{2, 3, 4, 5\}$, $i > j$. It follows that

$$\text{disc}(f_2) = \frac{\text{disc}(f)}{\prod_{i=2}^5 (\alpha_i - \alpha_1)^2} = \frac{19 \cdot 151}{f'(\alpha)^2} = \frac{19 \cdot 151}{4\alpha - 5} \in \mathbb{Z}[\alpha].$$

7 Extensions of Dedekind Domains

Since $N_{\mathbb{Q}}^K(4\alpha - 5) = 19 \cdot 151$, the ideal $(4\alpha - 5)$ of $\mathcal{O}_K = \mathbb{Z}[\alpha]$ is the product of an ideal of norm 19 and an ideal of norm 151. We have

$$\begin{aligned} 4\alpha - 5 &\equiv 4 \cdot 6 - 5 \equiv 19 \equiv 0 \pmod{\mathfrak{p}}, \\ 4\alpha - 5 &\equiv 4 \cdot 39 - 5 \equiv 151 \equiv 0 \pmod{\mathfrak{q}}. \end{aligned}$$

Hence $(4\alpha - 5) = \mathfrak{p}\mathfrak{q}$. It follows that $\text{disc}(f_2) \notin \mathfrak{p}, \mathfrak{q}$. So \mathfrak{p} and \mathfrak{q} do not ramify in $K(\alpha_2)$; therefore, they do not ramify in the splitting field L of f_2 over K .

EXERCISES

- Let R be a Dedekind domain, K its field of fractions, $L : K$ a Galois extension, S the integral closure of R in L , $\mathfrak{q} \in \text{Max}(S)$ above $\mathfrak{p} \in \text{Max}(R)$.
 - Let $\alpha \in S$. Show that the characteristic polynomial of α over K is a monic polynomial over R which splits over L .
 - Prove that $S/\mathfrak{q} : R/\mathfrak{p}$ is a normal extension.
- Let R be a Dedekind domain, K its field of fractions, $L : K$ a Galois extension, S the integral closure of R in L , $\mathfrak{q} \in \text{Max}(S)$ and $\mathfrak{p} \in \text{Max}(R)$. Show that

$$\mathfrak{q} \cap K = \mathfrak{p} \iff \mathfrak{q} \cap R = \mathfrak{p} \iff \mathfrak{q} \mid \mathfrak{p}S.$$

- Prove Proposition 7.3.
- Let $L : K$ be an extension of number fields and let \mathfrak{a} and \mathfrak{b} be nonzero ideals of \mathcal{O}_K such that $\mathfrak{a}\mathcal{O}_L \mid \mathfrak{b}\mathcal{O}_L$. Show that $\mathfrak{a} \mid \mathfrak{b}$.
- Give an example of a biquadratic number field in which 2 splits completely and also one in which 3 splits completely.
 - Let K be a biquadratic field in which 2 or 3 splits completely. Show that there is no $\alpha \in \mathcal{O}_K$ such that $\mathcal{O}_K = \mathbb{Z}[\alpha]$.
- Let R be a Dedekind domain, K its field of fractions, $L : K$ a finite separable field extension and S the integral closure of R in L .
 - Let $(\alpha_1, \dots, \alpha_n)$ be a K -basis of L with $\alpha_1, \dots, \alpha_n \in S$. Show that

$$v_{\mathfrak{p}}(\text{disc}(\alpha_1, \dots, \alpha_n)) \equiv v_{\mathfrak{p}}(\mathfrak{d}_R(S)) \pmod{2}$$

for all $\mathfrak{p} \in \text{Max}(R)$.

- Prove that the ideal class of $\mathfrak{d}_R(S)$ is a square in $\mathcal{C}(R)$.
- Show that the extension $\mathbb{Q}(\sqrt{2}, \sqrt{5}) : \mathbb{Q}(\sqrt{10})$ is unramified.
 - Prove that $\mathfrak{p} \in \text{Max}(\mathbb{Z}[\sqrt{10}])$ splits completely in $\mathbb{Q}(\sqrt{2}, \sqrt{5})$ if and only if \mathfrak{p} is a principal ideal.

8. Let L be a biquadratic number field. Suppose that 2 ramifies in each of the quadratic subfields. Show that 2 totally ramifies in L .
9. Let $\alpha \in \mathbb{R}$ such that $\alpha^3 = \alpha + 1$. Show that the extension $\mathbb{Q}(\alpha, \sqrt{-23}) : \mathbb{Q}(\sqrt{-23})$ is unramified.
10. Let $L : K$ be a Galois extension of number fields. Assume there is a $\mathfrak{p} \in \text{Max}(\mathcal{O}_K)$ which remains prime in L . Show that the group $\text{Gal}(L : K)$ is cyclic.
11. Let $L : K$ be a Galois extension of number fields with Galois group G . Suppose $\mathfrak{p} \in \text{Max}(\mathcal{O}_K)$ ramifies in L , but does not ramify in intermediate fields $\neq L$.
- Prove that there is a unique smallest nontrivial subgroup H of G .
 - Show that $\#(G)$ is a prime power.
 - Prove that H is a normal subgroup of G .
 - Show that $\#(H)$ is a prime number and that H is a central subgroup of G .
12. Let $L : K$ be a Galois extension of number fields with Galois group G . Suppose $\mathfrak{p} \in \text{Max}(\mathcal{O}_K)$ does not split completely in L , but does so in every intermediate field $\neq L$. Prove the same (i), (ii), (iii) and (iv) as in the previous exercise.
13. Let $L : K$ be a Galois extension of number fields with Galois group G . Suppose $\mathfrak{p} \in \text{Max}(\mathcal{O}_K)$ does not remain prime in L , but does so in every intermediate field $\neq L$. Prove that G is cyclic of prime power order.
14. Give a detailed proof of Corollary 7.49.
15. Let K be a quadratic number field. Show that odd prime divisors of $\text{disc}(K)$ ramify tamely in K and that 2 ramifies wildly if and only if $2 \mid \text{disc}(K)$.
16. An elementary proof of a weaker version of Theorem 8.37 of the next chapter.
- Let $f = a_0X^m + \cdots + a_1X + a_m \in \mathbb{Z}[X]$ be of degree $m \geq 1$. Show that there are infinitely many primes p such that $\bar{f} \in \mathbb{F}_p[X]$ has a root in \mathbb{F}_p . (Consider $f(n!)$ in case $a_m = 1$. For the general case look at $f(a_mX)/a_m$.)
 - Let K be a number field. Prove that there are infinitely many $\mathfrak{p} \in \text{Max}(\mathcal{O}_K)$ such that $f_{\mathbb{Q}}(\mathfrak{p}) = 1$.
 - Let $L : K$ be an extension of number fields. Prove that there are infinitely many $\mathfrak{p} \in \text{Max}(\mathcal{O}_K)$ which split completely in L .
17. Let R be a Dedekind domain with finite residue fields, K its field of fractions, $L : K$ a Galois extension of degree n and S the integral closure of R in L . Suppose $\mathfrak{p} \in \text{Max}(R)$ totally tamely ramifies in L : $\mathfrak{p}S = \mathfrak{q}^n$ with $\mathfrak{q} \in \text{Max}(S)$.
- Show that R/\mathfrak{p}^* contains a primitive n -th root of unity and that the group $\text{Gal}(L : K)$ is cyclic.
- Assume that also K contains a primitive n -th root of unity. Then by some Galois theory one shows that there exists a $\beta \in L$ such that $L = K(\beta)$ and $\beta^n \in K$. See also Proposition 15.9 in the section on Kummer extensions.
- Put $v_{\mathfrak{q}}(\beta) = k$ and write $\beta = \pi^k \gamma$, where $v_{\mathfrak{q}}(\pi) = 1$. Prove that $k \equiv 1 \pmod{n}$.

7 Extensions of Dedekind Domains

- (iii) Show that there is a $\beta \in L$ such that $L = K(\beta)$, $\beta^n \in K$ and $v_{\mathfrak{q}}(\beta) = 1$.
18. Let $L : K$ be a Galois extension of number fields and \mathfrak{p} a maximal ideal of \mathcal{O}_K which totally ramifies in L . Let \mathfrak{q} be the prime ideal of \mathcal{O}_L above \mathfrak{p} and $\pi \in \mathcal{O}_L$ such that $v_{\mathfrak{q}}(\pi) = 1$. Show that $v_{\mathfrak{p}}(N_K^L(\pi)) = 1$.
19. Let p be an odd prime and K the unique subfield of degree p of $\mathbb{Q}(\zeta_{p^2})$. Compute $\text{disc}(K)$.
20. Let K be a quadratic number field in which the prime number 2 ramifies. Put $K = \mathbb{Q}(\sqrt{m})$ with $m \in \mathbb{Z}$ squarefree. Then $m \equiv 3 \pmod{4}$ or $m \equiv 2 \pmod{4}$. Let $\mathfrak{q} \in \text{Max}(\mathcal{O}_K)$ be above 2. There is a unique $t \in \mathbb{N}$ such that $V_t(\mathfrak{q}) \setminus V_{t+1}(\mathfrak{q})$ is nonempty. Compute t for both cases.
21. Let $K = \mathbb{Q}(\sqrt{-2}, \sqrt{3})$. The prime 2 totally ramifies in K , see Example 5.23. Let \mathfrak{p} be the prime ideal of \mathcal{O}_K above 2. Compute $V_{\mathbb{Q}, i}(\mathfrak{p})$ for all $i \in \mathbb{N}$.
22. Let $K = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$. The prime 3 totally ramifies in K , see Example 7.17. Let \mathfrak{p} be the prime ideal of \mathcal{O}_K above 3. Compute $V_{\mathbb{Q}, i}(\mathfrak{p})$ for all $i \in \mathbb{N}$.
23. In Example 7.64 the ramification groups of an odd prime p in $\mathbb{Q}(\zeta_{p^r})$ have been computed. Compute the ramification groups of 2 in $\mathbb{Q}(\zeta_{2^r})$.

8 Analytic Methods

The splitting behavior of primes in a number field K determines a complex analytic function, the Dedekind zeta function $\zeta_K(s)$. It is defined by an infinite series (a Dirichlet series) determined by the sequence $(j_K(n))_{n \geq 1}$, where $j_K(n)$ denotes the number of ideals of \mathcal{O}_K of norm n . For the convergence properties we will need the asymptotic behavior of sequences like these and this is studied in section 8.2. It is based on estimates in section 8.1 for the number of lattice points inside a bounded domain in a real vector space. It is remarkable that deep properties of a number field are hidden in its Dedekind zeta function and, therefore, are determined by the splitting behavior of primes in the number field alone. Dirichlet series are considered in general in section 8.3. An important example is the Riemann zeta function, the Dedekind zeta function of the number field \mathbb{Q} . In section 8.5 the notion of Dirichlet density is introduced. It is a measure for collections of prime ideals in a number field. A positive density implies that the collection contains infinitely many of them.

8.1 Counting lattice points in a bounded domain

Let D be a bounded measurable domain in the standard Euclidean space \mathbb{R}^n and let the boundary ∂D be not too wild: let's assume that it is covered by the images of a finite number of Lipschitz maps $f_1, \dots, f_k: [0, 1]^{n-1} \rightarrow \mathbb{R}^n$.

A map $f: [0, 1]^{n-1} \rightarrow \mathbb{R}^n$ is a *Lipschitz map* if there is an upper bound for the quotients $\|f(x) - f(y)\|/\|x - y\|$. The condition on the boundary prevents it to have a complicated fractal structure, i.e. to have a fractal dimension $> n - 1$.

Let, furthermore, Λ be a lattice in \mathbb{R}^n . Since D is bounded, by Proposition 5.3 the set $D \cap \Lambda$ is finite. Our aim is to estimate the number of elements of $D \cap \Lambda$, more precisely to give an estimate of $\#(aD \cap \Lambda)$ as a function of $a \in [1, \infty)$. Note that $\#(aD \cap \Lambda) = \#(D \cap \frac{1}{a}\Lambda)$. Since D is measurable, it will follow that

$$\lim_{a \rightarrow \infty} \delta\left(\frac{1}{a}\Lambda\right) \cdot \#(D \cap \frac{1}{a}\Lambda) = \text{vol}(D).$$

So an estimate for the number $\#(aD \cap \Lambda)$ is $\frac{\text{vol}(D)}{\delta(\Lambda)} a^n$. We will see that the condition on the boundary of D implies the following for the error term.

8.1 Proposition. *Let D , a and Λ be as above. Then for $\#(aD \cap \Lambda)$ as a function of a we have*

$$\#(aD \cap \Lambda) - \frac{\text{vol}(D)}{\delta(\Lambda)} a^n = O(a^{n-1}).$$

PROOF. Let F be the mesh of Λ determined by a \mathbb{Z} -basis (v_1, \dots, v_n) of Λ and let v be the center of \overline{F} : $v = \frac{1}{n}(v_1 + \dots + v_n)$. The Euclidean space is covered by the translates of \overline{F} centered at lattice points:

$$\mathbb{R}^n = \bigcup_{x \in \Lambda} (x - v + \overline{F}).$$

For $a \in [1, \infty)$ put

$$\begin{aligned} S^-(a) &= \{x \in \Lambda \mid x - v + \overline{F} \subseteq aD\}, & N^-(a) &= \#(S^-(a)), \\ S^+(a) &= \{x \in \Lambda \mid (x - v + \overline{F}) \cap aD \neq \emptyset\}, & N^+(a) &= \#(S^+(a)), \\ S(a) &= \Lambda \cap aD, & N(a) &= \#(S(a)). \end{aligned}$$

Then

$$S^-(a) \subseteq S(a) \subseteq S^+(a).$$

and so $N^-(a) \leq N(a) \leq N^+(a)$. We have

$$N^-(a)\delta(\Lambda) \leq N(a)\delta(\Lambda) \leq N^+(a)\delta(\Lambda) \quad \text{and} \quad N^-(a)\delta(\Lambda) \leq \text{vol}(aD) \leq N^+(a)\delta(\Lambda).$$

Therefore,

$$|N(a)\delta(\Lambda) - \text{vol}(aD)| \leq (N^+(a) - N^-(a))\delta(\Lambda).$$

For $x \in \Lambda$ we have

$$x \in S^+(a) \setminus S^-(a) \iff (x - v + \overline{F}) \cap \partial(aD) \neq \emptyset.$$

This and the condition for ∂D will be used for estimating $(N^+(a) - N^-(a))\delta(\Lambda)$. Let ∂D be covered by Lipschitz maps $f_1, \dots, f_k: [0, 1]^{n-1} \rightarrow \mathbb{R}^n$. Take $\lambda > 0$ such that $\|f_i(x) - f_i(y)\| \leq \lambda\|x - y\|$ for $i = 1, \dots, k$ and for all $x, y \in [0, 1]^{n-1}$. Divide $[0, 1]$ into $[a]$ segments of equal length $1/[a]$. The n -cube $[0, 1]$ is subdivided into $[a]^{n-1}$ cubes with edges of length $1/[a]$. The boundary $\partial(aD)$ is covered by the images of the maps af_1, \dots, af_k . Let c be any of these cubes. Put $d = \text{diam}([0, 1]^{n-1}) = \sqrt{n-1}$. Then $\text{diam}(c) = d/[a]$ and so $\text{diam}(af_i(c)) \leq a\lambda d/[a] \leq 2\lambda d$ for $i = 1, \dots, k$. It follows that $af_i(c)$ is contained in an n -ball with radius λd . Let r be the radius of an n -ball with center v and contained in \overline{F} . Comparison of volumes yields that the number of disjoint n -balls with radius r contained in an n -ball with radius λd is less than $(\lambda d/r)^n$. It follows that the number of $x \in \Lambda$ with $af_i(c) \cap (x - v + \overline{F}) \neq \emptyset$ is less than $(\lambda d/r)^n$. The number of small cubes is $k([a])^{n-1}$, so

$$N^+(a) - N^-(a) \leq k([a])^{n-1} \cdot \left(\frac{\lambda d}{r}\right)^n \leq k\left(\frac{\lambda d}{r}\right)^n \cdot a^{n-1}.$$

Hence $N(a)\delta(\Lambda) - \text{vol}(aD) = O(a^{n-1})$, i.e.

$$\#(aD \cap \Lambda) - \frac{\text{vol}(D)}{\delta(\Lambda)}a^n = O(a^{n-1}). \quad \square$$

8.2 The distribution of ideals over the ideal classes

Given an ideal class of a number field K and an $N \in \mathbb{N}^*$, in this section we estimate the number of ideals of \mathcal{O}_K of norm $\leq N$ in the given ideal class.

8.2 Notations. Let K be a number field of degree d . It determines an arithmetic function

$$j_K: \mathbb{N}^* \rightarrow \mathbb{N} \subseteq \mathbb{C}, \quad n \mapsto \#\{\mathfrak{a} \mid \mathfrak{a} \text{ is an ideal of } \mathcal{O}_K \text{ with } N(\mathfrak{a}) = n\}$$

and a corresponding sequence of partial sums $(J_K(N))_{N \geq 1}$:

$$J_K(N) = \sum_{n=1}^N j_K(n) = \#\{\mathfrak{a} \in \mathbb{I}^+(K) \mid 1 \leq N(\mathfrak{a}) \leq N\}.$$

This counting of ideals will be done for ideal classes separately. For that purpose we introduce the following notations, where C is an ideal class of K :

$$j_C(n) = \#\{\mathfrak{a} \in C \mid N(\mathfrak{a}) = n\} \quad \text{and} \quad J_C(N) = \sum_{n=1}^N j_C(n).$$

Clearly

$$j_K(n) = \sum_C j_C(n) \quad \text{and} \quad J_K(N) = \sum_C J_C(N).$$

We will see that $J_C(N)$ tends for $N \rightarrow \infty$ asymptotically to a constant times N , the constant being equal for all ideal classes, see Theorem 8.3. Moreover, the error term will be of order $N^{1-\frac{1}{d}}$. For $J_K(N)$ it follows that asymptotically it tends with an error term of the same order to a constant times N as well, the constant being the constant for $J_C(N)$ multiplied by the class number.

Fix $\mathfrak{b} \in C^{-1}$. Then we have a correspondence

$$\begin{array}{ccc} \left\{ \begin{array}{l} \text{ideals } \mathfrak{a} \text{ in } C \\ \text{with } N(\mathfrak{a}) \leq N \end{array} \right\} & \begin{array}{c} \longrightarrow \\ \longleftarrow \end{array} & \left\{ \begin{array}{l} \text{principal ideals } (\alpha) \subseteq \mathfrak{b} \\ \text{with } |\mathbb{N}_{\mathbb{Q}}^K(\alpha)| \leq N \cdot N(\mathfrak{b}) \text{ and } \alpha \neq 0 \end{array} \right\} \\ \mathfrak{a} & \longmapsto & \mathfrak{a}\mathfrak{b} \\ \alpha\mathfrak{b}^{-1} & \longleftarrow & (\alpha) \end{array}$$

So instead of counting ideals we can count principal ideals:

$$J_C(N) = \#\{\mathfrak{a} \mid \mathfrak{a} \text{ a nonzero principal ideal, } \mathfrak{a} \subseteq \mathfrak{b}, N(\mathfrak{a}) \leq N \cdot N(\mathfrak{b})\}.$$

Generators of principal ideals are determined up to a unit factor. The idea is to have a domain in $\mathbb{R}^r \times \mathbb{C}^s$, the \mathbb{R} -vector space in which \mathcal{O}_K is embedded as a lattice, containing exactly one generator for each nonzero principal ideal. The group \mathcal{O}_K^* embeds as a subgroup of $(\mathbb{R}^r \times \mathbb{C}^s)^* = (\mathbb{R}^*)^r \times (\mathbb{C}^*)^s$ and acts on it by multiplication. In principle we want a fundamental domain for this action. It is, however, easier to use the subgroup of \mathcal{O}_K^* generated by a fundamental system of units. It is a free abelian group of rank $r + s - 1$, mapped under ψ isomorphically to the lattice $\psi(\mathcal{O}_K^*)$ in the subspace H of \mathbb{R}^{r+s} . A fundamental domain of its action on $\mathbb{R}^{*r} \times \mathbb{C}^{*s}$ contains exactly $w(K) := \#(\mu(K))$ elements of $\iota(\mathcal{O}_K^*)$.

Choose a fundamental system $(\varepsilon_1, \dots, \varepsilon_{r+s-1})$ of units and let F be the fundamental parallelotope spanned by $\psi(\varepsilon_1), \dots, \psi(\varepsilon_{r+s-1})$. Put $v_k = \psi(\varepsilon_k)$ for $k = 1, \dots, r + s - 1$, then

$$F = \left\{ \sum_{k=1}^{r+s-1} t_k v_k \mid 0 \leq t_k < 1 \right\}.$$

Let $v = (\overbrace{1, \dots, 1}^r, \overbrace{2, \dots, 2}^s) \in \mathbb{R}^{r+s}$. Then $v \notin H$ and

$$D = L^{-1}(F + \mathbb{R}v) \subseteq \mathbb{R}^{*r} \times \mathbb{C}^{*s}$$

is a fundamental domain for the action of $\langle \varepsilon_1, \dots, \varepsilon_{r+s-1} \rangle$ on $\mathbb{R}^{*r} \times \mathbb{C}^{*s}$. For positive reals a put $D_a = \{x \in D \mid |N(x)| \leq a\}$. The advantage of the particular choice of v is the homogeneity of D_a in the sense that

$$D_a = \sqrt[d]{a} \cdot D_1,$$

which implies that $\text{vol}(D_a) = a \cdot \text{vol}(D_1)$. The counting of ideals of norm $\leq N$ in a given ideal class comes down to counting lattice points in a bounded domain:

$$w(K) \cdot J_C(N) = \#(\Lambda_{\mathfrak{b}} \cap D_{N \cdot N(\mathfrak{b})}).$$

We will apply Proposition 8.1. A parameterization of $D' := D_1 \cap ((0, \infty)^r \cap \mathbb{C}^s)$ will be given. It will show that $\partial D'$, and by symmetry also ∂D_1 , is Lipschitz parameterizable. The parameterization will be used for a calculation of $\text{vol}(D')$. Then again by symmetry $\text{vol}(D_1) = 2^r \text{vol}(D')$. Thus we have

$$w(K) \cdot J_C(N) = \frac{\text{vol}(D_1)N(\mathfrak{b})}{\delta(\Lambda_{\mathfrak{b}})} N + O(N^{1-\frac{1}{d}})$$

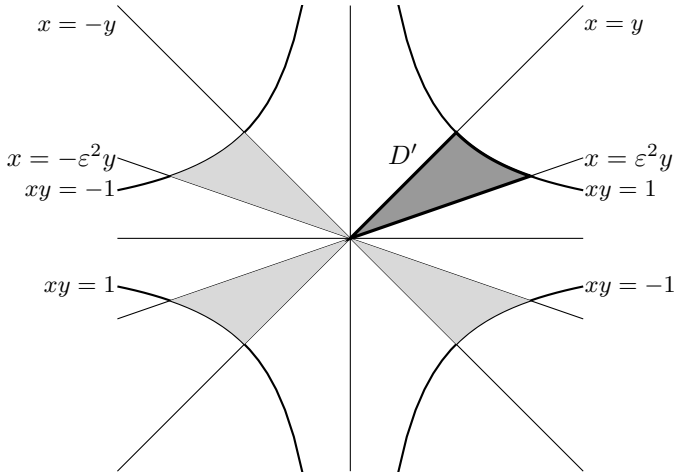


Figure 8.1: D_1 and D' for real quadratic number fields

and by Corollary 5.8

$$J_C(N) = \frac{2^{r+s} \text{vol}(D')}{w \sqrt[d]{|\text{disc}(K)|}} + O(N^{1-\frac{1}{d}}). \quad (8.1)$$

The v_k are vectors in \mathbb{R}^{r+s} . We will use the notation

$$v_k = (v_k^{(1)}, \dots, v_k^{(r+s)}).$$

Then $(x_1, \dots, z_1, \dots) \in D'$ if and only if there are $t_1, \dots, t_{r+s} \in [0, 1)$ and $u \in (-\infty, 0]$ such that

$$\begin{aligned} \log x_1 &= \left(\sum_{k=1}^{r+s} t_k v_k^{(1)} \right) + u \\ &\vdots \\ \log x_r &= \left(\sum_{k=1}^{r+s} t_k v_k^{(r)} \right) + u \\ 2 \log z_1 &= \left(\sum_{k=1}^{r+s} t_k v_k^{(r+1)} \right) + 2u \\ &\vdots \\ 2 \log z_s &= \left(\sum_{k=1}^{r+s} t_k v_k^{(r+s)} \right) + 2u. \end{aligned}$$

8 Analytic Methods

Now put $z_j = \rho_j e^{i\vartheta_j}$ and $t_{r+s} = e^u$. Then for

$$(x_1, \dots, x_r, \rho_1 e^{i\vartheta_1}, \dots, \rho_s e^{i\vartheta_s}) \in D'$$

we have

$$\begin{aligned} x_j &= t_{r+s} e^{\sum t_k v_k^{(j)}} && (\text{for } 1 \leq j \leq r), \\ \rho_j &= t_{r+s} e^{\frac{1}{2} \sum t_k v_k^{(j)}} && (\text{for } r+1 \leq j \leq r+s), \\ \vartheta_j &= 2\pi t_{r+j} && (\text{for } r+1 \leq j \leq r+s). \end{aligned}$$

Thus we have a parameterization of the interior of D' and for the computation of $\text{vol}(D')$ it can best be seen as the composition:

$$(0, 1)^d \xrightarrow{A_1} \mathbb{R}^{r+s} \times \mathbb{R}^s \xrightarrow{A_2} \mathbb{R}^{r+s} \times \mathbb{R}^s \xrightarrow{A_3} \mathbb{R}^r \times (0, \infty)^s \times \mathbb{R}^s \xrightarrow{A_4} \mathbb{R}^r \times \mathbb{C}^s.$$

These maps are defined as follows:

$$A_1(t_1, \dots, t_d) = (t_1, \dots, t_{r+s-1}, \log(t_{r+s}), t_{r+s+1}, \dots, t_{r+2s}),$$

$$A_2(u_1, u_2) = (u_1 M, u_2), \text{ where } M \text{ is the } (r+s) \times (r+s)\text{-matrix } \begin{pmatrix} v_1 \\ \vdots \\ v_{r+s-1} \\ v \end{pmatrix},$$

$$A_3(a_1, \dots, a_r, b_1, \dots, b_s; c_1, \dots, c_s) = (e^{a_1}, \dots, e^{a_r}; e^{b_1/2}, \dots, e^{b_s/2}; 2\pi c_1, \dots, 2\pi c_s),$$

$$A_4(x_1, \dots, x_r; \rho_1, \dots, \rho_s; \vartheta_1, \dots, \vartheta_s) = (x_1, \dots, x_r, \rho_1 e^{i\vartheta_1}, \dots, \rho_s e^{i\vartheta_s}).$$

The volume of D' can be computed by standard calculus techniques. In the computation occurs a Jacobian determinant

$$J(t_1, \dots, t_d) = \frac{\pi^s x_1 \cdots x_r \rho_1 \cdots \rho_s}{t_{r+s}} \det(M).$$

Also note that $\log x_1 + \cdots + 2 \log \rho_1 + \cdots = ru + 2su = d \cdot u$ and so $x_1 \cdots \rho_1^2 \cdots = e^{d \cdot u} = (e^u)^d = t_{r+s}^d$. Furthermore, for the matrix M we have by the formula on page 128: $|\det(M)| = d \cdot \text{Reg}(K)$.

$$\begin{aligned} \text{vol}(D') &= \int_{D'} \rho_1 \cdots \rho_s dx_1 \cdots dx_r d\rho_1 \cdots d\rho_s d\vartheta_1 \cdots d\vartheta_s \\ &= \int_{[0,1]^d} \rho_1 \cdots \rho_s |J(t_1, \dots, t_d)| dt_1 \cdots dt_d \\ &= \pi^s |\det(M)| \int_{[0,1]^d} \frac{x_1 \cdots x_r \rho_1^2 \cdots \rho_s^2}{t_{r+s}} dt_1 \cdots dt_d \\ &= \pi^s |\det(M)| \int_{[0,1]^d} t_{r+s}^{d-1} dt_1 \cdots dt_d = \frac{1}{d} \pi^s |\det(M)| = \pi^s \text{Reg}(K). \end{aligned}$$

8.3 Theorem. *Let K be a number field of degree d . Then for every ideal class C of K we have*

$$J_C(N) = \frac{2^r (2\pi)^s \operatorname{Reg}(K)}{w(K) \sqrt{|\operatorname{disc}(K)|}} \cdot N + O(N^{1-\frac{1}{d}})$$

and hence

$$J_K(N) = \frac{2^r (2\pi)^s h(K) \operatorname{Reg}(K)}{w(K) \sqrt{|\operatorname{disc}(K)|}} \cdot N + O(N^{1-\frac{1}{d}}),$$

where $h(K) = \#(\mathcal{C}(K))$, the class number of K .

PROOF. The parameterization of D' satisfies a Lipschitz condition because the partial derivatives are bounded. Restriction to the 2^d faces of the d -cube is a Lipschitz parameterization of $\partial D'$. So the formula for $J_C(N)$ follows from the above computation of $\operatorname{vol}(D')$ and formula (8.1). \square

In particular the number of ideals of a given norm N tends asymptotically to a constant times N for $N \rightarrow \infty$:

$$J_K(N) \sim \frac{2^r (2\pi)^s h(K) \operatorname{Reg}(K)}{w(K) \sqrt{|\operatorname{disc}(K)|}} \cdot N \quad \text{for } N \rightarrow \infty.$$

8.4 Examples.

1. For K imaginary quadratic, say $K = \mathbb{Q}(\sqrt{m})$ with $m < -3$ and squarefree, we have

$$J_K(N) = \frac{\pi h(K)}{\sqrt{-D_m}} \cdot N + O(\sqrt{N}).$$

2. For K real quadratic, $K = \mathbb{Q}(\sqrt{m})$ with $m > 1$ and squarefree

$$J_K(N) = \frac{2h(K) \log \varepsilon}{\sqrt{D_m}} \cdot N + O(\sqrt{N}),$$

where ε is the fundamental unit of K .

8.3 Dirichlet series

Power series can be seen as generating functions of sequences of numbers. Another type of generating function is the Dirichlet series. This type of function is especially useful in case we are dealing with a multiplicative arithmetic function, see Definition 8.15.

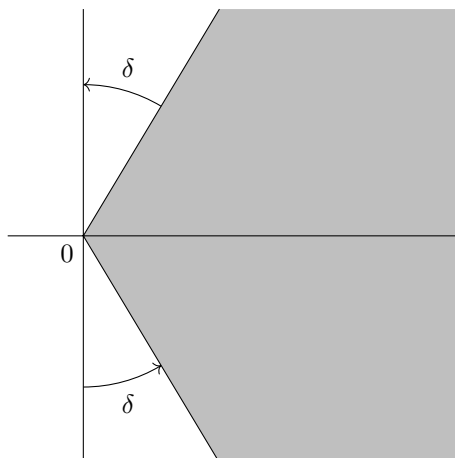


Figure 8.2: Domain used in the proof of Proposition 8.8

8.5 Definition. A series of type

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

with $a_n \in \mathbb{C}$ and $s \in \mathbb{C}$ is called a *Dirichlet series*. The terms $\frac{a_n}{n^s}$ ($= a_n e^{-s \log n}$) of such a series are functions in the complex variable s .

8.6 Notation. When dealing with Dirichlet series one traditionally denotes the complex variable by s instead of z . One also writes $s = \sigma + it$ with $\sigma, t \in \mathbb{R}$: the real and imaginary part are denoted by σ and t respectively.

8.7 Example. An important example of a Dirichlet series is $\sum_{n=1}^{\infty} \frac{1}{n^s}$ ($= \zeta(s)$), the *Riemann zeta function*. Since $|\frac{1}{n^s}| = \frac{1}{n^\sigma}$, it converges on the half-plane $\sigma > 1$, and—as we will see—to an analytic function on this half-plane.

8.8 Proposition. *Let the Dirichlet series $\sum \frac{a_n}{n^s}$ converge for $s = s_0$. Then it converges on the half-plane $\Re(s) > \Re(s_0)$ to an analytic function.*

PROOF. Under translation a Dirichlet series transforms into a Dirichlet series: replacement of s by $s + s_0$ in a term $\frac{a_n}{n^s}$ gives $\frac{a_n n^{-s_0}}{n^s}$. So we may assume that $s_0 = 0$, meaning that $\sum a_n$ converges. Then to prove the convergence for all s with $\sigma > 0$. We will prove that $\sum \frac{a_n}{n^s}$ converges uniformly on the domain

$$\{s \mid |\arg(s)| \leq \frac{\pi}{2} - \delta\}$$

for arbitrary small δ , see Figure 8.2. Then it follows that the sum is an analytic function on this domain and, since δ was arbitrary, it is so on the half-plane $\sigma > 0$.

Put

$$A_N = \sum_{n=1}^N a_n \quad \text{and} \quad A_{M,N} = \sum_{n=M}^N a_n \quad (= 0 \text{ if } M > N).$$

Let $\varepsilon > 0$. Choose N_0 such that $|A_{M,N}| \leq \varepsilon$ for all $N \geq M \geq N_0$. Such an N_0 exists because the series $\sum_{n=1}^{\infty} a_n$ converges. For $N \geq M \geq N_0$ we then have

$$\begin{aligned} \sum_{n=M}^N \frac{a_n}{n^s} &= \sum_{n=M}^N \frac{A_{M,n} - A_{M,n-1}}{n^s} = \sum_{n=M}^N \frac{A_{M,n}}{n^s} - \sum_{n=M-1}^{N-1} \frac{A_{M,n}}{(n+1)^s} \\ &= \frac{A_{M,N}}{N^s} + \sum_{n=M}^{N-1} A_{M,n} \left(\frac{1}{n^s} - \frac{1}{(n+1)^s} \right). \end{aligned}$$

From

$$\int_n^{n+1} \frac{s \, dx}{x^{s+1}} = \left[\frac{-1}{x^s} \right]_n^{n+1} = \frac{1}{n^s} - \frac{1}{(n+1)^s}$$

follows:

$$\left| \frac{1}{n^s} - \frac{1}{(n+1)^s} \right| \leq \int_n^{n+1} \frac{|s| \, dx}{x^{\sigma+1}} = \frac{|s|}{\sigma} \int_n^{n+1} \frac{\sigma \, dx}{x^{\sigma+1}} = \frac{|s|}{\sigma} \left(\frac{1}{n^\sigma} - \frac{1}{(n+1)^\sigma} \right).$$

If $|\arg s| \leq \frac{\pi}{2} - \delta$, then $\frac{|s|}{\sigma} \leq C$ for some constant C . So:

$$\begin{aligned} \left| \sum_{n=M}^N \frac{a_n}{n^s} \right| &\leq \frac{|A_{M,N}|}{|N^s|} + \sum_{n=M}^{N-1} |A_{M,n}| \left| \frac{1}{n^s} - \frac{1}{(n+1)^s} \right| \\ &\leq \frac{\varepsilon}{N^\sigma} + \varepsilon C \sum_{n=M}^{N-1} \left(\frac{1}{n^\sigma} - \frac{1}{(n+1)^\sigma} \right) = \frac{\varepsilon}{N^\sigma} + \varepsilon C \left(\frac{1}{M^\sigma} - \frac{1}{N^\sigma} \right) \\ &< \frac{\varepsilon}{N^\sigma} + \varepsilon C \frac{1}{M^\sigma} \leq \varepsilon(C+1). \quad \square \end{aligned}$$

8.9 Corollary. *There is a unique $\sigma_0 \in \mathbb{R} \cup \{-\infty, \infty\}$ such that $\sum \frac{a_n}{n^s}$ converges for all s with $\Re(s) > \sigma_0$ and diverges for all s with $\Re(s) < \sigma_0$. \square*

8.10 Definition. The unique σ_0 in Corollary 8.9 is called the *abscissa of convergence* of the Dirichlet series $\sum \frac{a_n}{n^s}$.

8.11 Example. The series $\zeta(s) = \sum \frac{1}{n^s}$ diverges for $s = 1$, so $\sigma_0 \geq 1$. It converges for all real s with $s > 1$. So the abscissa of convergence is 1.

8.12 Theorem. *Let $\alpha \in \mathbb{R}$ with $\alpha \geq 0$ such that $\sum_{n=1}^N a_n = O(N^\alpha)$. Then the abscissa of convergence σ_0 of the Dirichlet series $\sum \frac{a_n}{n^s}$ satisfies $\sigma_0 \leq \alpha$.*

PROOF. It suffices to show convergence for $\sigma \in \mathbb{R}$ with $\sigma > \alpha$. Put $A_N = \sum_{n=1}^N a_n$. Then $|A_N| \leq BN^\alpha$ for some $B > 0$. For partial sums of the Dirichlet series we have

$$\sum_{n=1}^N \frac{a_n}{n^\sigma} = \left(\sum_{n=1}^{N-1} A_n \left(\frac{1}{n^\sigma} - \frac{1}{(n+1)^\sigma} \right) \right) + \frac{A_N}{N^\sigma}.$$

Since $\sigma > 0$ we have

$$\begin{aligned} \left| A_n \left(\frac{1}{n^\sigma} - \frac{1}{(n+1)^\sigma} \right) \right| &= |A_n| \left(\frac{1}{n^\sigma} - \frac{1}{(n+1)^\sigma} \right) \leq Bn^\alpha \sigma \int_n^{n+1} \frac{dx}{x^{\sigma+1}} \\ &\leq B\sigma \frac{1}{n^{\sigma+1-\alpha}}. \end{aligned}$$

Convergence now follows from $\sigma > \alpha$:

$$\left| \sum_{n=1}^N \frac{a_n}{n^\sigma} \right| \leq BN^{\alpha-\sigma} + B\sigma \sum_{n=1}^N n^{\alpha-\sigma-1}. \quad \square$$

8.13 Theorem. $\lim_{\sigma \downarrow 1} (\sigma - 1)\zeta(\sigma) = 1$.

PROOF. The function $f_\sigma: x \mapsto \frac{1}{x^\sigma}$ is monotone decreasing on the interval $(0, \infty)$. So, see Figure 8.3:

$$\sum_{n=2}^{\infty} \frac{1}{n^\sigma} < \int_1^{\infty} \frac{dx}{x^\sigma} < \sum_{n=1}^{\infty} \frac{1}{n^\sigma}.$$

It follows that $\zeta(\sigma) - 1 < \frac{1}{\sigma-1} < \zeta(\sigma)$, and so $1 < (\sigma - 1)\zeta(\sigma) < \sigma$. Therefore, $\lim_{\sigma \downarrow 1} (\sigma - 1)\zeta(\sigma) = 1$. \square

The Riemann zeta function has a continuation to a meromorphic function on \mathbb{C} , also denoted by $\zeta(s)$. Here we confine to a simple proof that shows it has a continuation to the half-plane $\Re(s) > 0$. This suffices for our purposes: we will focus on its behavior near $s = 1$.

8.14 Theorem. *The Riemann zeta function has a continuation to a meromorphic function on $\Re(s) > 0$ which is analytic for all $s \neq 1$ and has a simple pole in $s = 1$. Its residue in $s = 1$ equals 1.*

PROOF. The series $\zeta_2(s) = 1 - \frac{1}{2^s} + \frac{1}{3^s} - \frac{1}{4^s} + \dots$ converges for all s with $\Re(s) > 0$, because $\sum_{n=1}^N a_n = O(1)$. There is absolute convergence in the half-plane $\Re(s) > 1$. In this domain we have

$$\zeta_2(s) = \zeta(s) - 2 \left(\frac{1}{2^s} + \frac{1}{4^s} + \dots \right) = \zeta(s) - \frac{1}{2^{s-1}} \zeta(s).$$

So

$$\zeta(s) = \frac{\zeta_2(s)}{1 - \frac{1}{2^{s-1}}}.$$

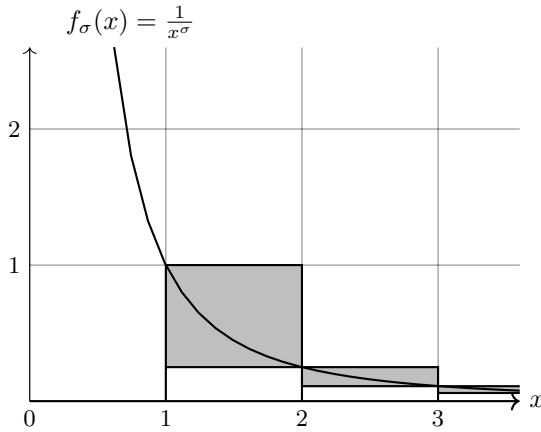


Figure 8.3: Proof of Theorem 8.13

The function $1 - \frac{1}{2^{s-1}}$ is analytic on \mathbb{C} and $\zeta_2(s)$ is analytic on the half-plane $\sigma > 0$. Thus we have continued $\zeta(s)$ to a meromorphic function on this half-plane. By Theorem 8.13 it is clear that it has a pole of first order in $s = 1$ with residue 1. We will show that there are no other poles. Poles can only occur in the zeros of $1 - \frac{1}{2^{s-1}}$, so if $2^{s-1} = 1$, that is $s - 1 = \frac{2k\pi i}{\log 2}$ with $k \in \mathbb{Z}$. If we also consider $\zeta_3(s) = (1 + \frac{1}{2^s} - \frac{2}{3^s}) + (\frac{1}{4^s} + \frac{1}{5^s} - \frac{2}{6^s}) + \dots$, then we get

$$\zeta(s) = \frac{\zeta_3(s)}{1 - \frac{1}{3^{s-1}}}.$$

This is another description of the (unique) continuation of $\zeta(s)$ to a meromorphic function on the half-plane $\sigma > 0$. We have $1 - \frac{1}{3^{s-1}} = 0$ for $s - 1 = \frac{2l\pi i}{\log 3}$ with $l \in \mathbb{Z}$. If s with $\Re(s) > 0$ is a pole, then $s - 1 = \frac{2k\pi i}{\log 2} = \frac{2l\pi i}{\log 3}$, that is $3^k = 2^l$. Then $k = 0$ and so $s = 1$. So the meromorphic function $\zeta(s)$ on the half-plane $\sigma > 0$ is analytic for all $s \neq 1$. \square

As remarked above $\zeta(s)$ has a continuation even to a meromorphic function on \mathbb{C} , analytic for all $s \neq 1$. The construction uses the gamma function $\Gamma(s)$, a meromorphic function on the complex plane extending the function $(n - 1)!$ on \mathbb{N}^* ; for $\Re(s) > 0$ it is defined by

$$\Gamma(s) = \int_0^\infty e^{-y} y^s \frac{dy}{y}.$$

The gamma function has no zeros and the only poles are simple poles at $s = -n$ with $n \in \mathbb{N}$. The residue at $s = -n$ is $-\frac{1}{n!}$. The function

$$Z(s) = \pi^{-\frac{s}{2}} \Gamma(\frac{s}{2}) \zeta(s) \tag{8.2}$$

is called the *completed zeta function*. It is a meromorphic function satisfying the functional equation $Z(s) = Z(1-s)$ and its only poles are simple poles at $s = 0$ and $s = 1$. The residues at these poles are -1 and 1 respectively. The Riemann zeta function has ‘trivial’ zeros in $-2, -4, -6, \dots$. The famous Riemann Conjecture states that all other zeros are located on the line $\sigma = \frac{1}{2}$. See section VII.1 of [31] for details.

8.15 Definition. A sequence $a: \mathbb{N}^* \rightarrow \mathbb{C}$ is also called an *arithmetic function*. Such a function is called *multiplicative* if $a(mn) = a(m)a(n)$ for all $m, n \in \mathbb{N}^*$ with $\gcd(m, n) = 1$. If $a(mn) = a(m)a(n)$ holds for all $m, n \in \mathbb{N}^*$ it is said to be *completely multiplicative*.

For a multiplicative arithmetic function its Dirichlet series is an infinite product, known as the *Euler product* of the Dirichlet series:

8.16 Theorem (Euler product). *Let $a: \mathbb{N}^* \rightarrow \mathbb{C}$ be multiplicative and let the Dirichlet series $\sum \frac{a(n)}{n^s}$ be absolute convergent for an $s \in \mathbb{C}$. Then for this s the series is representable by an infinite product:*

$$\sum_{n=1}^{\infty} \frac{a(n)}{n^s} = \prod_p \sum_{k=0}^{\infty} \frac{a(p^k)}{p^{ks}}.$$

(The product is over all prime numbers p .)

PROOF. Note that for each prime p the series $\sum_{k=0}^{\infty} \frac{a(p^k)}{p^{ks}}$ converges absolutely:

$$\sum_{k=0}^{\infty} \left| \frac{a(p^k)}{p^{ks}} \right| \leq \sum_{n=1}^{\infty} \left| \frac{a(n)}{n^s} \right| < \infty.$$

The first term (for $k = 0$) of the series $\sum_{k=0}^{\infty} \frac{a(p^k)}{p^{ks}}$ is 1. The infinite product converges absolutely. This follows from

$$\sum_p \left| \sum_{k=1}^{\infty} \frac{a(p^k)}{p^{ks}} \right| \leq \sum_p \sum_{k=1}^{\infty} \left| \frac{a(p^k)}{p^{ks}} \right| \leq \sum_{n=1}^{\infty} \left| \frac{a(n)}{n^s} \right| < \infty.$$

An infinite product $\prod_{n=1}^{\infty} b_n$ is said to *converge* if the sequence $\prod_{k=1}^n b_k$ of partial products converges to a number $\neq 0$. If the partial products converge to 0 the infinite product is said to *diverge to 0*.

An infinite product $\prod_{n=1}^{\infty} (1 + a_n)$ with $1 + a_n \neq 0$ for all n is said to be *absolute convergent* if $\prod_{n=1}^{\infty} (1 + |a_n|)$ converges and this is equivalent to $\sum_{n=1}^{\infty} |a_n|$ being convergent. Absolute convergence implies convergence.

Let \mathcal{R} be the set of all maps

$$m: \{\text{prime numbers}\} \rightarrow \mathbb{N}, \quad p \mapsto m_p$$

with $m_p \neq 0$ for only finitely many primes p . By unique factorization the map $n \mapsto (p \mapsto v_p(n))$ is bijection from \mathbb{N}^* to \mathcal{R} . In the domain of absolute convergence of the Dirichlet series $\sum \frac{a(n)}{n^s}$ we then have

$$\sum_{n=1}^{\infty} \frac{a(n)}{n^s} = \sum_{m \in \mathcal{R}} \frac{a(\prod_p p^{m_p})}{(\prod_p p^{m_p})^s} = \sum_{m \in \mathcal{R}} \frac{\prod_p a(p^{m_p})}{\prod_p p^{m_p s}} = \sum_{m \in \mathcal{R}} \prod_p \frac{a(p^{m_p})}{p^{m_p s}}.$$

Now let $N \in \mathbb{N}^*$. Then for \mathcal{R}_N the set of all maps

$$m: \{\text{prime numbers} \leq N\} \rightarrow \mathbb{N}, \quad p \mapsto m_p$$

and $A_N = \{n \in \mathbb{N}^* \mid v_p(n) = 0 \text{ for all } p > N\}$ we have

$$\sum_{n \in A_N} \frac{a(n)}{n^s} = \sum_{m \in \mathcal{R}_N} \prod_{p \leq N} \frac{a(p^{m_p})}{p^{m_p s}} = \prod_{p \leq N} \sum_{k=0}^{\infty} \frac{a(p^k)}{p^{ks}}.$$

From

$$\left| \sum_{n=1}^{\infty} \frac{a(n)}{n^s} - \sum_{n \in A_N} \frac{a(n)}{n^s} \right| = \left| \sum_{n \notin A_N} \frac{a(n)}{n^s} \right| \leq \sum_{n \notin A_N} \left| \frac{a(n)}{n^s} \right| \leq \sum_{n > N} \left| \frac{a(n)}{n^s} \right|$$

and the convergence of $\sum_{n=1}^{\infty} \left| \frac{a(n)}{n^s} \right|$ it then follows that

$$\prod_p \sum_{k=0}^{\infty} \frac{a(p^k)}{p^{ks}} = \lim_{N \rightarrow \infty} \prod_{p \leq N} \sum_{k=0}^{\infty} \frac{a(p^k)}{p^{ks}} = \lim_{N \rightarrow \infty} \sum_{n \in A_N} \frac{a(n)}{n^s} = \sum_{n=1}^{\infty} \frac{a(n)}{n^s}. \quad \square$$

8.17 Corollary. *Let a be a completely multiplicative arithmetic function and $s \in \mathbb{C}$ such that $\sum \frac{a(n)}{n^s}$ converges absolutely. Then*

$$\sum_{n=1}^{\infty} \frac{a(n)}{n^s} = \prod_p \frac{1}{1 - \frac{a(p)}{p^s}}.$$

PROOF. For each p the series

$$\sum_{k=0}^{\infty} \frac{a(p^k)}{p^{ks}} = \sum_{k=0}^{\infty} \left(\frac{a(p)}{p^s} \right)^k$$

is a converging geometric series. Its sum is $\frac{1}{1 - \frac{a(p)}{p^s}}$. □

8.18 Corollary. *For the Riemann zeta function $\zeta(s)$ we have for $\sigma > 1$:*

$$\zeta(s) = \prod_p \frac{1}{1 - \frac{1}{p^s}}.$$

In particular, $\zeta(s)$ does not vanish in the half-plane $\sigma > 1$. □

The factor $\pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})$ in (8.2) can be seen as the ‘Euler factor’ at the prime ∞ .

As we know since Euclid, there are infinitely many prime numbers. This is also implied by this product representation of the Riemann zeta function: if there were only finitely many, then $\zeta(s)$ would not have a pole at $s = 1$. This is of course a far from elementary way of reasoning. However, it will be helpful when looking at special collections of prime numbers or prime ideals. The first steps in this direction will be made in section 8.5.

8.4 The Dedekind zeta function of a number field

With each number field we associate a Dirichlet series which contains a lot of information on the number field.

Since in the context of Dirichlet series a complex variable is denoted by s , the notations for the numbers of real and complex primes of a number field K will be $r(K)$ and $s(K)$ instead of simply r and s .

8.19 Definition. Let K be a number field. The Dirichlet series of the arithmetic function

$$j_K: \mathbb{N}^* \rightarrow \mathbb{N} \subseteq \mathbb{C}, \quad n \mapsto \#\{\mathfrak{a} \mid \mathfrak{a} \text{ is an ideal of } \mathcal{O}_K \text{ with } N(\mathfrak{a}) = n\},$$

considered in section 8.3, is called the *Dedekind zeta function* of K ; notation: $\zeta_K(s)$. So

$$\zeta_K(s) = \sum_{n=1}^{\infty} \frac{j_K(n)}{n^s}.$$

Given an ideal class C of K we have the *partial Dedekind zeta function* of the ideal class C

$$\zeta_C(s) = \sum_{n=1}^{\infty} \frac{j_C(n)}{n^s}.$$

determined by the function j_C which only counts ideals in the class C . Obviously,

$$\zeta_K(s) = \sum_{C \in \mathcal{C}(K)} \zeta_C(s).$$

The Dedekind zeta function generalizes the Riemann zeta function: $\zeta(s) = \zeta_{\mathbb{Q}}(s)$. By Theorem 8.3 $\sum_{n=1}^N j_C(n) = O(N)$, so by Theorem 8.12 the series converge for $\sigma > 1$. Theorem 8.3 contains more detailed information on the asymptotic behavior of $J_C(N)$ and $J_K(N)$. This leads to:

8.20 Theorem. *Let K be a number field of degree d with r real embeddings and s pairs of complex embeddings. Then for each ideal class C the partial zeta function $\zeta_C(s)$ has a continuation to a meromorphic function on the half-plane $\Re(s) > 1 - \frac{1}{d}$ with one simple pole in $s = 1$ and so has the Dedekind zeta function $\zeta_K(s)$. The residue of $\zeta_C(s)$ at $s = 1$ equals*

$$\frac{2^{r(K)}(2\pi)^{s(K)} \operatorname{Reg}(K)}{w(K)\sqrt{|\operatorname{disc}(K)|}}$$

and the residue of $\zeta_K(s)$ at $s = 1$ equals

$$\frac{2^{r(K)}(2\pi)^{s(K)} h(K) \operatorname{Reg}(K)}{w(K)\sqrt{|\operatorname{disc}(K)|}}.$$

PROOF. Put $\kappa = \frac{2^{r(K)}(2\pi)^{s(K)} \operatorname{Reg}(K)}{w(K)\sqrt{|\operatorname{disc}(K)|}}$ and consider the Dirichlet series

$$\sum_{n=1}^{\infty} \frac{j_C(n) - \kappa}{n^s}.$$

By Theorem 8.3 we have

$$\sum_{n=1}^N (j_C(n) - \kappa) = J_C(N) - \kappa N = O(N^{1-\frac{1}{d}}).$$

So by Theorem 8.12 the Dirichlet series converges to an analytic function on $\Re(s) > 1 - \frac{1}{d}$. On the other hand we have

$$\zeta_C(s) = \sum_{n=1}^{\infty} \frac{j_C(n)}{n^s} = \sum_{n=1}^{\infty} \frac{j_C(n) - \kappa}{n^s} + \sum_{n=1}^{\infty} \frac{\kappa}{n^s} = \left(\sum_{n=1}^{\infty} \frac{j_C(n) - \kappa}{n^s} \right) + \kappa \cdot \zeta(s).$$

The theorem now follows from Theorem 8.14. \square

The real number

$$g(K) = \log \frac{w(K)\sqrt{|\operatorname{disc}(K)|}}{2^{r(K)}(2\pi)^{s(K)}}$$

is, motivated by an analogy with function fields, known as the *genus* of the number field K . So, with this notation, the residue at $s = 1$ of the Dedekind zeta function is

$$\frac{h(K) \operatorname{Reg}(K)}{e^{g(K)}}.$$

As for the Riemann zeta function, there is a completed Dedekind zeta function

$$Z_K(s) = Z_{\infty}(s)\zeta_K(s)$$

satisfying the functional equation $Z_K(s) = Z_K(1-s)$. It is a meromorphic function with only poles at $s = 0$ and $s = 1$. These are simple poles with residues

$$-\frac{2^{r(K)}h(K)\operatorname{Reg}(K)}{w(K)} \quad \text{and} \quad \frac{2^{r(K)}h(K)\operatorname{Reg}(K)}{w(K)}.$$

The factor $Z_\infty(s)$ depends on a higher-dimensional gamma function $\Gamma_K(s)$:

$$Z_\infty(s) = |\operatorname{disc}(K)|^{\frac{s}{2}} \pi^{-\frac{ns}{2}} \Gamma_K\left(\frac{s}{2}\right).$$

For details see the sections 4 and 5 of Chapter VII of [31].

8.21 Definition and notation. For $\sigma > 1$ the Dedekind zeta function converges absolutely. It easily follows that for such σ there is no ambiguity in writing

$$\zeta_K(s) = \sum_{\mathfrak{a} \in \mathbb{I}^+(K)} \frac{1}{\mathbf{N}(\mathfrak{a})^s}.$$

More generally, for a given $b: \mathbb{I}^+(K) \rightarrow \mathbb{C}$ we have an arithmetic function a given by

$$a(n) = \sum_{\substack{\mathfrak{a} \in \mathbb{I}^+(K) \\ \mathbf{N}(\mathfrak{a})=n}} b(\mathfrak{a})$$

and we define the *Dirichlet series* of the function $b: \mathbb{I}^+(K) \rightarrow \mathbb{C}$ by

$$\sum_{\mathfrak{a} \in \mathbb{I}^+(K)} \frac{b(\mathfrak{a})}{\mathbf{N}(\mathfrak{a})^s} = \sum_{n=1}^{\infty} \frac{a(n)}{n^s}.$$

If the Dirichlet series $\sum_n \frac{a(n)}{n^s}$ is absolutely convergent, the Dirichlet series of b is absolutely convergent with respect to any ordering of its terms. In this case it is said to be *absolutely convergent* as well.

The next theorem is a straightforward generalization of Theorem 8.16. First we generalize the definitions of multiplicative and completely multiplicative.

8.22 Definition. Let K be a number field. We call a function $b: \mathbb{I}^+(K) \rightarrow \mathbb{C}$ *multiplicative* if for all comaximal $\mathfrak{a}_1, \mathfrak{a}_2 \in \mathbb{I}^+(K)$ we have $b(\mathfrak{a}_1\mathfrak{a}_2) = b(\mathfrak{a}_1)b(\mathfrak{a}_2)$. The function is called *completely multiplicative* if $b(\mathfrak{a}_1\mathfrak{a}_2) = b(\mathfrak{a}_1)b(\mathfrak{a}_2)$ for all $\mathfrak{a}, \mathfrak{b} \in \mathbb{I}^+(K)$.

8.23 Theorem. Let K be a number field, $b: \mathbb{I}^+(K) \rightarrow \mathbb{C}$ multiplicative and $s \in \mathbb{C}$ such that the series

$$\sum_{\mathfrak{a} \in \mathbb{I}^+(K)} \frac{b(\mathfrak{a})}{\mathbf{N}(\mathfrak{a})^s}$$

converges absolutely. Then the series is representable by an infinite product:

$$\sum_{\mathfrak{a} \in \mathbb{I}^+(K)} \frac{b(\mathfrak{a})}{N(\mathfrak{a})^s} = \prod_{\mathfrak{p}} \sum_{k=0}^{\infty} \frac{b(\mathfrak{p}^k)}{N(\mathfrak{p})^{k.s}},$$

where the infinite product is over all $\mathfrak{p} \in \text{Max}(\mathcal{O}_K)$.

PROOF. As in the proof of Theorem 8.16 use unique factorization. In this situation the unique factorization of nonzero ideals as a product of prime ideals. \square

8.24 Corollary. Let K be a number field and let $b: \mathbb{I}^+(K) \rightarrow \mathbb{C}$ be completely multiplicative. If the series $\sum_{\mathfrak{a}} \frac{b(\mathfrak{a})}{N(\mathfrak{a})^s}$ converges absolutely in $s \in \mathbb{C}$, then for this s we have

$$\sum_{\mathfrak{a}} \frac{b(\mathfrak{a})}{N(\mathfrak{a})^s} = \prod_{\mathfrak{p}} \frac{1}{1 - \frac{b(\mathfrak{p})}{N(\mathfrak{p})^s}}. \quad \square$$

8.25 Corollary. For the Dedekind zeta function of a number field K we have

$$\zeta_K(s) = \prod_{\mathfrak{p}} \frac{1}{1 - \frac{1}{N(\mathfrak{p})^s}}$$

for $\Re(s) > 1$. \square

The formula

$$\text{Res}_{s=1} \zeta_K(s) = \frac{2^{r(K)} (2\pi)^{s(K)} h(K) \text{Reg}(K)}{w(K) \sqrt{|\text{disc}(K)|}}$$

is known as the *class number formula*. Especially in connection with Corollary 8.25 it gives information on the product $h(K) \text{Reg}(K)$.

We have continued the Dedekind zeta function of a number field K to a meromorphic function on the half-plane $\Re(s) > 1 - \frac{1}{[K:\mathbb{Q}]}$. For our purposes this suffices, but more is possible: it has a continuation to a meromorphic function on the entire complex plane. Also this continuation has just one pole, the simple pole at $s = 1$.

8.5 Dirichlet density

For P a collection of nonzero prime ideals of the ring of integers of a number field K consider the series

$$\sum_{\mathfrak{p} \in P} \frac{1}{N(\mathfrak{p})^s}.$$

It is the Dirichlet series of the function

$$\mathbb{I}^+(K) \rightarrow \mathbb{C}, \quad \mathfrak{a} \mapsto \begin{cases} 1 & \text{if } \mathfrak{a} \text{ is a maximal ideal,} \\ 0 & \text{otherwise.} \end{cases}$$

The series converges absolutely in the half-plane $\sigma > 1$:

$$\sum_{\mathfrak{p} \in P} \left| \frac{1}{N(\mathfrak{p})^s} \right| = \sum_{\mathfrak{p} \in P} \frac{1}{N(\mathfrak{p})^\sigma} \leq \sum_{\mathfrak{a} \in \mathbb{I}^+(K)} \frac{1}{N(\mathfrak{a})^\sigma}.$$

The Dirichlet density of the collection P is determined by its behavior near $s = 1$:

8.26 Definition. Let K be a number field and P a set of nonzero prime ideals of \mathcal{O}_K . The set P is said to have *Dirichlet density* $\delta(P)$ if

$$\delta(P) = \lim_{s \downarrow 1} \frac{\sum_{\mathfrak{p} \in P} \frac{1}{N(\mathfrak{p})^s}}{\sum_{\mathfrak{p}} \frac{1}{N(\mathfrak{p})^s}},$$

provided that the limit exists.

Rules for a density are satisfied by the Dirichlet density:

8.27 Proposition. Let K be a number field and let $P, P' \subseteq \text{Max}(\mathcal{O}_K)$ both have a Dirichlet density. Then:

- (i) $\delta(\text{Max}(\mathcal{O}_K)) = 1$.
- (ii) $\delta(P) \in \mathbb{R}$ and $0 \leq \delta(P) \leq 1$.
- (iii) If $P \cap P' = \emptyset$, then $\delta(P \cup P') = \delta(P) + \delta(P')$.
- (iv) If $P \subseteq P'$, then $\delta(P) \leq \delta(P')$.

PROOF. (i) and (iii) are obvious and for (ii) restrict the domain to $(1, \infty)$. For (iv) apply (iii) to $P' \setminus P$ and P . \square

8.28 Notation. The notation $f \sim g$ is used to express that the difference $f - g$ of functions f, g defined on $\sigma > 1$ is bounded in a neighborhood of $s = 1$.

8.29 Definition. Let K be a number field. A function $\chi: \mathbb{I}^+(K) \rightarrow \mathbb{C}$ is called an *ideal character* of K if

- 1. $\chi(\mathfrak{a}\mathfrak{b}) = \chi(\mathfrak{a})\chi(\mathfrak{b})$ for all $\mathfrak{a}, \mathfrak{b} \in \mathbb{I}^+(K)$,
- 2. $|\chi(\mathfrak{a})| = 1$ or $\chi(\mathfrak{a}) = 0$ for all $\mathfrak{a} \in \mathbb{I}^+(K)$.

So an ideal character of K is a completely multiplicative map $\chi: \mathbb{I}^+(K) \rightarrow \mathbb{C}$ in the sense of Definition 8.22 which satisfies the second condition above. An ideal character is determined by the values $\chi(\mathfrak{p})$ for $\mathfrak{p} \in \text{Max}(\mathcal{O}_K)$.

An ideal character χ determines a set $P = \{\mathfrak{p} \in \text{Max}(\mathcal{O}_K) \mid \chi(\mathfrak{p}) = 0\}$ and induces a group homomorphism

$$\chi': \mathbb{I}^P(K) \rightarrow \mathbb{C}^*,$$

where $\mathbb{I}^P(K) = \{\mathfrak{a} \in \mathbb{I}(K) \mid v_{\mathfrak{p}}(\mathfrak{a}) = 0 \text{ for all } \mathfrak{p} \in P\}$. The homomorphism χ' is a character of the group $\mathbb{I}^P(K)$ with values in the unit circle in \mathbb{C} .

8.30 Convention. The complex function \log always stands for the principal branch of the logarithm: for $r, \vartheta \in \mathbb{R}$, $r > 0$ and $-\pi < \vartheta \leq \pi$ we have $\log(re^{i\vartheta}) = \log r + i\vartheta$, where the last \log denotes the real natural logarithm.

8.31 Proposition. Let K be a number field and χ an ideal character of K . Then the series $\sum_{\mathfrak{a}} \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s}$ converges absolutely for $\Re(s) > 1$ and in this half-plane the series is representable by an infinite product

$$\sum_{\mathfrak{a}} \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s} = \prod_{\mathfrak{p}} \frac{1}{1 - \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s}}.$$

Moreover, $\sum_{\mathfrak{p}} \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s}$ converges absolutely on the half-plane $\Re(s) > 1$ and

$$\log\left(\sum_{\mathfrak{a}} \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s}\right) \sim \sum_{\mathfrak{p}} \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s}.$$

PROOF. $\sum_{\mathfrak{a}} \left| \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s} \right|$ and $\sum_{\mathfrak{p}} \left| \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s} \right|$ both are dominated by the Dedekind zeta function of K , a series converging absolutely on the half-plane $\Re(s) > 1$. The product representation on $\Re(s) > 1$ follows from Corollary 8.24.

In a neighborhood of $s = 1$ we have

$$\begin{aligned} \log\left(\sum_{\mathfrak{a}} \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s}\right) &= \log\left(\prod_{\mathfrak{p}} \frac{1}{1 - \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s}}\right) \sim \sum_{\mathfrak{p}} \log \frac{1}{1 - \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s}} \\ &= -\sum_{\mathfrak{p}} \log\left(1 - \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s}\right) = \sum_{\mathfrak{p}} \sum_{k=1}^{\infty} \frac{\chi(\mathfrak{p})^k}{kN(\mathfrak{p})^{ks}} \\ &= \sum_{\mathfrak{p}} \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s} + \sum_{\mathfrak{p}} \sum_{k=2}^{\infty} \frac{\chi(\mathfrak{p})^k}{kN(\mathfrak{p})^{ks}} \end{aligned}$$

and for each \mathfrak{p}

$$\left| \sum_{k=2}^{\infty} \frac{\chi(\mathfrak{p})^k}{kN(\mathfrak{p})^{ks}} \right| \leq \sum_{k=2}^{\infty} \frac{1}{kN(\mathfrak{p})^{k\sigma}} \leq \sum_{k=2}^{\infty} \frac{1}{2N(\mathfrak{p})^{k\sigma}} = \frac{1}{2N(\mathfrak{p})^{2\sigma}} \frac{1}{1 - \frac{1}{N(\mathfrak{p})^\sigma}} \leq \frac{1}{N(\mathfrak{p})^{2\sigma}}$$

Hence

$$\left| \sum_{\mathfrak{p}} \sum_{k=2}^{\infty} \frac{\chi(\mathfrak{p})^k}{kN(\mathfrak{p})^{ks}} \right| \leq \sum_{\mathfrak{p}} \frac{1}{N(\mathfrak{p})^{2\sigma}}$$

and this is bounded for $\sigma > \frac{1}{2}$. □

In particular we have:

8.32 Corollary. *Let K be a number field. Then*

$$\log \zeta_K(s) \sim \sum_{\mathfrak{p}} \frac{1}{N(\mathfrak{p})^s}. \quad \square$$

8.33 Proposition. *Let K be a number field. Then*

$$\lim_{s \downarrow 1} \frac{\sum_{\mathfrak{p}} \frac{1}{N(\mathfrak{p})^s}}{-\log(s-1)} = 1.$$

PROOF. For the Dedekind zeta function of K we have by Theorem 8.20

$$\lim_{s \rightarrow 1} (s-1)\zeta_K(s) = \kappa \neq 0,$$

where κ is the residue of $\zeta_K(s)$ at $s = 1$. The last identity implies that

$$\log \zeta_K(s) \sim \log(s-1).$$

By Corollary 8.32 the function $f(s) = \sum_{\mathfrak{p}} \frac{1}{N(\mathfrak{p})^s} + \log(s-1)$ is bounded in a neighborhood of $s = 1$. So we have

$$\frac{\sum_{\mathfrak{p}} \frac{1}{N(\mathfrak{p})^s}}{-\log(s-1)} = \frac{f(s) - \log(s-1)}{-\log(s-1)} = 1 - \frac{f(s)}{\log(s-1)} \rightarrow 1 \quad \text{for } s \downarrow 1. \quad \square$$

8.34 Corollary. *Let K be a number field and $P \subseteq \text{Max}(\mathcal{O}_K)$. Then*

$$\lim_{s \downarrow 1} \frac{\sum_{\mathfrak{p} \in P} \frac{1}{N(\mathfrak{p})^s}}{\sum_{\mathfrak{p}} \frac{1}{N(\mathfrak{p})^s}} = \lim_{s \downarrow 1} \frac{\sum_{\mathfrak{p} \in P} \frac{1}{N(\mathfrak{p})^s}}{-\log(s-1)}.$$

(If one of the limits exists, then so does the other.) □

So an alternative definition of the Dirichlet density is

$$\delta(P) = \lim_{s \downarrow 1} \frac{\sum_{\mathfrak{p} \in P} \frac{1}{N(\mathfrak{p})^s}}{-\log(s-1)}.$$

8.35 Corollary. *Let K be a number field. Finite sets of nonzero prime ideals of \mathcal{O}_K have Dirichlet density 0.*

PROOF. For P finite $\sum_{\mathfrak{p} \in P} \frac{1}{N(\mathfrak{p})^s}$ is a finite sum of functions which are analytic in $s = 1$. □

The Dirichlet density is often used to show the existence of infinitely many prime ideals that satisfy certain conditions: if a collection of prime ideals has a nonzero Dirichlet density, the collection is infinite.

The *absolute residue class degree* of a prime ideal of a number field is its residue class degree over \mathbb{Q} . It equals 1 if and only if the norm of the prime ideal is a prime number. Prime ideals of absolute residue class degree > 1 do not contribute to the Dirichlet density. This follows from the following proposition.

8.36 Proposition. *Let K be a number field and P_1 the set of prime ideals of \mathcal{O}_K of absolute residue class degree 1. Then $\delta(P_1) = 1$.*

PROOF. Let Q be the set of all prime ideals of K of absolute residue class degree > 1 . It suffices to prove that $\sum_{\mathfrak{p} \in Q} \frac{1}{N(\mathfrak{p})^s} \sim 0$. For $\mathfrak{p} \in Q$ we have $N(\mathfrak{p}) \geq p^2$, where p is the prime number below \mathfrak{p} . For each prime number p there are at most $[K : \mathbb{Q}]$ prime ideals of \mathcal{O}_K above p . Therefore, for $\sigma > 1$ we have

$$\begin{aligned} \left| \sum_{\mathfrak{p} \in Q} \frac{1}{N(\mathfrak{p})^s} \right| &\leq \sum_p \sum_{\substack{\mathfrak{p} \in Q \\ \text{above } p}} \frac{1}{N(\mathfrak{p})^\sigma} \leq \sum_p \sum_{\substack{\mathfrak{p} \in Q \\ \text{above } p}} \frac{1}{p^2} \leq \sum_p \frac{[K : \mathbb{Q}]}{p^2} \\ &\leq [K : \mathbb{Q}] \sum_{n=1}^{\infty} \frac{1}{n^2} = [K : \mathbb{Q}] \zeta(2). \quad \square \end{aligned}$$

8.37 Theorem (Kronecker). *Let $L : K$ be a Galois extension of number fields and P the collection of prime ideals of \mathcal{O}_K which split completely in L . Then $\delta(P) = \frac{1}{[L : K]}$.*

PROOF. Let Q be the set of prime ideals of \mathcal{O}_L above prime ideals in P and Q_1 the set of prime ideals of L having absolute residue class degree 1. Prime ideals in $Q_1 \setminus Q$ are ramified over K and so they are finite in number. Hence $\delta(Q \cap Q_1) = \delta(Q_1) = 1$ and since $Q \supseteq Q \cap Q_1$ it follows that $\delta(Q) = 1$, that is

$$\lim_{s \downarrow 1} \frac{\sum_{\mathfrak{q} \in Q} \frac{1}{N(\mathfrak{p})^s}}{-\log(s-1)} = 1.$$

Because

$$\sum_{\mathfrak{q} \in Q} \frac{1}{N(\mathfrak{q})^s} = \sum_{\mathfrak{p} \in P} \sum_{\substack{\mathfrak{q} \in Q \\ \mathfrak{q} \cap K = \mathfrak{p}}} \frac{1}{N(\mathfrak{p})^s} = \sum_{\mathfrak{p} \in P} \frac{[L : K]}{N(\mathfrak{p})^s} = [L : K] \sum_{\mathfrak{p} \in P} \frac{1}{N(\mathfrak{p})^s},$$

we now have

$$\delta(P) = \lim_{s \downarrow 1} \frac{\sum_{\mathfrak{p} \in P} \frac{1}{N(\mathfrak{p})^s}}{-\log(s-1)} = \frac{1}{[L : K]}. \quad \square$$

8.38 Corollary. *Let $L_1 : K$ and $L_2 : K$ be Galois extensions of number fields and P_i the collection of prime ideals of \mathcal{O}_K which split completely in L_i (for $i = 1, 2$). Then $L_1 \subseteq L_2 \iff P_1 \supseteq P_2$.*

PROOF. If $L_1 \subseteq L_2$, then clearly $P_1 \supseteq P_2$. So assume $P_1 \supseteq P_2$ and consider the extension $L_1L_2 : K$. By Theorem 7.50 the prime ideals which split completely in L_1L_2 are precisely the prime ideals which split completely in both L_1 and L_2 , so this set of prime ideals is $P_1 \cap P_2 = P_2$. By Theorem 8.37 we have

$$[L_1L_2 : K] = \frac{1}{\delta(P_2)} = [L_2 : K]$$

and hence $L_1L_2 = L_2$, that is $L_1 \subseteq L_2$. \square

This is an interesting result: Galois extensions of a number field K are determined by the collection of prime ideals of \mathcal{O}_K which split completely in the extension field. It was conjectured by Kronecker and proved by M. Bauer in 1903. It does not tell, however, which are the prime ideal collections that occur as such collections. For abelian extensions the solution of this problem is given by class field theory. It is described in chapter 13 and the proof is completed in chapter 15.

8.6 Frobenius Density Theorem

There are various theorems on the Dirichlet density of collections of prime ideals with a given splitting behavior in a field extension. The simplest, but important, one is Theorem 8.37 in the previous section. Much more advanced is Chebotarev's Density Theorem proved in section 15.4. A weaker version of this theorem is the Frobenius Density Theorem. First we consider the case of an abelian extension.

8.39 Theorem. *Let $L : K$ be an abelian number field extension. Let Z be a cyclic subgroup of $\text{Gal}(L : K)$ of order n and P the collection of nonramifying prime ideals of \mathcal{O}_K which satisfy $\langle \varphi_{\mathfrak{p}}^{(L)} \rangle = Z$. Then $\delta(P) = \frac{\varphi(n)}{[L:K]}$.*

PROOF. The proof is by induction on n . For $n = 1$ the theorem reduces to Theorem 8.37. So let's assume that $n > 1$ and that the theorem is true for smaller cyclic subgroups of the Galois group. The collection P consists of nonramifying prime ideals with their Frobenius automorphism in Z , but not in a proper subgroup of Z . Subgroups of Z correspond to divisors of n . Let Z_d be the subgroup of Z of order d and P_d the collection of nonramifying primes \mathfrak{p} with $\langle \varphi_{\mathfrak{p}}^{(L)} \rangle = Z_d$. Then $Z_n = Z$ and $P_n = P$. Let Q be the collection of nonramifying primes \mathfrak{p} with $\varphi_{\mathfrak{p}}^{(L)} \in Z$. Then $\mathfrak{p} \in Q$ if and only if \mathfrak{p} splits completely in L^Z . Hence by Theorem 8.37 $\delta(Q) = \frac{1}{[L^Z:K]} = \frac{n}{[L:K]}$. The set Q is the disjoint union of all P_d with $d \mid n$. By induction hypothesis all P_d with $d \neq n$ have a Dirichlet density, so P has a Dirichlet density as well and we have

$$\delta(P) = \delta(Q) - \sum_{\substack{d \mid n \\ d \neq n}} \delta(P_d) = \frac{n}{[L:K]} - \sum_{\substack{d \mid n \\ d \neq n}} \frac{\varphi(d)}{[L:K]} = \frac{\varphi(n)}{[L:K]}. \quad \square$$

If there is a prime ideal which remains prime in a Galois extension, then the Galois group of this extension is cyclic. We now have:

8.40 Corollary. *Let $L : K$ be a cyclic extension of number fields of degree n and P the set of prime ideals of \mathcal{O}_K which remain prime in L . Then $\delta(P) = \frac{\varphi(n)}{n}$. In particular infinitely many prime ideals of \mathcal{O}_K remain prime.* \square

We generalize Theorem 8.39 to the case of a Galois extension of number fields.

8.41 Definition. An equivalence relation \simeq in G is defined by

$$\sigma_1 \simeq \sigma_2 \iff \langle \sigma_1 \rangle = \sigma \langle \sigma_2 \rangle \sigma^{-1} \quad \text{for some } \sigma \in G.$$

The equivalence classes are called *divisions* of G and the division represented by $\sigma \in G$ is denoted by $[\sigma]$.

8.42 Lemma. *Let G be a finite group, $\sigma \in G$ of order n and $Z = \langle \sigma \rangle$. Then $\#([\sigma]) = \varphi(n)(G : N_G(Z))$.*

PROOF. The number of subgroups of G conjugate to Z is $(G : N_G(Z))$. Generators of different subgroups conjugate to Z differ and each of them has $\varphi(n)$ generators. \square

8.43 Frobenius Density Theorem. *Let $L : K$ be a Galois extension of number fields, $G = \text{Gal}(L : K)$, D a division in G and P the collection of prime ideals \mathfrak{p} of \mathcal{O}_K for which there is a prime ideal \mathfrak{q} of \mathcal{O}_L above \mathfrak{p} with $\varphi_K(\mathfrak{q}) \in D$. Then $\delta(P) = \frac{\#(D)}{[L : K]}$.*

PROOF. Let $\mathfrak{p} \in P$ and \mathfrak{q} a prime ideal of \mathcal{O}_L above \mathfrak{p} with $\varphi_K(\mathfrak{q}) \in D$. Put $\sigma = \varphi_K(\mathfrak{q})$ and $Z = \langle \sigma \rangle$. By Proposition 7.54 the number of prime ideals of \mathcal{O}_{L^Z} above \mathfrak{p} with residue class degree 1 is equal to $(G : N_G(Z))$. For the set P' of prime ideals \mathfrak{p}' of \mathcal{O}_{L^Z} above a prime ideal $\mathfrak{p} \in P$ with $f_K(\mathfrak{p}') = 1$ we have

$$\delta(P') = (N_G(Z) : Z) \cdot \delta(P).$$

For the set Q of prime ideals \mathfrak{p}' of \mathcal{O}_{L^Z} which do not ramify in L and satisfy $\varphi_{\mathfrak{p}'}^{(L)} \in D$ we have by Theorem 8.39

$$\delta(Q) = \frac{\varphi(n)}{n},$$

where $n = o(\sigma)$. Because $P' \subseteq Q$ and $Q \setminus P'$ consists of prime ideals with residue class degree over K equal to 1 and a finite collection of ramified primes, the sets P' and Q have equal Dirichlet density. Hence by Lemma 8.42

$$\begin{aligned} \delta(P) &= \frac{\delta(P')}{(N_G(Z) : Z)} = \frac{\delta(Q)}{(N_G(Z) : Z)} \\ &= \frac{\varphi(n)}{n \cdot (N_G(Z) : Z)} = \frac{\varphi(n)}{\#(N_G(Z))} = \frac{\varphi(n) \cdot (G : N_G(Z))}{\#(G)} = \frac{\#(D)}{[L : K]}. \quad \square \end{aligned}$$

EXERCISES

1. Compute the residue at $s = 1$ of the Dedekind zeta functions of the fields

$$\mathbb{Q}(\sqrt{-2}, \sqrt{3}), \quad \mathbb{Q}(\sqrt{2}, \sqrt{3}) \quad \text{and} \quad \mathbb{Q}(i, \sqrt{6}).$$

2. Compute at $s = 1$ the residue of the Dedekind zeta functions of the fields

$$\mathbb{Q}(\sqrt[3]{2}), \quad \mathbb{Q}(\sqrt[3]{7}) \quad \text{and} \quad \mathbb{Q}(\sqrt[3]{11}).$$

3. Compute the residue at $s = 1$ of the Dedekind zeta function of the field $\mathbb{Q}(\zeta_5)$.

4. The class number formula is based on counting ideals in ideal classes. What is the effect on the formula if narrow ideal classes are used? Narrow ideal classes were introduced in exercise 10 of chapter 6.

5. Determine the Dirichlet density of the set of prime numbers for which 2 is a square modulo p . What about 2 a cube modulo p ? And 2 a fourth power modulo p ?

6. Let K be a number field, $g \in \mathcal{O}_K[X]$ monic and irreducible over K , L the splitting field of g over K and $\alpha \in L$ such that $g(\alpha) = 0$.

- (i) Prove that for all but finitely many $\mathfrak{p} \in \text{Max}(\mathcal{O}_K)$ the following are equivalent:

g has a root modulo \mathfrak{p} ,

$f_K(\mathfrak{p}') = 1$ for some $\mathfrak{p}' \in \text{Max}(\mathcal{O}_{K(\alpha)})$ above \mathfrak{p} ,

$Z_K(\mathfrak{q}) \subseteq \text{Gal}(L : K(\alpha))$ for some $\mathfrak{q} \in \text{Max}(\mathcal{O}_L)$ above \mathfrak{p} .

- (ii) Assume that $\deg(g) > 1$. Prove that g has no roots modulo \mathfrak{p} for infinitely many $\mathfrak{p} \in \text{Max}(\mathcal{O}_K)$.

7. Let K be a number field and $f \in \mathcal{O}_K[X]$ monic, irreducible over K and of prime degree. Prove that f is irreducible modulo \mathfrak{p} for infinitely many $\mathfrak{p} \in \text{Max}(\mathcal{O}_K)$.

9 Abelian Number Fields

In section 9.1 the Kronecker-Weber Theorem is proved: every abelian number field is contained in a cyclotomic field. As we have seen in the previous chapter, for the splitting of primes in cyclotomic fields there is a simple description. As a consequence the same is true for any abelian number field. This leads in section 9.3 to the notion of Dirichlet character. These characters describe the splitting behavior of primes in an abelian number field. In section 9.4 it is shown that abelian number fields correspond to finite groups of Dirichlet characters. Since Dedekind zeta functions of abelian number fields are determined by this splitting behavior, Dirichlet characters are particularly useful in the study of these zeta functions. A Dirichlet character determines a Dirichlet series, the L -series of the character (section 9.5). Via Gauß sums of Dirichlet characters this leads to applications concerning class numbers of abelian number fields and units of cyclotomic fields, described in the last section.

In this chapter and later chapters the terminology of categories and functors is used. However, more advanced category theory is avoided.

9.1 The Kronecker-Weber Theorem

The first complete proof of the Kronecker-Weber Theorem was Hilbert's in 1896. It made use of the theory of ramification groups, here described in section 7.5. Let p be an odd prime and $r \in \mathbb{N}^*$. The cyclotomic field $\mathbb{Q}(\zeta_{p^{r+1}})$ contains a unique subfield K of degree p^r . The prime p is the only prime that ramifies in K . We will see that this is the only number field of degree p^r with this property (Proposition 9.5). For the prime 2 we will derive a similar result (Proposition 9.8). The main ingredient for the odd prime case is the next proposition. The Kronecker-Weber Theorem will follow by reduction to these special cases.

9.1 Lemma. *Let p be an odd prime and K an abelian number field of degree p in which p is the only ramifying prime: $p\mathcal{O}_K = \mathfrak{p}^p$ with $\mathfrak{p} \in \text{Max}(\mathcal{O}_K)$. Then $V_2(\mathfrak{p}) = \{1\}$ and $\text{disc}(K) = p^{2(p-1)}$.*

PROOF. There is a unique $t \in \mathbb{N}^*$ such that $V_t(\mathfrak{p}) = \text{Gal}(K : \mathbb{Q})$ and $V_{t+1}(\mathfrak{p}) = \{1\}$. We will prove that $t = 1$. Take $\pi \in \mathcal{O}_K$ with $v_{\mathfrak{p}}(\pi) = 1$ and let $f \in \mathbb{Z}[X]$ be

the minimal polynomial of π over \mathbb{Q} . Then $\deg(f) = p$. Let σ be a generator of $\text{Gal}(K : \mathbb{Q})$. Then

$$f(X) = (X - \pi)(X - \sigma(\pi)) \cdots (X - \sigma^{p-1}(\pi)) \quad (9.1)$$

and so

$$f'(\pi) = (\pi - \sigma(\pi))(\pi - \sigma^2(\pi)) \cdots (\pi - \sigma^{p-1}(\pi)).$$

We have $V_t \setminus V_{t+1} = \{\sigma, \sigma^2, \dots, \sigma^{p-1}\}$ and so $v_{\mathfrak{p}}(\pi - \sigma^i(\pi)) = t+1$ for $i = 1, \dots, p-1$. Hence

$$v_{\mathfrak{p}}(f'(\pi)) = (t+1)(p-1).$$

Put $f(X) = X^p + a_1X^{p-1} + a_2X^{p-2} + \cdots + a_{p-1}X + a_p$ with $a_1, \dots, a_p \in \mathbb{Z}$. From identity (9.1) it follows that

$$\bar{f}(X) = X^p \in (\mathcal{O}_K/\mathfrak{p})[X].$$

(In fact, by exercise 20(i) of chapter 3 the polynomial f is an Eisenstein p -polynomial; see also Theorem 7.20.) We have $a_1, \dots, a_p \in \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, say $v_{\mathfrak{p}}(a_i) = n_i$ with $n_i \in \mathbb{N}^*$ or $n_i = \infty$. Then $v_{\mathfrak{p}}(a_i) = n_i p$. Apply $v_{\mathfrak{p}}$ to

$$f'(\pi) = p\pi^{p-1} + a_1(p-1)\pi^{p-2} + \cdots + a_{p-1}.$$

The valuations of terms on the right hand side are subsequently

$$p + (p-1), \quad n_1 p + (p-2), \quad n_2 p + (p-3), \quad \dots, \quad n_{p-1} p.$$

Some, but not all, of these might equal ∞ . The others are all different, because they differ modulo p . It follows that

$$(t+1)(p-1) = \min(2p-1, n_1 p + (p-2), \dots, n_{p-1} p) \leq 2p-1,$$

that is $(t-1)p \leq t$ and so, since $p \geq 3$, we have $2t \leq 3$. Hence, $t = 1$.

By Proposition 7.21 $(\mathcal{O}_K)_{\mathfrak{p}} = \mathbb{Z}_{\{p\}}[\pi]$. Since K is totally real and p is the only ramifying prime, we have $\mathcal{O}_K = \mathbb{Z}[\pi]$ and $\text{disc}(K) = \text{disc}(1, \pi, \dots, \pi^{p-1}) = N_{\mathbb{Q}}^K(f'(\pi)) = p^N$, where $N = v_{\mathfrak{p}}(N_{\mathbb{Q}}^K(f'(\pi))) = v_{\mathfrak{p}}(f'(\pi)) = 2(p-1)$. \square

9.2 Lemma. *Let p be a prime and L an abelian number field of degree p^2 in which p totally ramifies. Let K be a subfield of L of degree p . Then $v_{\mathfrak{p}}(\mathfrak{d}_K(L)) = v_p(\text{disc}(L)) - p \cdot v_p(\text{disc}(K))$, where \mathfrak{p} is the unique prime ideal of \mathcal{O}_K above p .*

PROOF. Let \mathfrak{q} be the unique prime ideal of \mathcal{O}_L above p and $\rho \in \mathcal{O}_L$ such that $v_{\mathfrak{q}}(\rho) = 1$. Put $\pi = N_K^L(\rho) \in \mathcal{O}_K$. By Proposition 7.67 $v_{\mathfrak{p}}(\pi) = 1$. Then by Theorem 7.21 $(\mathcal{O}_L)_{\mathfrak{q}} = (\mathcal{O}_K)_{\mathfrak{p}}[\rho]$ and $(\mathcal{O}_K)_{\mathfrak{p}} = \mathbb{Z}_{\{p\}}[\pi]$. So $(\mathcal{O}_L)_{\mathfrak{q}} = \mathbb{Z}_{\{p\}}[\pi, \rho]$. This means that the elements $\pi^i \rho^j$ with $i = 0, \dots, p-1$ and $j = 1, \dots, p-1$ form a $\mathbb{Z}_{\{p\}}$ -basis of $(\mathcal{O}_L)_{\mathfrak{q}}$. From Proposition 7.23 and Theorem 7.25 follows that

$$v_{\mathfrak{p}}(\text{disc}(L)) = v_{\mathfrak{p}}(\text{disc}(\dots, \pi^i \rho^j, \dots)), \quad v_{\mathfrak{p}}(\text{disc}(K)) = v_{\mathfrak{p}}(\text{disc}(1, \pi, \dots, \pi^{p-1}))$$

and $v_{\mathfrak{p}}(\mathfrak{d}_K(L)) = v_{\mathfrak{p}}(\text{disc}_K(1, \rho, \dots, \rho^{p-1}))$.

By Proposition 1.33

$$\text{disc}(\dots, \pi^i \rho^j, \dots) = (\text{disc}(1, \pi, \dots, \pi^{p-1}))^p \cdot N_K^L(\text{disc}_K(1, \rho, \dots, \rho^{p-1})).$$

So

$$\begin{aligned} v_{\mathfrak{p}}(\mathfrak{d}_K(L)) &= v_{\mathfrak{p}}(\text{disc}(1, \rho, \dots, \rho^{p-1})) = v_p(N_K^L(\text{disc}(1, \rho, \dots, \rho^{p-1}))) \\ &= v_p(\text{disc}(\dots, \pi^i \rho^j, \dots)) - p \cdot v_p(\text{disc}(1, \pi, \dots, \pi^{p-1})) \\ &= v_p(\text{disc}(L)) - p \cdot v_p(\text{disc}(K)). \end{aligned} \quad \square$$

9.3 Lemma. *Let p be an odd prime and L an abelian number field of degree p^2 in which p is the only ramifying prime. Then $\text{Gal}(L : \mathbb{Q})$ is cyclic.*

PROOF. The prime p totally ramifies in L , since otherwise there would be an unramified extension of \mathbb{Q} of degree p . Let K be a subfield of degree p of L , \mathfrak{q} the prime ideal of \mathcal{O}_L above p and $\mathfrak{p} = \mathfrak{q} \cap K$. By Lemma 9.1 we have $\text{disc}(K) = p^{2(p-1)}$. Put $N = v_p(\text{disc}(L))$. Then by Lemma 9.2

$$\mathfrak{d}_K(L) = \mathfrak{p}^{N-2p(p-1)}.$$

Let $\rho \in \mathcal{O}_L$ such that $v_{\mathfrak{q}}(\rho) = 1$. Then, since \mathfrak{p} is the only prime ideal of \mathcal{O}_K which ramifies in L , we have $\mathcal{O}_L = \mathcal{O}_K[\rho]$. Let σ be a generator of the group $\text{Gal}(L : K)$ and $t \in \mathbb{N}^*$ such that $V_{K,t}(\mathfrak{q}) = \text{Gal}(L : K)$ and $V_{K,t+1}(\mathfrak{q}) = \{1\}$. For the minimal polynomial f of ρ over K we have

$$f'(\rho) = (\rho - \sigma(\rho))(\rho - \sigma^2(\rho)) \dots (\rho - \sigma^{p-1}(\rho)).$$

Because $V_{K,t}(\mathfrak{q}) \setminus V_{K,t+1}(\mathfrak{q}) = \{\sigma, \sigma^2, \dots, \sigma^{p-1}\}$, we have

$$v_{\mathfrak{p}}(\mathfrak{d}_K(L)) = v_{\mathfrak{p}}(N_K^L(f'(\rho))) = v_{\mathfrak{q}}(f'(\rho)) = (t+1)(p-1).$$

Hence $(t+1)(p-1) = N - 2p(p-1)$. In particular the value of t is the same for all subfields K of degree p . Let $s \in \mathbb{N}^*$ be such that $V_{\mathbb{Q},s}(\mathfrak{q}) = \text{Gal}(L : \mathbb{Q})$ and $V_{\mathbb{Q},s+1}(\mathfrak{q}) \neq \text{Gal}(L : \mathbb{Q})$. Then by Proposition 7.59 $V_{\mathbb{Q},s+1}(\mathfrak{q})$ is of order p . For subfields K of degree p of L we have by Proposition 7.63

$$V_{K,s+1}(\mathfrak{q}) = V_{\mathbb{Q},s+1}(\mathfrak{q}) \cap \text{Gal}(L : K) = \begin{cases} \text{Gal}(L : K) & \text{if } \text{Gal}(L : K) = V_{\mathbb{Q},s+1}(\mathfrak{q}), \\ \{1\} & \text{otherwise.} \end{cases}$$

Since t does not depend on K , there is only one such subfield. This means that $\text{Gal}(L : \mathbb{Q})$ has a unique subgroup of order p . \square

9.4 Lemma. *Let p be an odd prime. The subfield K of $\mathbb{Q}(\zeta_{p^2})$ of degree p is the unique abelian number field of degree p in which p is the only prime that ramifies.*

PROOF. Suppose there is another abelian number field L of degree p in which p is the only prime that ramifies. Then KL is a noncyclic abelian number field of degree p^2 and by Theorem 7.50 only the prime p ramifies in KL . This contradicts Lemma 9.3. \square

9.5 Proposition. *Let p be an odd prime and $r \in \mathbb{N}^*$. The subfield K of $\mathbb{Q}(\zeta_{p^{r+1}})$ of degree p^r is the unique abelian number field of degree p^r in which p is the only prime that ramifies.*

PROOF. Let L be another abelian number field of degree p^r in which only p ramifies. Then $\text{Gal}(KL : \mathbb{Q})$ is a noncyclic abelian p -group of order $> p^r$. By Theorem 7.50 only the prime p ramifies in KL . For H a subgroup of $\text{Gal}(KL : \mathbb{Q})$ of index p , the field $(KL)^H$ is an abelian number field of degree p in which p is the only prime that ramifies. By Lemma 9.4 the subgroup H is the unique subgroup of index p . It follows that $\text{Gal}(KL : \mathbb{Q})$ is cyclic. Contradiction. \square

9.6 Lemma. *The only quadratic number fields in which only the prime 2 ramifies are $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-2})$.*

PROOF. These are the only quadratic number fields having a discriminant without odd prime divisors. \square

9.7 Proposition. *Let $r \in \mathbb{N}^*$. The field $K = \mathbb{Q}(\zeta_{2^{r+2}} + \zeta_{2^{r+2}}^{-1})$ is the unique real abelian number field of degree 2^r in which 2 is the only prime that ramifies.*

PROOF. Let L be another real abelian number field of degree 2^r in which only 2 ramifies. Then $\text{Gal}(KL : \mathbb{Q})$ is a noncyclic abelian 2-group of order $> 2^r$. By Theorem 7.50 only the prime 2 ramifies in KL . For H a subgroup of $\text{Gal}(KL : \mathbb{Q})$ of index 2, the field $(KL)^H$ is a real quadratic number field in which 2 is the only prime that ramifies. This is the field $\mathbb{Q}(\sqrt{2})$. So $\text{Gal}(KL : \mathbb{Q})$ has a unique subgroup of index 2. Therefore, $\text{Gal}(KL : \mathbb{Q})$ is cyclic. Contradiction. \square

9.8 Proposition. *Let $r \in \mathbb{N}^*$. The only complex abelian number fields of degree 2^r in which only the prime 2 ramifies are*

$$\mathbb{Q}(\zeta_{2^{r+1}}) \quad \text{and} \quad \mathbb{Q}(\zeta_{2^{r+2}} - \zeta_{2^{r+2}}^{-1}).$$

PROOF. Let K be a complex abelian number field of degree 2^r in which only the prime 2 ramifies. Let τ be complex conjugation. If $i \in K$, then by Proposition 9.7

$$K = K^\tau(i) = \mathbb{Q}(\zeta_{2^{r+1}} + \zeta_{2^{r+1}}^{-1})(i) = \mathbb{Q}(\zeta_{2^{r+1}}).$$

If $i \notin K$, then apply this to $K(i)$:

$$K(i) = \mathbb{Q}(\zeta_{2^{r+2}}).$$

The subfield fixed under the automorphism given by $\zeta_{2^{r+2}} \mapsto -\zeta_{2^{r+2}}^{-1}$:

$$K = \mathbb{Q}(\zeta_{2^{r+2}} - \zeta_{2^{r+2}}^{-1}). \quad \square$$

We have determined all abelian number fields of prime power degree in which this prime is the only ramifying prime. In particular they are subfields of cyclotomic fields. Now we consider a more general case.

9.9 Proposition. *Let p be a prime. Let K be an abelian number field such that $\text{Gal}(K : \mathbb{Q})$ is a p -group. Then K is contained in a cyclotomic field.*

PROOF. The proof will be by induction on the number of primes $\neq p$ which ramify in K . If this number is 0, we know by the Propositions 9.5 and 9.8 that K is contained in a cyclotomic field.

Put $[K : \mathbb{Q}] = p^r$. Suppose q is a prime $\neq p$ which ramifies in K . Let $\mathfrak{q} \in \text{Max}(\mathcal{O}_K)$ be above q and consider the ramification group $V_1 = V_1(\mathfrak{q})$ of \mathfrak{q} over \mathbb{Q} . By Theorem 7.61 V_1 is a q -group. Because V_1 is a subgroup of the p -group $\text{Gal}(K : \mathbb{Q})$, we have $V_1 = \{1\}$, that is q tamely ramifies in K . Now consider the inertia group $T = T_{\mathbb{Q}}(\mathfrak{q})$. Being a subgroup of $\text{Gal}(K : \mathbb{Q})$ it is a p -group, say $\#(T) = p^t$, where $t \leq r$. By Proposition 7.60 $p^t \mid q - 1$. Let L be the unique subfield of $\mathbb{Q}(\zeta_q)$ of degree p^t . The prime q totally ramifies in L , because it does so in $\mathbb{Q}(\zeta_q)$. Since q is the only prime which ramifies in $\mathbb{Q}(\zeta_q)$, it also is the only one which ramifies in L .

Consider the abelian number field KL and let $\mathfrak{q}'' \in \text{Max}(\mathcal{O}_{KL})$ be above \mathfrak{q} . Because $[KL : \mathbb{Q}]$ is a power of p , again we have $V_1(\mathfrak{q}'') = \{1\}$. So $T'' = T_{\mathbb{Q}}(\mathfrak{q}'')$ is a cyclic p -group. The restriction to T'' of the injective group homomorphism

$$\text{Gal}(KL : \mathbb{Q}) \rightarrow \text{Gal}(K : \mathbb{Q}) \times \text{Gal}(L : \mathbb{Q}), \quad \sigma \mapsto (\sigma|_K, \sigma|_L)$$

yields an injective group homomorphism

$$T'' \rightarrow T \times \text{Gal}(L : \mathbb{Q}).$$

The group on the right hand side is isomorphic to $C_{p^t} \times C_{p^t}$. The order of T'' is a multiple of p^t , the order of the inertia group of q in L . It follows that T'' is cyclic of order p^t .

By Theorem 7.50 the primes which ramify in KL are the same as those which ramify in K . Now consider the field

$$K' = (KL)^{T''}.$$

Prime numbers which ramify in K' also ramify in KL . However, q does not ramify in K' . Hence the number of primes ramifying in K' is less than the number of primes ramifying in K . So we can assume that K' is contained in a cyclotomic field, say $K' \subseteq \mathbb{Q}(\zeta_m)$. We have: q does not ramify in $K' \cap L$ (it does not in K') and q totally ramifies in $K' \cap L$ (it does in L). It follows that $K' \cap L = \mathbb{Q}$ and therefore,

$$[K'L : \mathbb{Q}] = [K' : \mathbb{Q}][L : \mathbb{Q}] = [K' : \mathbb{Q}][KL : K'] = [KL : \mathbb{Q}].$$

So $K'L = KL$, because $K' \subseteq KL$ and $L \subseteq KL$. Hence

$$K \subseteq KL = K'L \subseteq \mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_q) = \mathbb{Q}(\zeta_{m'})$$

with $m' = \text{lcm}(m, q)$. □

Finally we have:

9.10 Theorem (Kronecker-Weber). *Let K be an abelian number field. Then K is contained in a cyclotomic field.*

PROOF. The Galois group G is a direct product of p -groups, say

$$G = G_1 \cdots G_r,$$

where G_i is say a Sylow p_i -subgroup. Put $H_i = G_1 \cdots G_{i-1}G_{i+1} \cdots G_r$. Then

$$K = K^{(1)} = K \cap H_i = K^{H_1} \cdots K^{H_r}$$

and we have

$$\text{Gal}(K^{H_i} : \mathbb{Q}) \cong G/H_i \cong G_i.$$

By Proposition 9.9 each of the K^{H_i} is contained in a cyclotomic field and so the same holds for their composite K . □

The intersection of cyclotomic fields is a cyclotomic field as well: $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_d)$, where $d = \text{gcd}(m, n)$. So for an abelian number field K there is a least m such that K is contained in $\mathbb{Q}(\zeta_m)$. This justifies the following definition.

9.11 Definition. Let K be an abelian number field. The least $m \in \mathbb{N}^*$ for which $K \subseteq \mathbb{Q}(\zeta_m)$ is called the *conductor* of K . The conductor of K is denoted by N_K .

For a conductor N of an abelian number field we have $N \not\equiv 2 \pmod{4}$, because for $N \equiv 2 \pmod{4}$ we have $\mathbb{Q}(\zeta_{N/2}) = \mathbb{Q}(\zeta_N)$.

Composition and intersection of cyclotomic fields yield cyclotomic fields, i.e. for $m, n \in \mathbb{N}^*$, $d = \text{gcd}(m, n)$ and $k = \text{lcm}(m, n)$:

$$\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_k) \quad \text{and} \quad \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_d).$$

This implies:

9.12 Proposition. *Let K_1 and K_2 be abelian number fields. Then*

$$N_{K_1 K_2} = \text{lcm}(N_{K_1}, N_{K_2}) \quad \text{and} \quad N_{K_1 \cap K_2} = \text{gcd}(N_{K_1}, N_{K_2}). \quad \square$$

For quadratic number fields we have:

9.13 Proposition. *For $m \in \mathbb{Z}$ squarefree $\neq 1$ the conductor of $\mathbb{Q}(\sqrt{m})$ is $|D_m|$.*

PROOF. Write $m = up_1^* \cdots p_r^*$, where $u \in \{\pm 1, \pm 2\}$ and p_1, \dots, p_r are different odd primes. The conductor of $\mathbb{Q}(\sqrt{n})$ for $n = -1, 2, -2, p_i^*$ is respectively 4, 8, 8 and p . It follows that $\mathbb{Q}(\sqrt{m}) \subseteq \mathbb{Q}(\zeta_N)$, where $N = |D_m|$. Because all prime divisors of D_m ramify in $\mathbb{Q}(\sqrt{m})$, this field is not contained in a smaller cyclotomic field. □

9.2 Characters of finite abelian groups

In the next section Dirichlet characters are introduced. They describe the splitting behavior of primes in abelian number fields and are essentially characters of a group $(\mathbb{Z}/N)^*$ for some $N \in \mathbb{N}^*$. We will need some generalities on characters of groups, in particular characters of finite abelian groups.

9.14 Definition. Let G be an abelian group. A *character* χ of G is a group homomorphism $\chi: G \rightarrow \mathbb{C}^*$. The character $\varepsilon: G \rightarrow \mathbb{C}^*$ defined by $\varepsilon(g) = 1$ for all $g \in G$ is called the *trivial* or *principal character* on G .

If G is a torsion group, which means that each element of G is of finite order, then $\chi(G) \subseteq \mu(\mathbb{C}) \cong \mathbb{Q}/\mathbb{Z}$ for each character χ of G . So for such groups, e.g. finite abelian groups, we could take characters to be homomorphisms of G to \mathbb{Q}/\mathbb{Z} .

9.15 Definition. Let χ_1 and χ_2 be characters of a group G . Then their *product* $\chi_1\chi_2$ is defined by:

$$(\chi_1\chi_2)(g) = \chi_1(g)\chi_2(g) \quad \text{for all } g \in G.$$

Clearly this imposes an abelian group structure on the set of characters of G . This group we denote by G^\vee and is called the *character group* of G or also the *dual* of G . The trivial character ε is the unit element of G^\vee .

9.16 Definition. Let $f: G_1 \rightarrow G_2$ be a homomorphism of groups. The group homomorphism

$$f^\vee: G_2^\vee \rightarrow G_1^\vee, \quad \chi \mapsto \chi f$$

is called the *dual* of f .

One easily verifies that $1_{G^\vee} = 1_{G^\vee}$ and $(gf)^\vee = f^\vee g^\vee$. Thus $G \mapsto G^\vee$ is a contravariant functor from the category of groups to the category of abelian groups.

For any abelian group C we have a contravariant functor $\text{Hom}_{\mathbb{Z}}(-, C)$ from the category of abelian groups (= \mathbb{Z} -modules) to itself. Such a functor is *left exact*, which means that it maps a short exact sequence $0 \rightarrow A' \rightarrow A \rightarrow A'' \rightarrow 0$ to an exact sequence $0 \rightarrow \text{Hom}_{\mathbb{Z}}(A'', C) \rightarrow \text{Hom}_{\mathbb{Z}}(A, C) \rightarrow \text{Hom}_{\mathbb{Z}}(A', C)$. If it maps short exact sequences to short exact sequences the functor is said to be *exact* and the group C is then by definition an *injective* \mathbb{Z} -module. Injective \mathbb{Z} -modules are just the *divisible* abelian groups: abelian groups C with the property that for each $x \in C$ and each $n \in \mathbb{N}^*$ there is a $y \in C$ such that $ny = x$. Note that in the multiplicative notation this reads: $y^n = x$.

9.17 Proposition. Let $1 \rightarrow A' \rightarrow A \rightarrow A'' \rightarrow 1$ be a short exact sequence of abelian groups (in the multiplicative notation). Then the induced sequence of the duals $1 \rightarrow A''^\vee \rightarrow A^\vee \rightarrow A'^\vee \rightarrow 1$ is exact as well.

PROOF. $A^\vee = \text{Hom}_{\mathbb{Z}}(A, \mathbb{C}^*)$ and the group \mathbb{C}^* is divisible. □

9.18 Corollary. *Let A_1 and A_2 be abelian groups. Then $(A_1 \times A_2)^\vee \cong A_1^\vee \times A_2^\vee$.*

PROOF. Apply Proposition 9.17 to the split short exact sequence $1 \rightarrow A_1 \rightarrow A_1 \times A_2 \rightarrow A_2 \rightarrow 1$. \square

9.19 Proposition. *Let C_n be a cyclic group of order $n \in \mathbb{N}^*$. Then C_n^\vee is also cyclic of order n .*

PROOF. Let t be a generator of C_n . For each character χ of C_n , $\chi(t)$ is an n -th root of unity. The homomorphism $\chi \mapsto \chi(t)$ of C_n^\vee to the cyclic group μ_n of n -th roots of unity is an isomorphism. (A generator of the dual group is the character which maps t to ζ_n .) \square

9.20 Theorem. *Let A be a finite abelian group. Then $A^\vee \cong A$.*

PROOF. A finite abelian group is a product of cyclic groups. So the theorem is a consequence of Corollary 9.18 and Proposition 9.19. \square

The theorem merely states that an isomorphism exists. It depends on the factorization of the group as a product of cyclic groups and the isomorphisms from these cyclic groups to their duals. There is however a natural isomorphism from A to $A^{\vee\vee}$: $a \mapsto (\chi \mapsto \chi(a))$.

The finiteness of A is crucial:

$$\mathbb{Z}^\vee = \text{Hom}(\mathbb{Z}, \mathbb{C}^*) \cong \mathbb{C}^*,$$

and

$$\left(\bigoplus_{n=1}^{\infty} \mathbb{Z}/2\right)^\vee \cong \text{Hom}\left(\bigoplus_{n=1}^{\infty} \mathbb{Z}/2, \mathbb{Q}/\mathbb{Z}\right) \cong \prod_{n=1}^{\infty} \text{Hom}(\mathbb{Z}/2, \mathbb{Q}/\mathbb{Z}) \cong \prod_{n=1}^{\infty} \mathbb{Z}/2.$$

($\prod_{n=1}^{\infty} A_n$ consists of sequences (a_1, a_2, \dots) with $a_n \in A_n$ for all $n \in \mathbb{N}^*$, whereas $\bigoplus_{n=1}^{\infty} A_n$ consists of such sequences which satisfy an extra condition: $a_n \neq 0$ only for finitely many $n \in \mathbb{N}^*$.)

In the next section we will need the following propositions:

9.21 Proposition. *Let $p: A \rightarrow B$ be a surjective homomorphism of abelian groups. Then its dual $p^\vee: B^\vee \rightarrow A^\vee$ is injective and*

$$p^\vee(B^\vee) = \{\chi \in A^\vee \mid \text{Ker}(p) \subseteq \text{Ker}(\chi)\}.$$

PROOF. The dual of the short exact sequence

$$1 \longrightarrow \text{Ker}(p) \xrightarrow{i} A \xrightarrow{p} B \longrightarrow 1$$

is the short exact sequence

$$1 \longrightarrow B^\vee \xrightarrow{p^\vee} A^\vee \xrightarrow{i^\vee} \text{Ker}(p)^\vee \longrightarrow 1.$$

We have

$$\begin{aligned} p^\vee(B^\vee) &= \text{Ker}(i^\vee) = \{ \chi \in A^\vee \mid \chi i = \varepsilon \} \\ &= \{ \chi \in A^\vee \mid \chi(\text{Ker}(p)) = \{ \varepsilon \} \} = \{ \chi \in A^\vee \mid \text{Ker}(p) \subseteq \text{Ker}(\chi) \}. \quad \square \end{aligned}$$

A commutative diagram

$$\begin{array}{ccc} C & \xrightarrow{f_2} & A_2 \\ f_1 \downarrow & & \downarrow g_2 \\ A_1 & \xrightarrow{g_1} & B \end{array}$$

of homomorphisms of abelian groups is called a *cartesian square* if for each pair $h_1: X \rightarrow A_1, h_2: X \rightarrow A_2$ of homomorphisms of abelian groups such that $g_1 h_1 = g_2 h_2$, there exists a unique $h: X \rightarrow C$ such that $f_1 h = h_1$ and $f_2 h = h_2$. This comes down to: for each $(a_1, a_2) \in A_1 \times A_2$ such that $g_1(a_1) = g_2(a_2)$, there is a unique $c \in C$ such that $f_1(c) = a_1$ and $f_2(c) = a_2$. The square is cartesian if and only if the following sequence is exact:

$$0 \longrightarrow C \xrightarrow{\begin{pmatrix} f_1 \\ f_2 \end{pmatrix}} A_1 \oplus A_2 \xrightarrow{(g_1 \ -g_2)} B.$$

Dually, in the categorical sense, the square is called *cocartesian* if for each pair $k_1: A_1 \rightarrow Y, k_2: A_2 \rightarrow Y$ of homomorphisms of abelian groups such that $k_1 f_1 = k_2 f_2$ there exists a unique $k: B \rightarrow Y$ such that $k g_1 = k_1$ and $k g_2 = k_2$. The square is cocartesian if and only if the following sequence is exact:

$$C \xrightarrow{\begin{pmatrix} f_1 \\ f_2 \end{pmatrix}} A_1 \oplus A_2 \xrightarrow{(g_1 \ -g_2)} B \longrightarrow 0.$$

The square is called *bicartesian* if it is both cartesian and cocartesian. It follows that the square is bicartesian if and only if the sequence

$$0 \longrightarrow C \xrightarrow{\begin{pmatrix} f_1 \\ f_2 \end{pmatrix}} A_1 \oplus A_2 \xrightarrow{(g_1 \ -g_2)} B \longrightarrow 0$$

is a short exact sequence.

9.22 Proposition. *The dual of a bicartesian square of abelian groups is bicartesian.*

PROOF. According to Proposition 9.17 the dual of a short exact sequence is a short exact sequence. \square

9.3 Dirichlet characters

Dirichlet characters are essentially characters of groups $(\mathbb{Z}/N)^*$. In the next section it is shown that they describe the splitting behavior of primes in abelian number fields.

Let $N \in \mathbb{N}^*$. A character χ' of $(\mathbb{Z}/N)^*$ induces a map $\chi: \mathbb{Z} \rightarrow \mathbb{C}$ as follows:

$$\chi(n) = \begin{cases} \chi'(\bar{n}) & \text{if } \gcd(n, N) = 1, \\ 0 & \text{if } \gcd(n, N) > 1. \end{cases}$$

As is easily verified the map χ satisfies for all $m, n \in \mathbb{Z}$:

$$(D1) \quad \chi(n) = 0 \iff \gcd(n, N) > 1,$$

$$(D2) \quad \chi(mn) = \chi(m)\chi(n),$$

$$(D3) \quad m \equiv n \pmod{N} \implies \chi(m) = \chi(n).$$

9.23 Definitions and notation. Let $N \in \mathbb{N}^*$. A map $\chi: \mathbb{Z} \rightarrow \mathbb{C}$ satisfying (D1), (D2) and (D3) above is called a *Dirichlet character modulo N* . The N is called the *modulus* of the Dirichlet character. If χ_1 and χ_2 both are Dirichlet characters modulo N , then so is $\chi_1\chi_2$, the map defined by

$$(\chi_1\chi_2)(n) = \chi_1(n)\chi_2(n) \quad \text{for all } n \in \mathbb{Z},$$

The set of Dirichlet characters modulo N will be denoted by \mathcal{D}_N . Under the multiplication given above it is a group naturally isomorphic to $(\mathbb{Z}/N)^{* \vee}$. Dirichlet characters of order 2 are called *quadratic*. Only 0, 1 and -1 are values of a quadratic Dirichlet character.

Since $\mathcal{D}_N \xrightarrow{\sim} (\mathbb{Z}/N)^{* \vee} \cong (\mathbb{Z}/N)^*$, we have in particular $\#(\mathcal{D}_N) = \varphi(N)$.

If χ is a Dirichlet character modulo N , then its inverse χ^{-1} is given by

$$\chi^{-1}(n) = \begin{cases} \chi(n)^{-1} & \text{if } \gcd(n, N) = 1 \\ 0 & \text{if } \gcd(n, N) > 1. \end{cases}$$

So $\chi^{-1}(n) = \overline{\chi(n)}$ for all $n \in \mathbb{N}$. For this reason the inverse of a Dirichlet character χ is usually denoted by $\bar{\chi}$.

9.24 Example. Let p be an odd prime. The Legendre symbol determines a character of the group \mathbb{F}_p^* :

$$\mathbb{F}_p^* \rightarrow \mathbb{C}^*, \quad \bar{n} \mapsto \left(\frac{n}{p}\right).$$

It corresponds to a quadratic Dirichlet character

$$\mathbb{Z} \rightarrow \mathbb{C}, \quad n \mapsto \left(\frac{n}{p}\right).$$

Since all Dirichlet characters have the same domain and the same codomain, they can be multiplied, even if their moduli differ, and the result is again a Dirichlet character:

9.25 Definition. Let $\chi_1 \in \mathcal{D}_{N_1}$ and $\chi_2 \in \mathcal{D}_{N_2}$. We define $\chi_1\chi_2: \mathbb{Z} \rightarrow \mathbb{C}$ by

$$(\chi_1\chi_2)(n) = \chi_1(n)\chi_2(n)$$

for all $n \in \mathbb{Z}$. Clearly $\chi_1\chi_2 \in \mathcal{D}_{\text{lcm}(N_1, N_2)}$.

Let $N \in \mathbb{N}^*$ and $M \in \mathbb{N}^*$ be such that $M \mid N$. The canonical surjective ring homomorphism $\mathbb{Z}/N \rightarrow \mathbb{Z}/M$ induces a surjective group homomorphism $(\mathbb{Z}/N)^* \rightarrow (\mathbb{Z}/M)^*$ and so also an injective group homomorphism $(\mathbb{Z}/M)^{* \vee} \rightarrow (\mathbb{Z}/N)^{* \vee}$, which in turn induces an injective group homomorphism $i_N^M: \mathcal{D}_M \rightarrow \mathcal{D}_N$. For $\chi \in \mathcal{D}_M$ the Dirichlet character $i_N^M(\chi)$ is then given by

$$(i_N^M(\chi))(n) = \begin{cases} \chi(n) & \text{for all } n \in \mathbb{Z} \text{ with } \gcd(n, N) = 1, \\ 0 & \text{for all } n \in \mathbb{Z} \text{ with } \gcd(n, N) > 1. \end{cases}$$

Note that the surjectivity of $(\mathbb{Z}/N)^* \rightarrow (\mathbb{Z}/M)^*$ follows from the Chinese Remainder Theorem: given an $n \in \mathbb{Z}$ with $\gcd(n, M) = 1$, there exists an $n' \in \mathbb{Z}$ such that

$$n' \equiv \begin{cases} n \pmod{M} \\ 1 \pmod{p^{v_p(N)}} \end{cases} \text{ for all primes } p \text{ with } p \mid N \text{ and } p \nmid M.$$

For this n' we have $\gcd(n', N) = 1$ and $n' \equiv n \pmod{M}$.

9.26 Definition. Let $M, N \in \mathbb{N}^*$ such that $M \mid N$ and let $\chi \in \mathcal{D}_M$. Then the Dirichlet character $i_N^M(\chi) \in \mathcal{D}_N$ is said to be *induced* by χ . A Dirichlet character modulo N is said to be a *primitive* Dirichlet character modulo N if it is not induced by a Dirichlet character modulo M with M a proper divisor of N .

9.27 Examples.

1. For each $N \in \mathbb{N}^*$ there is the *trivial* or *principal Dirichlet character* χ_1 ; it is the unit element of the group \mathcal{D}_N :

$$\chi_1(n) = \begin{cases} 1 & \text{if } \gcd(n, N) = 1, \\ 0 & \text{if } \gcd(n, N) > 1. \end{cases}$$

Only for $N = 1$ it is primitive.

2. For $N = 3, 4, 6$ the group \mathcal{D}_N is of order 2. It contains one quadratic character.

For $N = 3$:

$$n \mapsto \begin{cases} 1 & \text{if } n \equiv 1 \pmod{3}, \\ -1 & \text{if } n \equiv 2 \pmod{3}, \\ 0 & \text{if } n \equiv 0 \pmod{3}. \end{cases}$$

For $N = 4$:

$$n \mapsto \begin{cases} 1 & \text{if } n \equiv 1 \pmod{4}, \\ -1 & \text{if } n \equiv 3 \pmod{4}, \\ 0 & \text{if } n \equiv 0 \pmod{2}. \end{cases}$$

For $N = 6$:

$$n \mapsto \begin{cases} 1 & \text{if } n \equiv 1 \pmod{6}, \\ -1 & \text{if } n \equiv 5 \pmod{6}, \\ 0 & \text{if } n \equiv 0, 2, 3, 4 \pmod{6}. \end{cases}$$

The first two are primitive; the last one is not: it is induced by the first.

3. For p a prime there are $p - 1$ Dirichlet characters modulo p and $p - 2$ of them are primitive. The group \mathcal{D}_p is cyclic of order $p - 1$. For p odd there is a unique quadratic Dirichlet character modulo p : the character given by the Legendre symbol, see Example 9.24.

9.28 Lemma. *Let $M_1, M_2, N \in \mathbb{N}^*$ be such that $M_1, M_2 \mid N$. Let $\chi \in \mathcal{D}_N$ be induced by a Dirichlet character modulo M_1 as well as by a Dirichlet character modulo M_2 . Then χ is induced by a Dirichlet character modulo M , where $M = \gcd(M_1, M_2)$.*

PROOF. We can assume that $N = \text{lcm}(M_1, M_2)$. From $(M_1) \cap (M_2) = (N)$ and $(M_1) + (M_2) = (M)$ it follows that the square

$$\begin{array}{ccc} \mathbb{Z}/N & \longrightarrow & \mathbb{Z}/M_2 \\ \downarrow & & \downarrow \\ \mathbb{Z}/M_1 & \longrightarrow & \mathbb{Z}/M \end{array}$$

is a bicartesian square of surjective ring homomorphisms. Taking units yields a bicartesian square

$$\begin{array}{ccc} (\mathbb{Z}/N)^* & \longrightarrow & (\mathbb{Z}/M_2)^* \\ \downarrow & & \downarrow \\ (\mathbb{Z}/M_1)^* & \longrightarrow & (\mathbb{Z}/M)^* \end{array}$$

of surjective group homomorphisms. By Proposition 9.21 the dual square is bicartesian. In the dual square the group homomorphisms are injective. It is canonically isomorphic to the square

$$\begin{array}{ccc}
 \mathcal{D}_M & \longrightarrow & \mathcal{D}_{M_2} \\
 \downarrow & & \downarrow \\
 \mathcal{D}_{M_1} & \longrightarrow & \mathcal{D}_N
 \end{array}$$

Because the homomorphisms are injective, we have

$$i_N^{M_1}(\mathcal{D}_{M_1}) \cap i_N^{M_2}(\mathcal{D}_{M_2}) = i_N^M(\mathcal{D}_M). \tag{9.2}$$

Since both $\chi \in i_N^{M_1}(\mathcal{D}_{M_1})$ and $\chi \in i_N^{M_2}(\mathcal{D}_{M_2})$, it follows that $\chi \in i_N^M(\mathcal{D}_M)$, which means that χ is induced by a Dirichlet character modulo M . \square

An important consequence is:

9.29 Corollary. *Let χ be a Dirichlet character modulo N . Then there is a unique $M \mid N$ such that χ is induced by a primitive Dirichlet character modulo M .* \square

9.30 Definition. Let χ be a Dirichlet character modulo N . The modulus of the unique primitive Dirichlet character which induces χ is called the *conductor* of χ . Notation: N_χ .

Induction of Dirichlet characters generates an equivalence relation: Dirichlet characters being equivalent if there is a Dirichlet character that induces both of them. The product of Dirichlet characters induces a product of equivalence classes. Each equivalence class contains a unique primitive Dirichlet character. Thus the product of equivalence classes induces a product of the representing primitive Dirichlet characters.

9.31 Definition and notation. The set of all primitive Dirichlet characters is denoted by \mathcal{D} . It is a group under the following multiplication. Let χ_1 and χ_2 be primitive Dirichlet characters. Then the product $\chi_1\chi_2$ as in Definition 9.25 is a Dirichlet character modulo $\text{lcm}(N_{\chi_1}, N_{\chi_2})$. The product of χ_1 and χ_2 in \mathcal{D} is the unique primitive Dirichlet character by which it is induced.

9.32 Change of notation. Henceforth all Dirichlet characters are assumed to be primitive. The notation \mathcal{D}_N will now be used for the subgroup of \mathcal{D} of all Dirichlet characters χ with $N_\chi \mid N$. That means that in \mathcal{D}_N as originally defined all characters are replaced by primitive characters and that the multiplication is changed accordingly. Under this convention identity 9.2 in the proof of Lemma 9.28 becomes

$$\mathcal{D}_{\text{gcd}(M_1, M_2)} = \mathcal{D}_{M_1} \cap \mathcal{D}_{M_2}.$$

Dirichlet characters as originally defined will be referred to as *Dirichlet pre-characters*.

Now the notion of conductor reads: the conductor N_χ of $\chi \in \mathcal{D}$ is the least $N \in \mathbb{N}^*$ for which $\chi \in \mathcal{D}_N$. More generally we define:

9.33 Definition. Let X be a finite group of Dirichlet characters. Then the *conductor* of X is the least N such that $X \subseteq \mathcal{D}_N$. Notation N_X .

9.4 Classification of abelian number fields

The splitting behavior of a nonramifying prime number in an abelian number field is given by its Frobenius automorphism. The ramifying primes in a cyclotomic field $\mathbb{Q}(\zeta_m)$ with $m \not\equiv 2 \pmod{4}$ are the prime divisors of m . The Frobenius automorphism of a prime $p \nmid m$ is the automorphism given by $\zeta_m \mapsto \zeta_m^p$. So the splitting behavior of such p depends only on its residue class modulo m . Since an abelian number field K is a subfield of a cyclotomic field $\mathbb{Q}(\zeta_m)$ and the Frobenius automorphism of p in $\text{Gal}(K : \mathbb{Q})$ is the restriction of its Frobenius automorphism in $\text{Gal}(\mathbb{Q}(\zeta_m) : \mathbb{Q})$, we have the same regularity for the splitting behavior in K .

There is a one-to-one correspondence between abelian number fields and finite groups of Dirichlet characters. This correspondence is as follows. For a fixed $N \in \mathbb{N}^*$ it is a correspondence between subfields of $\mathbb{Q}(\zeta_N)$ and subgroups of \mathcal{D}_N . Up to natural isomorphisms it comes from the correspondence between subgroups of $G_N := \text{Gal}(\mathbb{Q}(\zeta_N) : \mathbb{Q})$ and the duals of their factor groups. The last ones are naturally isomorphic to subgroups of \mathcal{D}_N . For X a finite subgroup of \mathcal{D}_N define

$$\text{Ker}(X) = \{ \sigma \in G_N \mid \chi(\sigma) = 1 \text{ for all } \chi \in X \}.$$

Note that $\chi \in \mathcal{D}_N$ determines a character on G_N via the isomorphism $(\mathbb{Z}/N)^* \xrightarrow{\sim} G_N$, $\bar{a} \mapsto \sigma_a$, σ_a being the automorphism given by $\zeta_N \mapsto \zeta_N^a$. For H a subgroup of G_N define

$$\text{Dir}(H) = \{ \chi \in \mathcal{D}_N \mid \chi(\sigma) = 1 \text{ for all } \sigma \in H \}.$$

Thus we have short exact sequences

$$1 \longrightarrow \text{Ker}(X) \longrightarrow G_N \longrightarrow X^\vee \longrightarrow 1$$

and

$$1 \longrightarrow \text{Dir}(H) \longrightarrow \mathcal{D}_N \longrightarrow H^\vee \longrightarrow 1.$$

Taking duals yields

$$\text{Dir}(\text{Ker}(X)) = X \quad \text{and} \quad \text{Ker}(\text{Dir}(H)) = H.$$

9.34 Definitions.

- a) Let K be an abelian number field and $N \in \mathbb{N}^*$ such that $K \subseteq \mathbb{Q}(\zeta_N)$. The *group of Dirichlet characters associated to K* is the group

$$\mathcal{D}(K) := \text{Dir}(\text{Gal}(\mathbb{Q}(\zeta_N) : K)).$$

(Note that this group does not depend on the choice of N .)

- b) Let X be a finite subgroup of \mathcal{D} and N such that $X \subseteq \mathcal{D}_N$. The *abelian number field associated to X* is the field

$$\mathbb{Q}_X := \mathbb{Q}(\zeta_N)^{\text{Ker}(X)}.$$

(This field does not depend on the choice of N .)

Now we have a one-to-one correspondence between abelian number fields and finite groups of Dirichlet characters:

9.35 Classification Theorem for Abelian Number Fields. *The maps*

$$\begin{array}{ccc} \begin{array}{c} \text{abelian} \\ \text{number fields} \end{array} & \longleftrightarrow & \begin{array}{c} \text{finite groups of} \\ \text{Dirichlet characters} \end{array} \\ K & \longmapsto & \mathcal{D}(K) \\ \mathbb{Q}_X & \longleftarrow & X \end{array}$$

are inverses of each other and they preserve the ordering given by inclusion. □

This implies:

9.36 Proposition.

- (i) Let K_1 and K_2 be abelian number fields. Then $\mathcal{D}(K_1 K_2) = \mathcal{D}(K_1) \mathcal{D}(K_2)$ and $\mathcal{D}(K_1 \cap K_2) = \mathcal{D}(K_1) \cap \mathcal{D}(K_2)$.
- (ii) Let X_1 and X_2 be finite groups of Dirichlet characters. Then $\mathbb{Q}_{X_1 X_2} = \mathbb{Q}_{X_1} \mathbb{Q}_{X_2}$ and $\mathbb{Q}_{X_1 \cap X_2} = \mathbb{Q}_{X_1} \cap \mathbb{Q}_{X_2}$.
- (iii) The conductor of an abelian number field K is equal to the conductor of $\mathcal{D}(K)$. □

9.37 Definition. A Dirichlet character χ is called *even* if $\chi(-1) = 1$. Otherwise, so if $\chi(-1) = -1$, it is called *odd*.

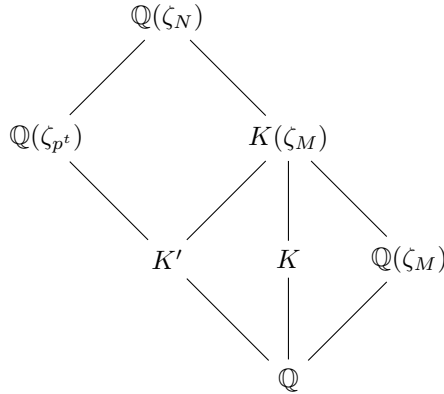
9.38 Proposition. An abelian number field is real if and only if the corresponding group of Dirichlet characters contains only even characters.

PROOF. Let the abelian number field K be contained in a cyclotomic field $\mathbb{Q}(\zeta_N)$. Then K is real if and only if $K \subseteq \mathbb{Q}(\zeta_N + \zeta_N^{-1})$, which is the case if and only if $\sigma_{-1} \in \text{Gal}(\mathbb{Q}(\zeta_N) : K)$. This is equivalent to $\chi(-1) = 1$ for all $\chi \in \mathcal{D}(K)$. \square

The group $\mathcal{D}(K)$ is isomorphic to the dual of $\text{Gal}(K : \mathbb{Q})$. It describes the splitting of primes in the field K .

9.39 Proposition. *Let K be an abelian number field and let p be a prime. Then p ramifies in K if and only if there is a $\chi \in \mathcal{D}(K)$ with $\chi(p) = 0$.*

PROOF. Let $N \in \mathbb{N}^*$ be such that $K \subseteq \mathbb{Q}(\zeta_N)$. Write $N = p^t M$ with $p \nmid M$. Consider the following diagram, where $K' = \mathbb{Q}(\zeta_{p^t}) \cap K(\zeta_M)$.



Since $\mathbb{Q}(\zeta_{p^t}) \cap \mathbb{Q}(\zeta_M) = \mathbb{Q}$, it follows that $K'(\zeta_M) = K(\zeta_M)$. Therefore, the extensions $K(\zeta_M) : K$ and $K(\zeta_M) : K'$ are both extensions with an M -th root of unity. So the primes above p in K and K' do not ramify in $K(\zeta_M)$. It follows that

$$e_p^K = e_p^{K(\zeta_M)} = e_p^{K'} = [K' : \mathbb{Q}].$$

So p ramifies in K if and only if $K' \neq \mathbb{Q}$. Since $\chi(p) = 0$ if and only if $\chi \neq \varepsilon$ for all $\chi \in \mathcal{D}_{p^t}$, we have that $K' \neq \mathbb{Q}$ if and only if there is a $\chi \in \mathcal{D}(K')$ with $\chi(p) = 0$. From $K'(\zeta_M) = K(\zeta_M)$ it also follows that $\mathcal{D}(K) \mathcal{D}_M = \mathcal{D}(K') \mathcal{D}_M$. Since $\chi(p) \neq 0$ for all $\chi \in \mathcal{D}_M$, there is a $\chi \in \mathcal{D}(K)$ with $\chi(p) = 0$ if and only if there is a $\chi \in \mathcal{D}(K')$ with $\chi(p) = 0$. \square

9.40 Theorem. *Let K be an abelian number field and let p be a prime. Put $Z = Z_p^{(K)}$ and $T = T_p^{(K)}$. Then*

- (i) K^T is associated to the group $Y = \{\chi \in \mathcal{D}(K) \mid \chi(p) \neq 0\}$;
- (ii) K^Z is associated to the group $Y' = \{\chi \in \mathcal{D}(K) \mid \chi(p) = 1\}$.

PROOF. For all $\chi \in Y$ we have $\chi(p) \neq 0$, so by Proposition 9.39 p does not ramify in \mathbb{Q}_Y . Since Y is the largest subgroup of $\mathcal{D}(K)$ with this property, \mathbb{Q}_Y is the largest subfield of K in which p does not ramify: $\mathbb{Q}_Y = K^T$.

Since p does not ramify in K^T , the field K^T is a subfield of $\mathbb{Q}(\zeta_N)$ for some $N \in \mathbb{N}^*$ with $p \nmid N$. For $Z' = Z_p^{\mathbb{Q}(\zeta_N)} = \langle \sigma_p \rangle$ we have

$$\begin{aligned} \text{Dir}(Z') &= \{ \chi \in \mathcal{D}_N \mid \chi(\sigma) = 1 \text{ for all } \sigma \in Z' \} \\ &= \{ \chi \in \mathcal{D}_N \mid \chi(\sigma_p) = 1 \} = \{ \chi \in \mathcal{D}_N \mid \chi(p) = 1 \}. \end{aligned}$$

Put $Z'' = Z_p^{(K^T)}$. By Corollary 7.47 $(K^T)^{Z''} = K \cap \mathbb{Q}(\zeta_N)^{Z''}$ and $(K^T)^{Z''} = K^T \cap K^Z = K^Z$. Hence by Proposition 9.36 we have

$$\mathcal{D}(K^Z) = \mathcal{D}(K) \cap \mathcal{D}(\mathbb{Q}(\zeta_N)^{Z'}) = \mathcal{D}(K) \cap \text{Dir}(Z') = Y'. \quad \square$$

9.41 Corollary. *In the notation of Theorem 9.40: $\mathcal{D}(K)/Y \cong T$, $\mathcal{D}(K)/Y' \cong Z$ and $Y/Y' \cong Z/T$.* □

9.42 Application. We will use Dirichlet characters to show that for each finite abelian group G there exists an extension $L : K$ of abelian number fields such that $\text{Gal}(L : K) \cong G$ and no prime ideal of K ramifies in L .

Let G be a finite abelian group. Then G is a product of cyclic groups, say $G \cong C_{n_1} \times \cdots \times C_{n_r}$ with $n_i > 1$ for all i . Choose r different primes p_1, \dots, p_r such that $p_i \equiv 1 \pmod{n_i}$ for $i = 1, \dots, r$. For each i there is a $\chi_i \in \mathcal{D}_{p_i}$ of order n_i . Choose another prime p_{r+1} such that $p_{r+1} \equiv 1 \pmod{n_1 \cdots n_r}$ and a $\chi_{r+1} \in \mathcal{D}_{p_{r+1}}$ of order $n_1 \cdots n_r$. For each i the conductor of χ_i is p_i . Let $X = \langle \chi_1, \dots, \chi_{r+1} \rangle$ and $X' = \langle \chi \rangle$, where $\chi = \chi_1 \cdots \chi_{r+1}$. Take $L = \mathbb{Q}_X$ and $K = \mathbb{Q}_{X'}$. Then $K \subseteq L$ and

$$\text{Gal}(L : K) \cong X/X' \cong \langle \chi_1, \dots, \chi_r \rangle \cong G.$$

The primes which ramify in L are p_1, \dots, p_{r+1} . From Corollary 9.41 it follows that for each i we have $e_p^{(K)} = e_p^{(L)}$:

$$\begin{aligned} T_{p_i}^{(L)} &\cong X/\langle \chi_1, \dots, \chi_{i-1}, \chi_{i+1}, \dots, \chi_{r+1} \rangle \cong \langle \chi_i \rangle \cong C_{n_i} \\ T_{p_i}^{(K)} &\cong \langle \chi \rangle / \langle \chi^{n_i} \rangle \cong C_{n_i}. \end{aligned}$$

So $e_p^{(L)} = 1$ for all $p \in \text{Max}(\mathcal{O}_K)$.

Quadratic number fields

Quadratic number fields correspond to subgroups of \mathcal{D} of order 2 and hence to quadratic Dirichlet characters. Say the field $\mathbb{Q}(\sqrt{m})$ with m squarefree $\neq 1$ corresponds to the quadratic Dirichlet character χ_m . We will describe this character. By Proposition 9.13 the conductor of $\mathbb{Q}(\sqrt{m})$ is $|D_m|$. So by Proposition 9.36(iii) $N_{\chi_m} = |D_m|$.

9.43 Proposition. *Let K be a quadratic number field. Then $\mathcal{D}(K)$ is of order 2 and generated by a quadratic Dirichlet character with conductor $|\text{disc}(K)|$. \square*

The character χ_m describes the splitting behavior of primes in $\mathbb{Q}(\sqrt{m})$:

$$\chi_m(p) = \begin{cases} 0 & \text{if } p \text{ ramifies,} \\ 1 & \text{if } p \text{ splits completely,} \\ -1 & \text{if } p \text{ remains prime.} \end{cases}$$

The field $\mathbb{Q}(\sqrt{m})$ is real if and only if $m > 0$, so

$$\chi_m(-1) = \text{sgn}(m).$$

These values determine χ_m , because it is completely multiplicative. The value of χ_m in odd primes p is given by the Legendre symbol:

$$\chi_m(p) = \left(\frac{m}{p}\right).$$

Therefore, the value in odd $n \in \mathbb{N}^*$ is given by the Jacobi symbol:

$$\chi_m(n) = \left(\frac{m}{n}\right).$$

9.5 Dirichlet L-series

A Dirichlet character is an arithmetic function. Because it is completely multiplicative, it is worthwhile to study the associated Dirichlet series.

9.44 Definition. The *L-series* of $\chi \in \mathcal{D}$ is the Dirichlet series

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

The *L*-function of the trivial Dirichlet character is the Riemann zeta function. Unlike the Riemann zeta function the *L*-function of a nontrivial Dirichlet character is analytic at $s = 1$. For this we need the following simple lemma.

9.45 Lemma. *Let χ be a nontrivial Dirichlet character. Then $\sum_{n=1}^{N_\chi} \chi(n) = 0$.*

PROOF. Since χ is nontrivial, there is a $k \in \mathbb{Z}$ such that $\chi(k) \notin \{0, 1\}$. Then

$$\chi(k) \sum_{n=1}^{N_\chi} \chi(n) = \sum_{n=1}^{N_\chi} \chi(kn) = \sum_{n=1}^{N_\chi} \chi(n).$$

Because $\chi(k) \neq 0$, this implies $\sum_{n=1}^{N_\chi} \chi(n) = 0$. \square

9.46 Proposition. *Let χ be a nontrivial Dirichlet character. Then the L-series converges to an analytical function on the half-plane $\Re(s) > 0$.*

PROOF. By Lemma 9.45 we have $\sum_{n=1}^N \chi(n) = O(1)$. The proposition follows from Theorem 8.12. \square

For $\chi \neq 1$ the function $L(s, \chi)$ has a continuation to an analytic function on the whole plane. The *completed* L-series is given by

$$\Lambda(s, \chi) = L_\infty(s, \chi)L(s, \chi) \quad \text{for } \Re(s) > 1,$$

where

$$L_\infty(s, \chi) = \left(\frac{N_\chi}{\pi}\right)^{\frac{s}{2}} \Gamma\left(\frac{s+k}{2}\right),$$

the number k depending on the sign of χ :

$$k = \begin{cases} 0 & \text{if } \chi \text{ is even,} \\ 1 & \text{if } \chi \text{ is odd.} \end{cases}$$

The completed L-series for nontrivial χ admit analytic continuations to the whole plane and satisfy the functional equations

$$\Lambda(s, \chi) = \frac{g(\chi)}{i^k \sqrt{N_\chi}} \Lambda(1-s, \bar{\chi}).$$

The $g(\chi)$ in this equation is the Gauß sum of the character. For the Gauß sum see the next section. For the continuation of $L(s, \chi)$ see section VII.2 of [31].

Since χ is completely multiplicative, by Corollary 8.17 the L-series has a product representation. Note that the series converges absolutely for $\Re(s) > 1$.

9.47 Proposition. *Let $\chi \in \mathcal{D}$. Then for $\Re(s) > 1$:*

$$L(s, \chi) = \prod_p \frac{1}{1 - \frac{\chi(p)}{p^s}} \quad \square$$

The group $\mathcal{D}(K)$ associated to an abelian number field K describes the splitting behavior of primes in K (Proposition 9.39 and Theorem 9.40). This leads to a relation between the L-series of the Dirichlet characters in $\mathcal{D}(K)$ and the Dedekind zeta function of K .

9.48 Theorem. *Let K be an abelian number field. Then*

$$\zeta_K(s) = \prod_{\chi \in \mathcal{D}(K)} L(s, \chi).$$

PROOF. The Dirichlet series $\zeta_K(s)$ and all $L(s, \chi)$ have a product representation for $\Re(s) > 1$. We prove the equality by comparing these product representations. Let p be a prime and put $e = e_p^{(K)}$ and $f = f_p^{(K)}$. Then $[K : \mathbb{Q}] = ref$, where r is the number of $\mathfrak{p} \in \text{Max}(\mathcal{O}_K)$ above p . We have to prove that

$$\prod_{\mathfrak{p}|p\mathcal{O}_K} \frac{1}{1 - \frac{1}{N(\mathfrak{p})^s}} = \prod_{\chi \in \mathcal{D}(K)} \frac{1}{1 - \frac{\chi(p)}{p^s}}.$$

For the left hand side we have

$$\prod_{\mathfrak{p}|p\mathcal{O}_K} \frac{1}{1 - \frac{1}{N(\mathfrak{p})^s}} = \left(\frac{1}{1 - \frac{1}{p^{fs}}} \right)^r$$

and for the right hand side, using the notation of Theorem 9.40,

$$\begin{aligned} \prod_{\chi \in \mathcal{D}(K)} \frac{1}{1 - \frac{\chi(p)}{p^s}} &= \prod_{\chi \in Y} \frac{1}{1 - \frac{\chi(p)}{p^s}} = \prod_{a=0}^{f-1} \prod_{\substack{\chi \in Y \\ \chi(p) = \zeta_f^a}} \frac{1}{1 - \frac{\chi(p)}{p^s}} = \prod_{a=0}^{f-1} \left(\frac{1}{1 - \frac{\zeta_f^a}{p^s}} \right)^r \\ &= \left(\prod_{a=0}^{f-1} \frac{1}{1 - \frac{\zeta_f^a}{p^s}} \right)^r = \left(\frac{1}{1 - \frac{1}{p^{fs}}} \right)^r. \quad \square \end{aligned}$$

We have a product of meromorphic functions on $\Re(s) > 0$:

$$\zeta_K(s) = \zeta(s) \cdot \prod_{\substack{\chi \in \mathcal{D}(K) \\ \chi \neq 1}} L(s, \chi),$$

where the two zeta functions have only one single pole at $s = 1$. The L -functions for $\chi \neq 1$ are analytic in the half-plane. So we can express for abelian K the residue of $\zeta_K(s)$ at $s = 1$ in terms of values of L -series for $s = 1$:

9.49 Corollary. *Let K be an abelian number field. Then*

$$\text{Res}_{s=1} \zeta_K(s) = \prod_{\substack{\chi \in \mathcal{D}(K) \\ \chi \neq 1}} L(1, \chi). \quad \square$$

For a given $\chi \in \mathcal{D}$ of order $n \neq 1$ we have in particular

$$\text{Res}_{s=1} \zeta_{\mathbb{Q}_\chi}(s) = \prod_{a=1}^{n-1} L(1, \chi^a).$$

The left hand side is nonzero by the class number formula for the number field \mathbb{Q}_χ , so the L -functions of nontrivial Dirichlet characters χ do not have a zero at $s = 1$:

9.50 Theorem. Let χ be a nontrivial Dirichlet character. Then $L(1, \chi) \neq 0$. \square

An application is a well-known theorem of Dirichlet on primes in an arithmetic progression. In its proof we will use the following lemma.

9.51 Lemma. Let $N \in \mathbb{N}^*$ and $a \in \mathbb{Z}$ such that $\gcd(a, N) = 1$. Then

$$\sum_{\chi \in \mathcal{D}_N} \chi(a) = \begin{cases} \varphi(N) & \text{if } a \equiv 1 \pmod{N}, \\ 0 & \text{if } a \not\equiv 1 \pmod{N}. \end{cases}$$

PROOF. For $a \equiv 1 \pmod{N}$ we have $\chi(a) = 1$ for all $\chi \in \mathcal{D}_N$. So assume that $a \not\equiv 1 \pmod{N}$. Then there exists a $\chi_0 \in \mathcal{D}_N$ such that $\chi_0(a) \neq 0, 1$ and we have

$$\chi_0(a) \sum_{\chi \in \mathcal{D}_N} \chi(a) = \sum_{\chi \in \mathcal{D}_N} (\chi_0 \chi)(a) = \sum_{\chi \in \mathcal{D}_N} \chi(a).$$

Since $\chi_0(a) \neq 1$ it follows that $\sum_{\chi \in \mathcal{D}_N} \chi(a) = 0$. \square

9.52 Theorem (Dirichlet). Let $N \in \mathbb{N}^*$, $a \in \mathbb{Z}$ such that $\gcd(a, N) = 1$. Then the set of primes $p \equiv a \pmod{N}$ has Dirichlet density $\frac{1}{\varphi(N)}$. In particular there are infinitely many of these primes.

PROOF. Let $\chi \in \mathcal{D}_N$. By Proposition 8.31 we have

$$\log L(s, \chi) \sim \sum_p \frac{\chi(p)}{p^s}.$$

Therefore, using Lemma 9.51

$$\begin{aligned} \sum_{\chi \in \mathcal{D}_N} \overline{\chi(a)} \log L(s, \chi) &\sim \sum_{\chi \in \mathcal{D}_N} \sum_p \frac{\overline{\chi(a)} \chi(p)}{p^s} = \sum_p \sum_{\chi \in \mathcal{D}_N} \frac{\overline{\chi(a)} \chi(p)}{p^s} \\ &= \sum_{p \equiv a \pmod{N}} \frac{\varphi(N)}{p^s}. \end{aligned}$$

On the other hand by Theorem 9.50

$$\sum_{\chi \in \mathcal{D}_N} \overline{\chi(a)} \log L(s, \chi) = \zeta(s) + \sum_{\substack{\chi \in \mathcal{D}_N \\ \chi \neq 1}} \overline{\chi(a)} \log L(s, \chi) \sim \zeta(s).$$

Hence

$$\sum_{p \equiv a \pmod{N}} \frac{1}{p^s} \sim \frac{1}{\varphi(N)} \zeta(s) \sim -\frac{1}{\varphi(N)} \log(s-1).$$

So by Corollary 8.34 we have $\delta(P) = \frac{1}{\varphi(N)}$ for P the set of primes $p \equiv a \pmod{N}$. \square

Another consequence of Theorem 9.48 is that it leads to formulas for class numbers. From this theorem and Theorem 8.20 follows:

9.53 Theorem. *Let K be an abelian number field of degree n . Then*

$$\prod_{\substack{\chi \in \mathcal{D}(K) \\ \chi \neq 1}} L(1, \chi) = \begin{cases} \frac{2^{n-1} h(K) \operatorname{Reg}(K)}{\sqrt{|\operatorname{disc}(K)|}}, & \text{if } K \text{ is totally real,} \\ \frac{(2\pi)^{n/2} h(K) \operatorname{Reg}(K)}{\#(\mu(K)) \sqrt{|\operatorname{disc}(K)|}}, & \text{if } K \text{ is totally imaginary.} \end{cases}$$

□

In particular for quadratic number fields we have:

9.54 Corollary. *Let $m \in \mathbb{Z}$ be squarefree $\neq 1$. Put $h_m = h(\mathbb{Q}(\sqrt{m}))$. Then $L(1, \chi_{-1}) = \frac{\pi}{4} h_{-1}$, $L(1, \chi_{-3}) = \frac{\pi\sqrt{3}}{9} h_{-3}$ and*

$$L(1, \chi_m) = \begin{cases} \frac{\pi h_m}{\sqrt{-D_m}} & \text{if } m < -3, \\ \frac{2 \log \varepsilon_m \cdot h_m}{\sqrt{D_m}} & \text{if } m > 0. \end{cases}$$

(ε_m is the fundamental unit of the real quadratic number field $\mathbb{Q}(\sqrt{m})$.) □

The next examples show how in principle $L(1, \chi_m)$ can be calculated for a given m . Later in this chapter a better technique will be described.

9.55 Example. For $m = -1$ we have

$$\begin{aligned} L(1, \chi_{-1}) &= 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots = \int_0^1 (1 - x^2 + x^4 - \cdots) dx \\ &= \int_0^1 \frac{dx}{1+x^2} = \arctan 1 = \frac{\pi}{4}. \end{aligned}$$

So indeed $h_{-1} = 1$.

9.56 Example. For $m = 5$ we have $h_5 = \frac{\sqrt{5}}{2 \log \frac{1+\sqrt{5}}{2}} L(1, \chi_5)$ and

$$\begin{aligned} L(1, \chi_5) &= (1 - \frac{1}{2} - \frac{1}{3} + \frac{1}{4}) + (\frac{1}{6} - \frac{1}{7} - \frac{1}{8} + \frac{1}{9}) + \cdots \\ &= \int_0^1 ((1 - x - x^2 + x^3) + (x^5 - x^6 - x^7 + x^8) + \cdots) dx \\ &= \int_0^1 (1 - x - x^2 + x^3)(1 + x^5 + x^{10} + \cdots) dx \\ &= \int_0^1 \frac{1 - x - x^2 + x^3}{1 - x^5} dx = \int_0^1 \frac{1 - x^2}{1 + x + \cdots + x^4} dx \end{aligned}$$

$$\begin{aligned}
&= -\int_0^1 \frac{1 - \frac{1}{x^2}}{\frac{1}{x^2} + \frac{1}{x} + 1 + x + x^2} dx = \int_2^\infty \frac{dy}{y^2 + y - 1} = \int_{\frac{5}{2}}^\infty \frac{dz}{z^2 - \frac{5}{2}} \\
&= \frac{1}{2\sqrt{\frac{5}{2}}} \log \frac{\frac{5}{2} + \frac{1}{2}\sqrt{5}}{\frac{5}{2} - \frac{1}{2}\sqrt{5}} = \frac{2}{\sqrt{5}} \log \frac{\sqrt{5} + 1}{2}.
\end{aligned}$$

So $h_5 = 1$.

9.57 Example: complex biquadratic number fields. Let K be a complex biquadratic number field and K_1, K_2 and K_3 its quadratic subfields, say K_1 is the real quadratic subfield and ε its fundamental unit. By Theorem 9.53 we have

$$\frac{4\pi^2 h(K) \operatorname{Reg}(K)}{w(K) \sqrt{|\operatorname{disc}(K)|}} = \frac{2h(K_1) \log \varepsilon}{\sqrt{|\operatorname{disc}(K_1)|}} \cdot \frac{2\pi h(K_2)}{w(K_2) \sqrt{|\operatorname{disc}(K_2)|}} \cdot \frac{2\pi h(K_3)}{w(K_3) \sqrt{|\operatorname{disc}(K_3)|}}.$$

It is shown in exercise 9 of chapter 1 that

$$\operatorname{disc}(K) = \operatorname{disc}(K_1) \cdot \operatorname{disc}(K_2) \cdot \operatorname{disc}(K_3).$$

So for $\#(\mu(K)) \neq 4, 6, 8, 12$ the formula reduces to

$$h(K) \operatorname{Reg}(K) = h(K_1)h(K_2)h(K_3) \log \varepsilon.$$

Inspection shows that this formula holds for $\#(\mu(K)) = 4, 6, 12$ as well, so $K = \mathbb{Q}(\zeta_8) = \mathbb{Q}(i, \sqrt{2})$ is the only exception. Hence for $K \neq \mathbb{Q}(\zeta_8)$:

$$h(K) = \frac{1}{2}Q(K)h(K_1)h(K_2)h(K_3),$$

where $Q(K)$ is the Hasse index of K . By Theorem 5.48 the Hasse index is 1 or 2.

9.58 Example: real biquadratic number fields. Let K be a real biquadratic number field, K_1, K_2 and K_3 its quadratic subfields with fundamental units $\varepsilon_1, \varepsilon_2$ and ε_3 respectively. By Theorem 9.53 we now have

$$\frac{2^4 h(K) \operatorname{Reg}(K)}{2\sqrt{|\operatorname{disc}(K)|}} = \frac{2^2 h(K_1) \log \varepsilon_1}{2\sqrt{|\operatorname{disc}(K_1)|}} \cdot \frac{2^2 h(K_2) \log \varepsilon_2}{2\sqrt{|\operatorname{disc}(K_2)|}} \cdot \frac{2^2 h(K_3) \log \varepsilon_3}{2\sqrt{|\operatorname{disc}(K_3)|}}.$$

This reduces to

$$h(K) \operatorname{Reg}(K) = h(K_1)h(K_2)h(K_3) \log \varepsilon_1 \log \varepsilon_2 \log \varepsilon_3.$$

The fundamental units of the quadratic subfields are units of K . The regulator of K is defined using a fundamental system of units of K . Taking the system $(\varepsilon_1, \varepsilon_2, \varepsilon_3)$ instead leads to

$$\operatorname{Reg}(\varepsilon_1, \varepsilon_2, \varepsilon_3) = \begin{vmatrix} \log \varepsilon_1 & \log \varepsilon_1 & -\log \varepsilon_1 \\ \log \varepsilon_2 & -\log \varepsilon_2 & \log \varepsilon_2 \\ \log \varepsilon_3 & -\log \varepsilon_3 & -\log \varepsilon_3 \end{vmatrix} = 4 \log \varepsilon_1 \log \varepsilon_2 \log \varepsilon_3.$$

From

$$(\mathcal{O}_K^* : \mathcal{O}_{K_1}^* \mathcal{O}_{K_2}^* \mathcal{O}_{K_3}^*) = \frac{\text{Reg}(\varepsilon_1, \varepsilon_2, \varepsilon_3)}{\text{Reg}(K)}$$

then follows

$$h(K) = \frac{1}{4}(\mathcal{O}_K^* : \mathcal{O}_{K_1}^* \mathcal{O}_{K_2}^* \mathcal{O}_{K_3}^*)h(K_1)h(K_2)h(K_3).$$

9.6 The Gauß sum of a Dirichlet character

In one of his proofs of the Quadratic Reciprocity Law Gauß expressed square roots of odd primes as sums of roots of unity, nowadays called Gauß sums.

9.59 Definition. Let $\chi \in \mathcal{D}$. We define

$$g(\chi) = \sum_{n=1}^{N_\chi} \chi(n) \zeta_{N_\chi}^n.$$

The number $g(\chi)$ is called the (*standard*) *Gauß sum* of the Dirichlet character χ . More generally we define for $k \in \mathbb{Z}$:

$$g_k(\chi) = \sum_{n=1}^{N_\chi} \chi(n) \zeta_{N_\chi}^{kn}.$$

(Thus $g(\chi) = g_1(\chi)$.)

The sum is over the numbers 1 up to N_χ . Of course any system of representatives of \mathbb{Z}/N_χ will do. The Gauß sum of a $\chi \in \mathcal{D}$ is an element of the m -th cyclotomic field for $m = \text{lcm}(o(\chi), N_\chi)$.

9.60 Lemma. Let $\chi \in \mathcal{D}$ and $k \in \mathbb{Z}$ such that $\text{gcd}(k, N_\chi) > 1$. Then $g_k(\chi) = 0$.

PROOF. Put $N_\chi = dN_1$ and $k = dk_1$, where $d = \text{gcd}(k, N_\chi)$. Then

$$g_k(\chi) = \sum_{n=1}^N \chi(n) \zeta_{N_1}^{k_1 n} = \sum_{m=1}^{N_1} \left(\zeta_{N_1}^{k_1 m} \sum_{\substack{n \equiv m \pmod{N_1} \\ 1 \leq n \leq N}} \chi(n) \right).$$

It suffices to show that

$$s_m := \sum_{\substack{n \equiv m \pmod{N_1} \\ 1 \leq n \leq N}} \chi(n) = 0.$$

There is a $t \in \mathbb{Z}$ such that $t \equiv 1 \pmod{N_1}$, $\gcd(t, N) = 1$ and $\chi(t) \neq 1$. We have

$$\chi(t)s_m = \sum_{\substack{n \equiv m \pmod{N_1} \\ 1 \leq n \leq N}} \chi(nt) = s_m.$$

So $s_m = 0$, because $\chi(t) \neq 1$. □

9.61 Proposition. *Let $\chi \in \mathcal{D}$ and $k \in \mathbb{Z}$. Then $g_k(\chi) = \overline{\chi(k)}g(\chi)$.*

PROOF. Put $N = N_\chi$. If $\gcd(k, N) > 1$, then $\chi(k) = 0$ and by Lemma 9.60 $g_k(\chi) = 0$. So we assume that $\gcd(k, N) = 1$. Take an $l \in \mathbb{Z}$ such that $kl \equiv 1 \pmod{N}$. Then

$$g_k(\chi) = \sum_{n=1}^N \chi(n)\zeta_N^{kn} = \sum_{n=1}^N \chi(nl)\zeta_N^n = \chi(l) \sum_{n=1}^N \chi(n)\zeta_N^n = \overline{\chi(k)}g(\chi). \quad \square$$

9.62 Corollary. *Let $\chi \in \mathcal{D}$. Then $\overline{g(\chi)} = \chi(-1)g(\overline{\chi})$.*

PROOF. $\overline{g(\chi)} = \sum_{n=1}^N \overline{\chi(n)\zeta_N^{-n}} = g_{-1}(\overline{\chi}) = \chi(-1)g(\overline{\chi})$. □

9.63 Theorem. *Let $\chi \in \mathcal{D}$. Then $g(\chi)\overline{g(\chi)} = N_\chi$.*

PROOF. Put $N = N_\chi$. We compute $\sum_{k=1}^N g_k(\chi)\overline{g_k(\chi)}$ in two ways.

$$\begin{aligned} \sum_{k=1}^N g_k(\chi)\overline{g_k(\chi)} &= \sum_{k=1}^N g(\chi)\overline{g(\chi)}\overline{\chi(k)}\chi(k) = g(\chi)\overline{g(\chi)} \sum_{k=1}^N \overline{\chi(k)}\chi(k) \\ &= g(\chi)\overline{g(\chi)} \cdot \varphi(N) \end{aligned}$$

and, using Lemma 9.45,

$$\begin{aligned} \sum_{k=1}^N g_k(\chi)\overline{g_k(\chi)} &= \sum_{k=1}^N \left(\sum_{l=1}^N \chi(l)\zeta_N^{kl} \right) \left(\sum_{m=1}^N \overline{\chi(m)\zeta_N^{-km}} \right) \\ &= \sum_{k=1}^N \sum_{l=1}^N \sum_{m=1}^N \chi(l)\overline{\chi(m)}\zeta_N^{(l-m)k} = \sum_{l=1}^N \sum_{m=1}^N \chi(l)\overline{\chi(m)} \sum_{k=1}^N \zeta_N^{(l-m)k} \\ &= \sum_{l=1}^N \chi(l)\overline{\chi(l)} \sum_{k=1}^N 1 = \varphi(N) \cdot N. \end{aligned}$$

Hence $g(\chi)\overline{g(\chi)} = N$. □

9.7 The Gauß sum of a quadratic Dirichlet character

By the results in the previous section the Gauß sum of a quadratic Dirichlet character is determined up to sign:

9.64 Proposition. *Let χ_m be the quadratic Dirichlet character corresponding to the quadratic number field $\mathbb{Q}(\sqrt{m})$, where m is squarefree. Then $g(\chi_m)^2 = D_m$.*

PROOF. By Theorem 9.63, Corollary 9.62 and Proposition 9.43 we have

$$g(\chi_m)^2 = g(\chi_m)\overline{g(\chi_m)} = \chi_m(-1)g(\chi_m)g(\overline{\chi_m}) = \chi_m(-1)|D_m| = D_m. \quad \square$$

We will show that in fact $g(\chi_m) = \sqrt{D_m}$ (with the usual convention for the square root of a real number). First the computation will be reduced to the case $m = p^*$ for p an odd prime. The character χ_{p^*} is the character given by the Legendre symbol $a \mapsto \left(\frac{a}{p}\right)$. Examples strongly suggest that the formula $g(\chi_{p^*}) = \sqrt{p^*}$ is indeed the right one, see the Figures 9.1 and 9.2, which are in fact just a variation on the graphical representation given in Figure 3.1. It took Gauß many years to establish this result.

9.65 Definition. For $a, b \in \mathbb{R}^*$ define

$$[a, b] = \begin{cases} -1 & \text{if } a < 0 \text{ and } b < 0, \\ 1 & \text{otherwise.} \end{cases}$$

9.66 Lemma. *For $a, b \in \mathbb{R}^*$ we have $\sqrt{a} \cdot \sqrt{b} = [a, b]\sqrt{ab}$.* □

9.67 Proposition. *Let $m_1, m_2 \in \mathbb{Z}$ be squarefree $\neq 1$ such that $\gcd(D_{m_1}, D_{m_2}) = 1$. Then $g(\chi_{m_1})g(\chi_{m_2}) = [m_1, m_2]g(\chi_{m_1 m_2})$.*

PROOF. Put $N_1 = |D_{m_1}|$ and $N_2 = |D_{m_2}|$. We have

$$\begin{aligned} g(\chi_{m_1})g(\chi_{m_2}) &= \left(\sum_{k=1}^{N_1} \chi_{m_1}(k) \zeta_{N_1}^k \right) \left(\sum_{l=1}^{N_2} \chi_{m_2}(l) \zeta_{N_2}^l \right) \\ &= \sum_{k=1}^{N_1} \sum_{l=1}^{N_2} \chi_{m_1}(k) \chi_{m_2}(l) \zeta_{N_1 N_2}^{k N_2 + l N_1} \\ &= \sum_{s=1}^{N_1 N_2} \chi_{m_1}(s) \chi_{m_2}(s) \zeta_{N_1 N_2}^{(N_1 + N_2)s} \quad (\text{Chinese Remainder Theorem}) \\ &= g_{N_1 + N_2}(\chi_{m_1 m_2}) = \chi_{m_1 m_2}(N_1 + N_2) g(\chi_{m_1 m_2}) \\ &= \chi_{m_1}(N_1 + N_2) \chi_{m_2}(N_1 + N_2) g(\chi_{m_1 m_2}) \\ &= \chi_{m_1}(N_2) \chi_{m_2}(N_1) g(\chi_{m_1 m_2}) \\ &= \chi_{m_1}(\text{sgn}(m_2)) \chi_{m_2}(\text{sgn}(m_1)) \chi_{m_1}(m_2) \chi_{m_2}(m_1) g(\chi_{m_1 m_2}) \end{aligned}$$

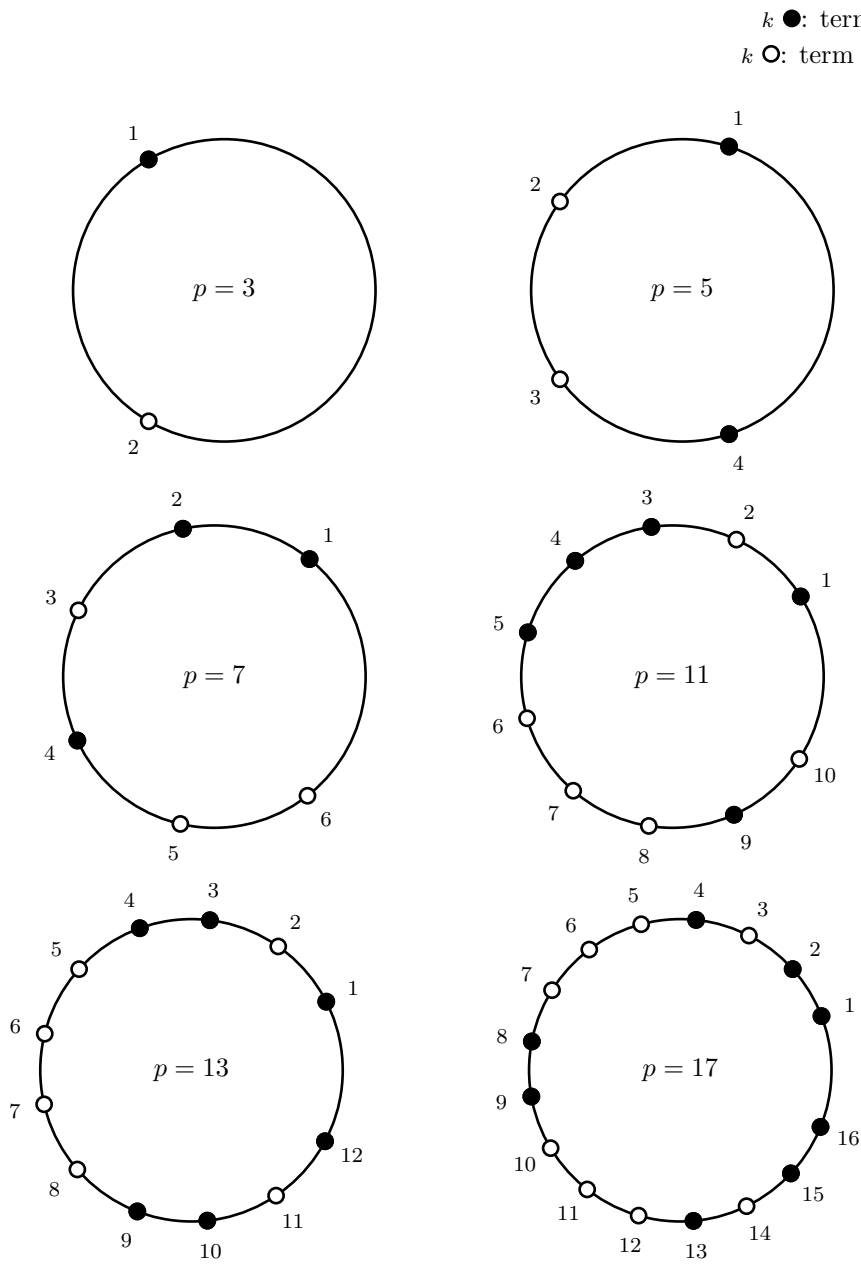


Figure 9.1: Terms of the Gauß sum for the first six odd primes

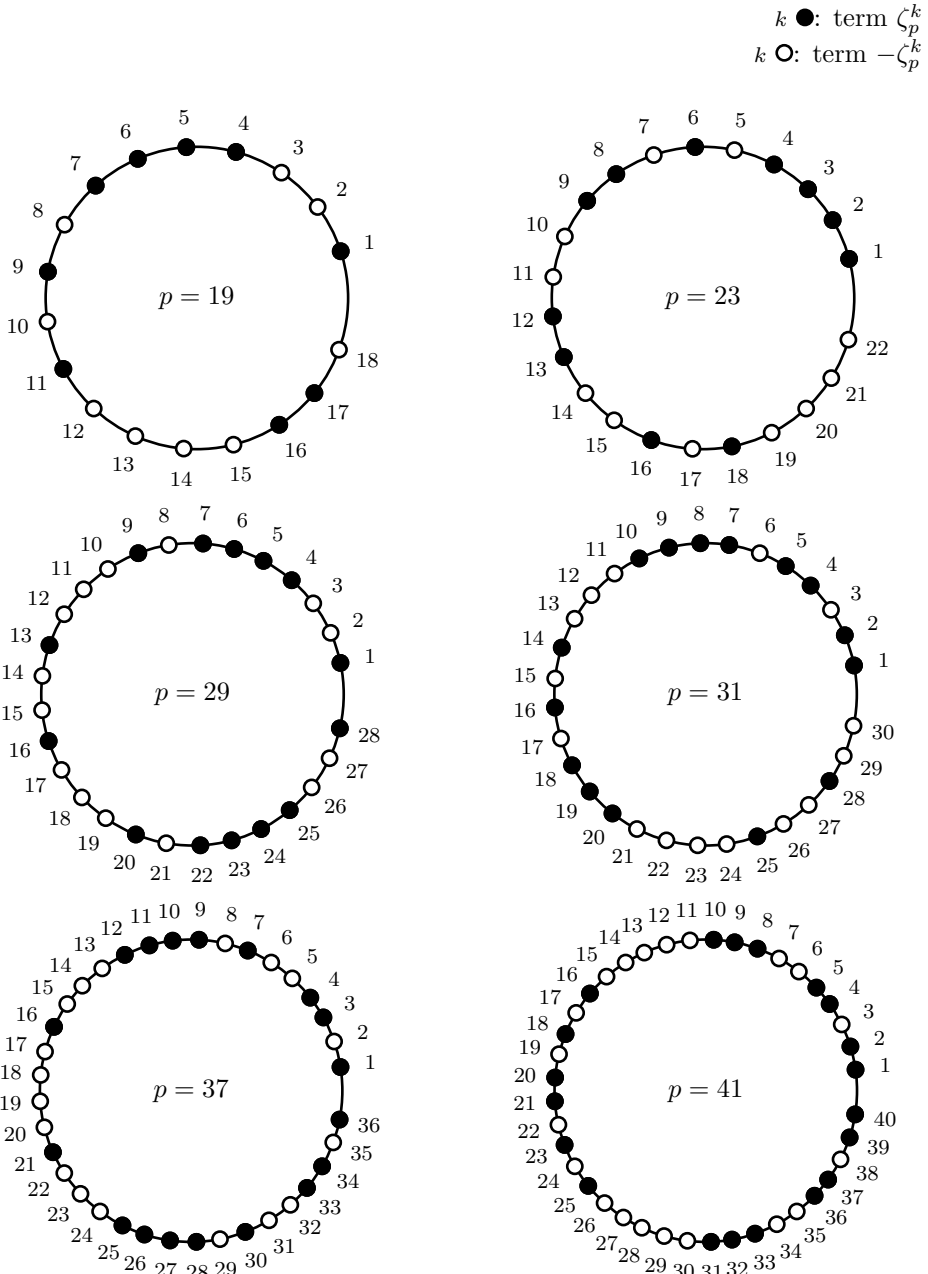


Figure 9.2: Terms of the Gauß sum for the next six odd primes

$$= \chi_{m_1}(m_2)\chi_{m_2}(m_1)g(\chi_{m_1 m_2}). \quad (\chi_{m_1}(\text{sgn}(m_2)) = [m_1, m_2])$$

So it remains to prove that

$$\chi_{m_1}(m_2)\chi_{m_2}(m_1) = [m_1, m_2].$$

If $m_1 = n_1 n_2$ such that $\gcd(D_{n_1}, D_{n_2}) = 1$, then

$$\begin{aligned} \chi_{m_1}(m_2)\chi_{m_2}(m_1) &= \chi_{n_1}(m_2)\chi_{n_2}(m_2)\chi_{m_2}(n_1)\chi_{m_2}(n_2) \\ &= \chi_{n_1}(m_2)\chi_{m_2}(n_1) \cdot \chi_{n_2}(m_2)\chi_{m_2}(n_2) \end{aligned}$$

and also

$$[m_1, m_2] = [n_1, m_2] \cdot [n_2, m_2].$$

So it suffices to verify the formula for $m_1 = p^*$ and $m_2 = q^*$ with p and q different odd primes, and also for $m_1 = p^*$ (with p an odd prime) and $m_2 \in \{-1, 2, -2\}$.

1. $\chi_{p^*}(q^*) = [p^*, q^*] \left(\frac{p^*}{q}\right) = [p^*, q^*] \left(\frac{q}{p}\right)$, so $\chi_{p^*}(q^*)\chi_{q^*}(p^*) = \left(\frac{q}{p}\right) \left(\frac{p}{q}\right) = [p^*, q^*]$.
2. $\chi_{p^*}(-1)\chi_{-1}(p^*) = \text{sgn}(p^*) = [p^*, -1]$.
3. $\chi_{p^*}(2)\chi_2(p^*) = (-1)^{\frac{p^*-1}{8}}\chi_2(p) = 1 = [p^*, 2]$.
4. $\chi_{p^*}(-2)\chi_{-2}(p^*) = \text{sgn}(p^*)\chi_{p^*}(2)\chi_2(p^*)\chi_{-1}(p^*) = \text{sgn}(p^*) = [p^*, -2]$. \square

This proposition and the lemma will enable us to reduce the computation of the sign of the Gauß sum of the character χ_m to the case where $m = p^*$, where p is an odd prime and the cases $m = -1$, $m = 2$ and $m = -2$.

9.68 Proposition. $g(\chi_{-1}) = \sqrt{-4}$, $g(\chi_2) = \sqrt{8}$ and $g(\chi_{-2}) = \sqrt{-8}$.

PROOF. $g(\chi_{-1}) = \zeta_4 - \zeta_4^3 = 2i = \sqrt{-4}$, $g(\chi_2) = \zeta_8 - \zeta_8^3 - \zeta_8^5 + \zeta_8^7 = 2\sqrt{2}$ and $g(\chi_{-2}) = \zeta_8 + \zeta_8^3 - \zeta_8^5 - \zeta_8^7 = 2\sqrt{-2}$. \square

9.69 Theorem. Let p be an odd prime. Then $g(\chi_{p^*}) = \sqrt{p^*}$.

PROOF. Put $\zeta_p = \zeta$. Let T be the linear transformation of the complex vector space $\mathbb{C}^{\mathbb{F}_p}$ of all maps $\mathbb{F}_p \rightarrow \mathbb{C}$ defined by

$$(Tf)(j) = \sum_{k=0}^{p-1} f(k)\zeta^k,$$

for all $f \in \mathbb{C}^{\mathbb{F}_p}$. (T is a ‘Fourier transformation’.) We will compute the determinant of this transformation T using two bases: the canonical basis and a basis of characters. Comparison of the results of the two computations will lead to a computation of the Gauß sum of the quadratic character on \mathbb{F}_p .

First computation

On the canonical basis e_0, \dots, e_{p-1} , where $e_i(j) = \delta_{ij}$, the matrix of T is of Vandermonde type:

$$(\zeta^{(i-1)(j-1)})_{\substack{1 \leq i \leq p \\ 1 \leq j \leq p}}$$

The square of this matrix is

$$\begin{pmatrix} p & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & p \\ 0 & 0 & 0 & \cdots & p & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & p & \cdots & 0 & 0 \\ 0 & p & 0 & \cdots & 0 & 0 \end{pmatrix}.$$

So $(\det(T))^2 = (-1)^{\frac{p-1}{2}} p^p$, hence

$$|\det(T)| = p^{\frac{p-1}{2}} \sqrt{p}.$$

(Alternatively, $\det(T)^2 = \text{disc}(X^p - 1) = (-1)^{\frac{p-1}{2}} \prod_{k=0}^{p-1} p \zeta_p^k$.)

On the other hand we can use the formula for the determinant of a Vandermonde matrix:

$$\det(T) = \prod_{\substack{i>j \\ 0 \leq i, j \leq p-1}} (\zeta^i - \zeta^j).$$

The factors in this product can be grouped in the following way:

$$\begin{aligned} \det(T) &= \prod_{\substack{i>j \\ 1 \leq i, j \leq \frac{p-1}{2}}} (\zeta^i - \zeta^j)(\zeta^{p-j} - \zeta^{p-i})(\zeta^{p-i} - \zeta^j)(\zeta^{p-j} - \zeta^i) \\ &\quad \cdot \prod_{i=1}^{\frac{p-1}{2}} (\zeta^i - 1)(\zeta^{p-i} - 1) \cdot \prod_{i=1}^{\frac{p-1}{2}} (\zeta^{p-i} - \zeta^i). \end{aligned}$$

All factors in the first and in the second product are positive reals, while the factors in the third product are equal to $-i$ times a positive real. So we have

$$\det(T) = (-i)^{\frac{p-1}{2}} p^{p-1} \sqrt{p}.$$

Second computation

For each of the $p - 1$ multiplicative characters χ of the field \mathbb{F}_p we have

$$(T\chi)(j) = \sum_{k=1}^{p-1} \chi(k) \zeta^{jk} = \overline{\chi(j)} g(\chi).$$

9.70 Theorem (Gauß). *Let $m \in \mathbb{Z}$ be squarefree $\neq 1$. Then*

$$g(\chi_m) = \sqrt{D_m}.$$

PROOF. Let $m = up_1^* \cdots p_r^*$ with $u \in \{\pm 1, \pm 2\}$ and p_1, \dots, p_r different odd primes. Then

$$\chi_m = \chi_u \chi_{p_1^*} \cdots \chi_{p_r^*},$$

a product of r (or $r - 1$ if $u = 1$) Dirichlet characters for which the theorem has shown to hold (Proposition 9.68 and Theorem 9.69). The theorem follows by induction using Lemma 9.66 and Proposition 9.67: let $m_1, m_2 \in \mathbb{Z}$ be squarefree $\neq 1$ such that $\gcd(D_{m_1}, D_{m_2}) = 1$, then

$$\begin{aligned} g(\chi_{m_1 m_2}) &= [m_1, m_2] g(\chi_{m_1}) g(\chi_{m_2}) = [m_1, m_2] \sqrt{D_{m_1}} \sqrt{D_{m_2}} \\ &= [m_1, m_2] [D_{m_1}, D_{m_2}] \sqrt{D_{m_1 m_2}} = \sqrt{D_{m_1 m_2}}. \end{aligned} \quad \square$$

An equivalent formulation is: for quadratic $\chi \in \mathcal{D}$ we have $g(\chi) = \sqrt{\chi(-1)N_\chi}$.

9.8 Class number formulas

We compute $L(1, \chi)$ for a $\chi \in \mathcal{D}$. Put $N = N_\chi$. By Proposition 9.61

$$\chi(k) = \frac{1}{g(\chi)} \sum_{n=1}^N \overline{\chi(n)} \zeta_N^{-kn}.$$

So we have

$$L(1, \chi) = \sum_{k=1}^{\infty} \frac{\chi(k)}{k} = \frac{1}{g(\chi)} \sum_{k=1}^{\infty} \frac{1}{k} \sum_{n=1}^{N-1} \overline{\chi(n)} e^{-\frac{2k\pi in}{N}} = \frac{1}{g(\chi)} \sum_{n=1}^{N-1} \overline{\chi(n)} \sum_{k=1}^{\infty} \frac{e^{-\frac{2\pi in k}{N}}}{k}.$$

9.71 Lemma. *Let $\vartheta \in \mathbb{R}$ such that $0 < \vartheta < 2\pi$. Then*

$$\sum_{k=1}^{\infty} \frac{e^{ik\vartheta}}{k} = -\log\left(2 \sin \frac{\vartheta}{2}\right) + i\left(\frac{\pi}{2} - \frac{\vartheta}{2}\right).$$

PROOF. The power series $\sum \frac{z^k}{k}$ converges for $|z| \leq 1$ and $z \neq 1$ to the principal value of $-\log(1 - z)$. For $|z| < 1$ the argument of $1 - z$ is between $-\frac{\pi}{2}$ and $\frac{\pi}{2}$. We have

$$|1 - e^{i\vartheta}| = \left| e^{\frac{i\vartheta}{2}} - e^{-\frac{i\vartheta}{2}} \right| = \left| 2i \sin \frac{\vartheta}{2} \right| = 2 \sin \frac{\vartheta}{2}$$

and

$$\arg(1 - e^{i\vartheta}) = \arg\left(e^{\frac{i\vartheta}{2}} - e^{-\frac{i\vartheta}{2}}\right) + \arg\left(e^{-\frac{i\vartheta}{2}}\right) = \frac{\pi}{2} - \frac{\vartheta}{2}.$$

Since $-\log(1 - z) = -\log|1 - z| - i \arg(1 - z)$, the lemma follows. □

9.72 Theorem. *Let $\chi \in \mathcal{D}$ and $N = N_\chi$. Then*

$$L(1, \chi) = -\frac{1}{g(\chi)} \sum_{n=1}^{N-1} \overline{\chi(n)} \log \sin \frac{n\pi}{N} + \frac{i\pi}{Ng(\chi)} \sum_{n=1}^{N-1} \overline{\chi(n)} n.$$

PROOF. By the lemma

$$\sum_{k=1}^{\infty} \frac{e^{-\frac{2\pi i n k}{N}}}{k} = -\log \left(2 \sin \frac{n\pi}{N} \right) + i \left(\frac{\pi}{2} + \frac{n\pi}{N} \right) = -\log 2 + \frac{i\pi}{2} - \log \sin \frac{n\pi}{N} + \frac{i\pi}{N} n.$$

□

Class number formulas for quadratic number fields

The Gauß sum of χ_m has been computed in section 9.6 (Theorem 9.70). It is purely imaginary for $m < 0$ and real for $m > 0$. So for the quadratic case Theorem 9.72 yields the following.

9.73 Theorem. *Let $m \in \mathbb{Z}$ be squarefree and $\neq 1$. Then*

$$L(1, \chi_m) = \frac{\pi}{D_m \sqrt{-D_m}} \sum_{n=1}^{-D_m-1} \chi_m(n) n$$

if $m < 0$, and

$$L(1, \chi_m) = -\frac{1}{\sqrt{D_m}} \sum_{n=1}^{D_m-1} \chi_m(n) \log \sin \frac{\pi n}{D_m}$$

if $m > 0$. □

Now we have two computations of $L(1, \chi_m)$. In one of them (Corollary 9.54) the class number occurs. Equating the two outcomes yields formulas for the class numbers.

9.74 Theorem. *Let $m \in \mathbb{Z}$ be squarefree and $\neq 1$. Then for $m < 0$*

$$h_m = \frac{w_m}{2D_m} \sum_{n=1}^{-D_m-1} \chi_m(n) n$$

and for $m > 0$

$$h_m = -\frac{1}{2 \log \varepsilon_m} \sum_{n=1}^{D_m-1} \chi_m(n) \log \sin \frac{\pi n}{D_m}. \quad \square$$

9.75 Examples.

$$h_{-3} = -\frac{6}{6} \sum_{n=1}^2 \chi_{-3}(n)n = -(1-2) = 1,$$

$$h_{-1} = -\frac{4}{8} \sum_{n=1}^3 \chi_{-1}(n)n = -\frac{1}{2}(1-3) = 1,$$

$$h_{-7} = -\frac{2}{14} \sum_{n=1}^6 \chi_{-7}(n)n = -\frac{1}{7}(1+2-3+4-5-6) = 1,$$

$$h_{-5} = -\frac{2}{40} \sum_{n=1}^{19} \chi_{-5}(n)n = -\frac{1}{20}(1+3+7+9-11-13-17-19) = 2.$$

9.76 Example. For $m > 0$ the formula can be put in the following form:

$$\varepsilon_m^{2h_m} = \prod_{n=1}^{D_m-1} \left(\sin \frac{\pi n}{D_m} \right)^{-\chi_m(n)}.$$

For $m = 5$:

$$\varepsilon_5^{2h_5} = \frac{\sin \frac{2\pi}{5} \sin \frac{3\pi}{5}}{\sin \frac{\pi}{5} \sin \frac{4\pi}{5}} = \left(\frac{\sin \frac{2\pi}{5}}{\sin \frac{\pi}{5}} \right)^2 = \left(2 \cos \frac{\pi}{5} \right)^2 = \left(\frac{1 + \sqrt{5}}{2} \right)^2 = \varepsilon_5^2,$$

so $h_5 = 1$.

9.77 Example. For $m > 0$ a somewhat different formula is often easier to handle. From

$$L(1, \chi_m) = -\frac{1}{\sqrt{D_m}} \sum_{n=1}^{D_m-1} \chi_m(n) \log(1 - \zeta_{D_m}^n)$$

and Corollary 9.54 follows

$$\varepsilon_m^{2h_m} = \prod_{n=1}^{D_m-1} (1 - \zeta_{D_m}^n)^{-\chi_m(n)} = \frac{\prod_{\chi_m(n)=-1} (1 - \zeta_{D_m}^n)}{\prod_{\chi_m(n)=1} (1 - \zeta_{D_m}^n)}.$$

For example

$$\varepsilon_2^{2h_2} = \frac{(1 - \zeta_8^3)(1 - \zeta_8^5)}{(1 - \zeta_8)(1 - \zeta_8^7)} = \frac{2 - \zeta_8^3 - \zeta_8^{-3}}{2 - \zeta_8 - \zeta_8^{-1}} = \frac{2 + \sqrt{2}}{2 - \sqrt{2}} = 3 + 2\sqrt{2} = \varepsilon_2^2.$$

So $h_2 = 1$.

Finally for $m < 0$ we further simplify the class number formula. For $m \equiv 2, 3 \pmod{4}$ will use the following.

9.78 Lemma. *Let $m < 0$ with $m \equiv 2, 3 \pmod{4}$ and m squarefree. Then*

$$\chi_m(n - 2m) = -\chi_m(n)$$

for all $n \in \mathbb{Z}$.

PROOF. We may assume that $n \geq 0$. For n with $\gcd(n, 4m) > 1$ this is trivially the case. So we assume that $\gcd(n, 4m) = 1$. Then for $m \equiv 3 \pmod{4}$:

$$\chi_m(n) = \left(\frac{m}{n}\right) = \left(\frac{-1}{n}\right) \left(\frac{-m}{n}\right) = \chi_{-1}(n) \chi_{-m}(n).$$

and so $\chi_m(n - 2m) = \chi_{-1}(n - 2m) \chi_{-m}(n - 2m) = -\chi_{-1}(n) \chi_{-m}(n) = -\chi_m(n)$. For $m \equiv 2 \pmod{4}$ we put $m = -2m_0$. Then

$$\chi_m(n) = \left(\frac{-2}{n}\right) \left(\frac{m_0}{n}\right) = \chi_{-2}(n) \chi_{m_0}(n).$$

So $\chi_m(n - 2m) = \chi_{-2}(n - 2m) \chi_{m_0}(n - 2m) = -\chi_{-2}(n) \chi_{m_0}(n) = -\chi_m(n)$. \square

9.79 Theorem. *Let $m < 0$ with $m \equiv 2, 3 \pmod{4}$ and m squarefree. Then*

$$h_m = \sum_{n=1}^{-m} \chi_m(n).$$

PROOF. For $m = -1$ the formula is correct. We assume that $m \neq -1$. Then

$$\begin{aligned} \sum_{n=1}^{-4m-1} \chi_m(n)n &= \sum_{n=1}^{-2m-1} \chi_m(n)n + \sum_{n=-2m+1}^{-4m-1} \chi_m(n)n \\ &= \sum_{n=1}^{-2m-1} \chi_m(n)n + \sum_{n=1}^{-2m-1} \chi_m(n-2m)(n-2m) \\ &= \sum_{n=1}^{-2m-1} \chi_m(n)n - \sum_{n=1}^{-2m-1} \chi_m(n)(n-2m) = 2m \sum_{n=1}^{-2m-1} \chi_m(n) \\ &= 2m \left(\sum_{n=1}^{-m-1} \chi_m(n) + \sum_{n=-m+1}^{-2m-1} \chi_m(n) \right) \\ &= 2m \left(\sum_{n=1}^{-m-1} \chi_m(n) - \sum_{n=m+1}^{-1} \chi_m(n) \right) \\ &= 2m \left(\sum_{n=1}^{-m-1} \chi_m(n) + \sum_{n=m+1}^{-1} \chi_m(-n) \right) = 4m \sum_{n=1}^{-m-1} \chi_m(n). \quad \square \end{aligned}$$

Next we look at the case $m \equiv 1 \pmod{4}$.

9.80 Theorem. *Let $m < -3$ with $m \equiv 1 \pmod{4}$ and m squarefree. Then*

$$h_m = \frac{1}{2 - \chi_m(2)} \sum_{n=1}^{\frac{-m-1}{2}} \chi_m(n).$$

PROOF. We have

$$\begin{aligned} \sum_{n=1}^{-m-1} \chi_m(n)n &= \sum_{n=1}^{\frac{-m-1}{2}} \chi_m(2n) \cdot 2n + \sum_{n=1}^{\frac{-m-1}{2}} \chi_m(2n-1)(2n-1) \\ &= 2\chi_m(2) \sum_{n=1}^{\frac{-m-1}{2}} \chi_m(n)n + \sum_{n=\frac{-m+1}{2}}^{-m-1} \chi_m(2n+m)(2n+m) \\ &= 2\chi_m(2) \sum_{n=1}^{-m-1} \chi_m(n)n + m\chi_m(2) \sum_{n=\frac{-m+1}{2}}^{-m-1} \chi_m(n) \\ &= 2\chi_m(2) \sum_{n=1}^{-m-1} \chi_m(n)n - m\chi_m(2) \sum_{n=1}^{\frac{-m-1}{2}} \chi_m(n). \end{aligned}$$

Hence

$$\sum_{n=1}^{-m-1} \chi_m(n)n = \frac{m}{2 - \chi_m(2)} \sum_{n=1}^{\frac{-m-1}{2}} \chi_m(n). \quad \square$$

9.81 Examples.

$$\begin{aligned} h_{-5} &= \chi_{-5}(1) + \chi_{-5}(3) = 1 + 1 = 2, \\ h_{-19} &= \frac{1}{3}(\chi_{-19}(1) + \chi_{-19}(2) + \chi_{-19}(3) + \chi_{-19}(4) + \chi_{-19}(5) + \chi_{-19}(6) \\ &\quad + \chi_{-19}(7) + \chi_{-19}(8) + \chi_{-19}(9)) \\ &= \frac{1}{3}(1 - 1 - 1 + 1 + 1 + 1 + 1 + 1 - 1 + 1) = 1. \end{aligned}$$

Now we have solved the problem on the distribution of quadratic residues mentioned in chapter 3 on page 53 for primes $\equiv 3 \pmod{4}$.

9.82 Corollary. *Let $p \neq 3$ be a prime with $p \equiv 3 \pmod{4}$. Then*

$$\sum_{n=1}^{\frac{p-1}{2}} \left(\frac{n}{p}\right) = \begin{cases} h_{-p} & \text{if } p \equiv 7 \pmod{8}, \\ 3h_{-p} & \text{if } p \equiv 3 \pmod{8}. \end{cases}$$

PROOF. This follows from $\chi_{-p}(n) = \left(\frac{n}{p}\right)$ for all $n \in \mathbb{Z}$. □

Among the numbers $1, \dots, p-1$ there are as many quadratic residues as there are nonquadratic residues. For $p \equiv 3 \pmod{4}$ in the first half of these numbers the quadratic residues outnumber the nonquadratic residues by h_{-p} or $3h_{-p}$, depending on p modulo 8. Note that for this we needed the sign of the quadratic Gauß sum: the Gauß sum is a factor in the class number formula. For $m \equiv 3 \pmod{4}$ we further simplify the class number formula.

9.83 Theorem. *Let $m < 0$ be squarefree and $m \equiv 3 \pmod{4}$. Then*

$$h_m = 2 \cdot \sum_{k=1}^{\frac{-m-1}{4}} \chi_{-m}(k).$$

PROOF.

$$\begin{aligned} h_m &= \sum_{k=1}^{-m-1} \chi_m(k) = \sum_{l=1}^{\frac{-m-1}{2}} \chi_m(2l-1) = \sum_{l=1}^{\frac{-m-1}{2}} \left(\frac{-1}{2l-1}\right) \chi_{-m}(2l-1) \\ &= \sum_{l=1}^{\frac{-m-1}{4}} \left(\frac{-1}{2l-1}\right) \chi_{-m}(2l-1) + \sum_{l=\frac{-m+3}{4}}^{\frac{-m-1}{2}} \left(\frac{-1}{2l-1}\right) \chi_{-m}(2l-1) \\ &= \sum_{l=1}^{\frac{-m-1}{4}} \left(\frac{-1}{2l-1}\right) \chi_{-m}(2l-1) + \sum_{s=1}^{\frac{-m-1}{4}} \left(\frac{-1}{m-2s}\right) \chi_{-m}(2s) \\ &= \sum_{\substack{1 \leq t \leq \frac{-m-1}{2} \\ t \equiv 0,1 \pmod{4}}} \chi_{-m}(t) - \sum_{\substack{1 \leq t \leq \frac{-m-1}{2} \\ t \equiv 2,3 \pmod{4}}} \chi_{-m}(t) = 2 \cdot \sum_{\substack{1 \leq t \leq \frac{-m-1}{2} \\ t \equiv 0,1 \pmod{4}}} \chi_{-m}(t) \\ &= 2 \cdot \left(\sum_{1 \leq a \leq \frac{-m-1}{8}} \chi_{-m}(a) + \sum_{\frac{-m+1}{8} \leq b \leq \frac{-m-1}{4}} \chi_{-m}(b) \right) = 2 \cdot \sum_{k=1}^{\frac{-m-1}{4}} \chi_{-m}(k). \quad \square \end{aligned}$$

Now we have a solution for the problem in chapter 3 for primes $\equiv 1 \pmod{4}$ as well.

9.84 Corollary. *Let p be a prime with $p \equiv 1 \pmod{4}$. Then*

$$\sum_{k=1}^{\frac{p-1}{4}} \left(\frac{k}{p}\right) = \frac{1}{2} h_{-p}.$$

PROOF. This follows from $\chi_p(n) = \left(\frac{n}{p}\right)$ for all $n \in \mathbb{Z}$. □

For primes p with $p \equiv 1 \pmod{4}$ we now have

$$h_{-p} = 2 \cdot \sum_{k=1}^{\frac{p-1}{4}} \binom{k}{p} \equiv 2 \cdot \frac{p-1}{4} \pmod{4}.$$

So $h_{-p} \equiv \frac{p-1}{2} \pmod{4}$. Further note that the 2-rank of $\mathcal{C}(\mathcal{O}_{-p})$ equals 1. For $p \equiv 1 \pmod{8}$ we have $h_{-p} \equiv 0 \pmod{4}$ and for $p \equiv 5 \pmod{8}$ we have $h_{-p} \equiv 2 \pmod{4}$. So for $p \equiv 1 \pmod{8}$ the 2-primary part of $\mathcal{C}(\mathcal{O}_{-p})$ is cyclic of order at least 4. For $p \equiv 5 \pmod{8}$ the 2-primary part of $\mathcal{C}(\mathcal{O}_{-p})$ is of order 2.

9.9 Cyclotomic units

Let $L = \mathbb{Q}(\zeta_m)$ and $K = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$, where $m \in \mathbb{N}^*$ with $m \not\equiv 2 \pmod{4}$ and $m \neq 1$.

9.85 Definition. A $\nu \in \mathcal{O}_L^*$ is called a *cyclotomic unit* if

$$\nu \in \langle -1, \zeta_m, 1 - \zeta_m, 1 - \zeta_m^2, \dots, 1 - \zeta_m^{m-1} \rangle.$$

The group of cyclotomic units in $\mathbb{Q}(\zeta_m)$ is denoted by \mathcal{C}_m and its subgroup of cyclotomic units in K by \mathcal{C}_m^+ .

From now on we assume that in this section m is a prime power, say $m = p^r$ with p a prime. By Theorem 5.51 a fundamental system of units of K is also a fundamental system of units of L . We will show that \mathcal{C}_m^+ is of finite index in \mathcal{O}_K^* .

9.86 Lemma.

$$\mathcal{C}_m = \langle -1, \zeta_m, 1 - \zeta_m^a \mid a \in \mathbb{Z} \setminus p\mathbb{Z} \rangle \cap \mathcal{O}_L^* = \left\langle -1, \zeta_m, \frac{1 - \zeta_m^a}{1 - \zeta_m} \mid a \in \mathbb{Z} \setminus p\mathbb{Z} \right\rangle.$$

PROOF. For $k, b \in \mathbb{N}^*$ with $k < r$ and $p \nmid b$ we have

$$1 - \zeta_m^{bp^k} = \prod_{j=0}^{p^k-1} (1 - \zeta_m^b \zeta_m^{pj}) = \prod_{j=0}^{p^k-1} (1 - \zeta_m^{b+jp^{r-k}}).$$

Because $p \nmid b + jp^{r-k}$, the first identity in the lemma follows from this. For the second identity use the fact that all $1 - \zeta_m^a$ with $p \nmid a$ generate the same ideal of $\mathbb{Z}[\zeta_m]$. \square

9.87 Notation. For $a \in \mathbb{Z} \setminus p\mathbb{Z}$ put

$$\xi_a = \zeta_{2m}^{1-a} \frac{1 - \zeta_m^a}{1 - \zeta_m} = \frac{\zeta_{2m}^a - \zeta_{2m}^{-a}}{\zeta_{2m} - \zeta_{2m}^{-1}} = \frac{\sin \frac{a\pi}{m}}{\sin \frac{\pi}{m}}.$$

9.88 Lemma. *Let $a \in \mathbb{Z} \setminus p\mathbb{Z}$. Then*

$$\xi_a \in \mathcal{C}_m^+, \quad \xi_{a+m} = -\xi_a \quad \text{and} \quad \xi_{-a} = -\xi_a.$$

PROOF. For p odd $\zeta_{2m} \in \langle -1, \zeta_m \rangle \subseteq \mathcal{C}_m$ and for $p = 2$ we have $\zeta_{2m}^{a-1} = \zeta_m^{(a-1)/2}$. So $\xi_a \in \mathcal{C}_m$ and from $\overline{\xi_a} = \xi_a$ follows that $\xi_a \in \mathcal{C}_m^+$. The identity $\xi_{a+m} = -\xi_a$ follows from $\zeta_{2m}^{-m} = -1$ and since $\zeta_{2m}^{-a} - \zeta_{2m}^a = -(\zeta_{2m}^a - \zeta_{2m}^{-a})$, we have $\xi_{-a} = -\xi_a$. \square

9.89 Proposition.

$$\mathcal{C}_m = \langle -1, \zeta_m, \xi_a \mid 1 < a < \frac{m}{2}, p \nmid a \rangle \quad \text{and} \quad \mathcal{C}_m^+ = \langle -1, \xi_a \mid 1 < a < \frac{m}{2}, p \nmid a \rangle.$$

PROOF. The second identity follows from the first. The first is a direct consequence of the Lemmas 9.86 and 9.88. \square

The ξ_a with $1 < a < \frac{m}{2}$ and $p \nmid a$ form a system of $\frac{\varphi(m)}{2} - 1$ units of \mathcal{O}_K^* . We will prove that \mathcal{C}_m^+ is of finite index in \mathcal{O}_K^* by showing that this system has a nonzero regulator. The following lemma on the computation of determinants will be used.

9.90 Lemma. *Let G be a finite abelian group and f a map from G to \mathbb{C} . Then*

- (i) $\det(f(\sigma\tau^{-1}))_{\sigma, \tau \in G} = \prod_{\chi \in G^\vee} \sum_{\sigma \in G} \chi(\sigma) f(\sigma),$
- (ii) $\det(f(\sigma\tau^{-1}) - f(\sigma))_{\substack{\sigma, \tau \in G \\ \sigma, \tau \neq 1}} = \prod_{\substack{\chi \in G^\vee \\ \chi \neq 1}} \sum_{\sigma \in G} \chi(\sigma) f(\sigma),$
- (iii) *if $\sum_{\sigma} f(\sigma) = 0$, then $\det(f(\sigma\tau^{-1}))_{\substack{\sigma, \tau \in G \\ \sigma, \tau \neq 1}} = \frac{1}{\#(G)} \prod_{\substack{\chi \in G^\vee \\ \chi \neq 1}} \sum_{\sigma \in G} \chi(\sigma) f(\sigma).$*

PROOF.

- (i) Consider the \mathbb{C} -linear transformation $T: \mathbb{C}^G \rightarrow \mathbb{C}^G$ defined by

$$T(h)(\tau) = \sum_{\sigma \in G} f(\sigma) h(\sigma\tau) \quad \text{for all } h \in \mathbb{C}^G \text{ and } \tau \in G.$$

On the canonical basis $(e_\sigma)_{\sigma \in G}$, where $e_\sigma(\tau) = \delta_{\sigma, \tau}$, the transformation T acts as follows

$$(Te_\sigma)(\tau) = \sum_{\rho} f(\rho) e_\sigma(\rho\tau) = f(\sigma\tau^{-1}).$$

So the matrix of T on the canonical basis is $(f(\sigma\tau^{-1}))_{\sigma, \tau \in G}$. The transformation T maps a character $\chi \in G^\vee$ to $T(\chi) \in \mathbb{C}^G$ defined by

$$T(\chi)(\tau) = \sum_{\sigma} f(\sigma) \chi(\sigma\tau) = \sum_{\sigma} f(\sigma) \chi(\sigma) \chi(\tau).$$

It follows that χ is an eigenvector of T with eigenvalue $\sum_{\sigma} f(\sigma)\chi(\sigma)$. The characters of G form a basis of \mathbb{C}^G . On this basis the matrix of T is diagonal. Therefore,

$$\det(f(\sigma\tau^{-1}))_{\sigma,\tau \in G} = \det(T) = \prod_{\chi \in G^\vee} \sum_{\sigma \in G} \chi(\sigma)f(\sigma).$$

- (ii) Let V be the linear subspace of \mathbb{C}^G of all h with $\sum_{\sigma} h(\sigma) = 0$. The transformation T induces a transformation T' of V : for $h \in V$ we have

$$\sum_{\tau} T(h)(\tau) = \sum_{\sigma,\tau} f(\sigma)h(\sigma\tau) = \sum_{\sigma,\rho} f(\sigma)h(\rho) = \left(\sum_{\sigma} f(\sigma)\right)\left(\sum_{\rho} h(\rho)\right) = 0.$$

The $e'_\tau = e_\tau - \frac{1}{\#(G)}$ with $\tau \neq 1$ form a basis of V . The matrix of T' on this basis is

$$(f(\sigma\tau^{-1}) - f(\sigma))_{\substack{\sigma,\tau \in G \\ \sigma,\tau \neq 1}}$$

The nontrivial characters form a basis of V . The formula follows from this.

- (iii) Given some ordering on the set $G \setminus \{1\}$, we have the following for determinants of matrices:

$$\begin{aligned} \det(f(\sigma\tau^{-1}) - f(\sigma))_{\substack{\sigma,\tau \in G \\ \sigma,\tau \neq 1}} &= \begin{vmatrix} 1 & 0 & \dots\dots\dots & 0 \\ f(\sigma) & & & \\ \vdots & (f(\sigma\tau^{-1}) - f(\sigma))_{\substack{\sigma,\tau \in G \\ \sigma,\tau \neq 1}} & & \\ f(\sigma) & & & \end{vmatrix} \\ &= \begin{vmatrix} 1 & 1 & \dots\dots & 1 \\ f(\sigma) & & & \\ \vdots & (f(\sigma\tau^{-1}))_{\substack{\sigma,\tau \in G \\ \sigma,\tau \neq 1}} & & \\ f(\sigma) & & & \end{vmatrix} = \begin{vmatrix} \#(G) & 1 & \dots\dots & 1 \\ 0 & & & \\ \vdots & (f(\sigma\tau^{-1}))_{\substack{\sigma,\tau \in G \\ \sigma,\tau \neq 1}} & & \\ 0 & & & \end{vmatrix}. \quad \square \end{aligned}$$

The regulator of the system $(\xi_a)_a$, where the a satisfy $1 < a < \frac{1}{2}p^r$ and $p \nmid a$, is the absolute value of the determinant with entries $\log|\tau(\xi_a)|$ with $\tau \in \text{Gal}(K : \mathbb{Q})$. For these entries we have

$$\begin{aligned} \log|\tau(\xi_a)| &= \log|1 - \tau(\zeta_m)^a| - \log|1 - \tau(\zeta_m)| \\ &= \log|1 - \tau\sigma_a(\zeta_m)| - \log|1 - \tau(\zeta_m)|. \end{aligned}$$

Apply lemma 9.90(ii) to $f(\sigma) = \log|1 - \sigma(\zeta)|$:

$$\begin{aligned} \text{Reg}((\xi_a)_a) &= \text{abs det}(\log|\tau(\xi_a)|)_{a,\tau \neq 1} \\ &= \text{abs det}(\log|1 - \tau(\zeta_m)^a| - \log|1 - \tau(\zeta_m)|)_{a,\tau \neq 1} \end{aligned}$$

$$\begin{aligned}
 &= \text{abs det}(\log|1 - \sigma\tau^{-1}(\zeta_m)| - \log|1 - \sigma(\zeta_m)|)_{\sigma, \tau \neq 1} \\
 &= \text{abs} \prod_{\substack{\chi \in G^\vee \\ \chi \neq 1}} \sum_{\sigma \in G} \chi(\sigma) \log|1 - \sigma(\zeta_m)| \\
 &= \text{abs} \prod_{\substack{\chi \in \mathcal{D}(K) \\ \chi \neq 1}} \sum_{1 \leq a < m/2} \chi(a) \log|1 - \zeta_m^a| \\
 &= \text{abs} \prod_{\substack{\chi \in \mathcal{D}(K) \\ \chi \neq 1}} \frac{1}{2} \sum_1^m \chi(a) \log|1 - \zeta_m^a|.
 \end{aligned}$$

For $N_\chi = p^k$ it follows from

$$1 - \zeta_{p^k}^a = \prod_{t=0}^{p^{r-k}-1} (1 - \zeta_{p^{r-k}}^t \zeta_{p^k}^a) = \prod_{t=0}^{p^{r-k}-1} (1 - \zeta_{p^r}^{t p^k + a})$$

that

$$\sum_1^m \chi(a) \log|1 - \zeta_m^a| = \sum_{a=1}^{p^k} \chi(a) \log|1 - \zeta_{p^k}^a|.$$

For $\chi \in \mathcal{D}(K)$ even and $N_\chi = p^k$ we have by Theorem 9.72

$$L(1, \chi) = -\frac{1}{g(\chi)} \sum_{a=1}^{p^k} \overline{\chi(a)} \log|1 - \zeta_{p^k}^a|$$

and so

$$\sum_{a=1}^{p^k} \log|1 - \zeta_{p^k}^a| = -\overline{g(\bar{\chi})} L(1, \bar{\chi}) = -g(\chi) L(1, \bar{\chi}).$$

Hence

$$\text{Reg}((\xi_a)_a) = \text{abs} \prod_{\substack{\chi \in \mathcal{D}(K) \\ \chi \neq 1}} \frac{1}{2} g(\chi) L(1, \bar{\chi}) \neq 0.$$

This implies that the cyclotomic units in K form a subgroup of \mathcal{O}_K^* of finite index. Since K is totally real, by Theorem 9.53

$$\begin{aligned}
 \text{Reg}((\xi_a)_a) &= \frac{1}{2^{(\varphi(m)/2)-1}} \prod_{\substack{\chi \in \mathcal{D}(K) \\ \chi \neq 1}} |g(\chi)| \cdot \prod_{\substack{\chi \in \mathcal{D}(K) \\ \chi \neq 1}} |L(1, \bar{\chi})| \\
 &= \frac{h(K) \text{Reg}(K)}{\sqrt{\text{disc}(K)}} \cdot \prod_{\chi \in \mathcal{D}(K)} \sqrt{N_\chi}
 \end{aligned}$$

and this can be further simplified using the following proposition.

9.91 Proposition. $\text{disc}(K) = \prod_{\chi \in \mathcal{D}(K)} N_\chi$ and $\text{disc}(L) = (-1)^{\varphi(m)/2} \prod_{\chi \in \mathcal{D}(L)} N_\chi$.

More generally for every abelian number field K

$$|\text{disc}(K)| = \prod_{\chi \in \mathcal{D}(K)} N_\chi.$$

This is the *Conductor-Discriminant Formula* for abelian number fields, a special case of the Conductor-Discriminant Formula for abelian number field extensions. A proof of this formula will be given in chapter 17.

PROOF. The sign of the discriminant is given by Proposition 1.46. In chapter 1 $\text{disc}(K)$ and $\text{disc}(L)$ have been computed (Propositions 1.55 and 1.54):

$$\text{disc}(K) = \begin{cases} (-1)^{\frac{p-1}{2}} p^{\frac{1}{2}(p^{r-1}(pr-r-1)-1)} & \text{if } p \text{ is odd,} \\ 2^{2^{r-2}(r-1)-1} & \text{if } p = 2. \end{cases}$$

and

$$\text{disc}(L) = (-1)^{\varphi(m)/2} p^{p^{r-1}(pr-r-1)}.$$

For $N \in \mathbb{N}^*$ put $a(N) = \#\{\chi \in \mathcal{D} \mid N_\chi = N\}$. Then

$$a(p^k) = \#(\mathcal{D}_{p^k}) - \#(\mathcal{D}_{p^{k-1}}) = \varphi(p^k) - \varphi(p^{k-1}) = \begin{cases} p^{k-2}(p-1)^2 & \text{if } k > 1, \\ p-2 & \text{if } k = 1. \end{cases}$$

For L we have

$$\prod_{\chi \in \mathcal{D}(L)} N_\chi = \prod_{\chi \in \mathcal{D}_m} N_\chi = \prod_{k=1}^r p^{k \cdot a(p^k)} = p^{p-2+(p-1)^2 \sum_{k=2}^r k p^{k-2}} = p^{p^{r-1}(pr-r-1)},$$

where the equality of the exponents of p is easily verified by induction on r . For the field K we need the number of even characters of a given conductor:

$$b(N) = \#\{\chi \in \mathcal{D} \mid N_\chi = N \text{ and } \chi(-1) = 1\}.$$

The number $b(p^k)$ is related to $a(p^k)$ by

$$b(p^k) = \begin{cases} \frac{1}{2}a(p^k) & \text{if } k > 1, \\ \frac{1}{2}(p-3) & \text{if } k = 1 \text{ and } p \text{ odd,} \\ 0 & \text{if } p^k = 2. \end{cases}$$

Now the Conductor-Discriminant Formula for K easily follows from the formula for L . \square

By the formula for $\text{disc}(K)$ we have

$$\text{Reg}((\xi_a)_a) = h(K) \text{Reg}(K)$$

and so we obtain the following remarkable theorem.

9.92 Theorem. $[\mathcal{O}_K^* : \mathcal{C}_{p^r}^+] = h(K)$. □

The abelian groups $\mathcal{O}_K^*/\mathcal{C}_{p^r}^+$ and $\mathcal{A}(K)$ are of the same order. However, it is unknown whether they are isomorphic.

EXERCISES

1. Let p be an odd prime and K the unique abelian number field of degree p . Let \mathfrak{p} be the prime ideal of \mathcal{O}_K above p . There is a unique $t \in \mathbb{N}^*$ such that $V_{K,t+1}(\mathfrak{q}) \neq V_{K,t}(\mathfrak{q})$. Compute t . (This t occurs in the proof of Lemma 9.2. See also exercise 19 of chapter 7.)
2. (i) Describe all characters of C_8 . Which of them are induced by a character of a proper factor group?
(ii) As part (i), but now for the group $C_4 \times C_2$.
3. Let G be a finite abelian group. Show that each character of G is induced by a character of a proper subgroup of G if and only if G is not a cyclic group.
4. Describe a character of $\bigoplus_{i=1}^{\infty} \mathbb{Z}/2$ which is not induced by a character of a proper factor group.
5. Give all Dirichlet pre-characters modulo 7, and also all Dirichlet pre-characters modulo 8, modulo 15 and modulo 24. Write each Dirichlet pre-character χ modulo 24 as a product of Dirichlet pre-characters with a conductor less than N_χ .
6. Determine the conductor of the quadratic Dirichlet character $\chi_{-1}\chi_{-73}$.
7. Determine the number of Dirichlet pre-characters with conductor 260. How many of them are quadratic?
8. Let $m, n \in \mathbb{Z}$ be different and squarefree $\neq 1$. Show that the conductor of $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ is equal to the least common multiple of the conductors of the quadratic number fields $\mathbb{Q}(\sqrt{m})$ and $\mathbb{Q}(\sqrt{n})$.
9. Verify the conductor-discriminant formula for quadratic and biquadratic number fields.
10. Let K be an abelian number field and p a prime number. Show that $p \mid N_K$ if and only if p ramifies.
11. Compute the class number of $\mathbb{Q}(\sqrt{-29})$ using Corollary 9.84.

9 Abelian Number Fields

12. (i) Compute the ideal class group of $\mathbb{Q}(\sqrt{-55})$.
(ii) For how many $n \in \mathbb{N}$ with $1 \leq n \leq 27$ do we have $\chi_{-55}(n) = -1$? Find the answer without computing character values.
13. Let χ be one of the two Dirichlet characters with conductor 5 and of order 4. Compute $|L(1, \chi)|$ using Theorem 9.73.
14. Let χ be one of the two Dirichlet characters with conductor 7 and of order 3. Compute $|L(1, \chi)|$ using Theorem 9.73.
15. Let $K = \mathbb{Q}(\sqrt{-2}, \sqrt{3})$. Compute $h(K) \text{Reg}(K)$ using Example 9.57. Compare with the calculations in Example 5.23 and Example 5.37.
16. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Compute $h(K) \text{Reg}(K)$ using Example 9.58. Compare with the calculations in Example 5.24 and Example 5.38.
17. Prove:

$$\mathbb{Z}[\zeta_9]^* = \langle -1, \zeta_9, 1 + \zeta_9, 1 + \zeta_9^2 \rangle \quad \text{and} \quad \mathbb{Z}[\zeta_9 + \zeta_9^{-1}]^* = \langle -1, \zeta_9 + \zeta_9^{-1}, \zeta_9^2 + \zeta_9^{-2} \rangle.$$

Part II

Class Field Theory

10 Completions of Number Fields

Absolute values on a field determine a metric on the field. So we have the notion of limit of a sequence of elements. Completion yields complete fields. In the proofs of the main theorems of class field theory completions of number fields are often used. There are two types of (nontrivial) absolute values: archimedean and nonarchimedean. For number fields a full classification of absolute values is derived. The archimedean absolute values are essentially the real and pairs of complex embeddings of the number field, the nonarchimedean ones correspond to prime ideals of the ring of integers, or, what amounts to the same, to discrete valuations of the number field. The archimedean absolute values of number fields are thought of corresponding to primes at infinity. This in analogy to fields of algebraic functions, for which all absolute values are nonarchimedean.

10.1 Absolute values

An absolute value on a field determines a ‘distance’ in the field, the absolute value being the distance to 0. It satisfies a triangle inequality with respect to addition and it respects multiplication.

10.1 Definitions. Let K be a field. A function $\|\cdot\|: K \rightarrow \mathbb{R}$ is called an *absolute value* on K if

- (AV1) $\|x\| \geq 0$ for all $x \in K$,
- (AV2) $\|x\| = 0 \iff x = 0$ for all $x \in K$,
- (AV3) $\|xy\| = \|x\| \cdot \|y\|$ for all $x, y \in K$,
- (AV4) $\|x + y\| \leq \|x\| + \|y\|$ for all $x, y \in K$.

The pair $(K, \|\cdot\|)$ is called a *valued field*. An *embedding* $\sigma: (K, \|\cdot\|) \rightarrow (L, \|\cdot\|)$ of valued fields is a field embedding $\sigma: K \rightarrow L$ which respects the absolute value: $\|\sigma(x)\| = \|x\|$ for all $x \in K$.

Usually, when we call K a valued field, the absolute value on K is understood and $\|\cdot\|$ will be used as a standard notation for this absolute value.

Note that (AV2) implies that an absolute value $\|\cdot\|: K \rightarrow \mathbb{R}$ can be restricted to a map $\|\cdot\|: K^* \rightarrow \mathbb{R}^*$ and so by (AV3) this map is a group homomorphism.

10.2 Examples.

1. The ‘ordinary’ absolute value $|\cdot|$ on \mathbb{Q} , \mathbb{R} and \mathbb{C} .
2. An embedding $\sigma: K \rightarrow \mathbb{C}$ determines an absolute value $\|\cdot\|_\sigma$ on the field K :

$$\|x\|_\sigma = |\sigma(x)| \quad \text{for all } x \in K.$$

Since $|\overline{\sigma(x)}| = |\sigma(x)|$, the absolute values $\|\cdot\|_\sigma$ and $\|\cdot\|_{\bar{\sigma}}$ are equal.

3. Let v be a discrete valuation of a field K . It determines an absolute value on K in the following way. Fix some $c \in \mathbb{R}$ with $0 < c < 1$. Then an absolute value $\|\cdot\|_v$ on K is defined by

$$\|x\|_v = c^{v(x)}.$$

(It is understood that $v(0) = \infty$ and accordingly $\|0\|_v = 0$.) Here a stronger version of (AV4) holds:

$$\|x + y\|_v \leq \max(\|x\|_v, \|y\|_v).$$

4. Let R be a Dedekind domain and K the field of fractions of R . A maximal ideal \mathfrak{p} of R determines a discrete valuation $v_{\mathfrak{p}}$ of K and so, by the previous example, also an absolute value on K . This absolute value is denoted by $\|\cdot\|_{\mathfrak{p}}$. The absolute value $\|\cdot\|_{\mathfrak{p}}$ is called the \mathfrak{p} -adic absolute value on K .
5. For a number field K and $\mathfrak{p} \in \text{Max}(\mathcal{O}_K)$ one usually takes $c = \frac{1}{N(\mathfrak{p})}$ in the previous example. Thus in particular for $K = \mathbb{Q}$ and p a prime number:

$$\|x\|_p = p^{-v_p(x)}.$$

6. Every field K has a *trivial* absolute value:

$$\|x\| = \begin{cases} 1 & \text{if } x \neq 0, \\ 0 & \text{if } x = 0. \end{cases}$$

There are no interesting absolute values on finite fields:

10.3 Proposition. *Let $\|\cdot\|$ be an absolute value on a finite field K . Then $\|\cdot\|$ is the trivial absolute value.*

PROOF. For all $x \in K^*$ the value $\|x\| \in \mathbb{R}^*$ is of finite order and positive. □

An absolute value $\|\cdot\|$ on a field K determines a metric d on K :

$$d(x, y) = \|x - y\|.$$

This metric defines a topology on K . Absolute values are considered to be equivalent if they induce the same topology. This comes down to: $\|\cdot\|_1$ and $\|\cdot\|_2$ are equivalent if

$$\|x\|_1 < \|y\|_1 \iff \|x\|_2 < \|y\|_2$$

and by (AV2) and (AV3) we can reduce this to the following definition.

10.4 Definition. Let $\|\cdot\|_1$ and $\|\cdot\|_2$ be absolute values on a field K . Then $\|\cdot\|_1$ and $\|\cdot\|_2$ are called *equivalent* if:

$$\|x\|_1 < 1 \iff \|x\|_2 < 1 \quad \text{for all } x \in K.$$

An equivalence class of nontrivial absolute values on a field K is called a *place* of K .

A trivial absolute value determines the discrete topology and this absolute value is only equivalent to itself.

10.5 Proposition. Let $\|\cdot\|_1$ and $\|\cdot\|_2$ be equivalent nontrivial absolute values on a field K . Then there exists a positive real number a such that

$$\|x\|_1^a = \|x\|_2 \quad \text{for all } x \in K.$$

PROOF. Fix a $y \in K$ such that $\|y\|_1 > 1$. We can do so because $\|\cdot\|_1$ is nontrivial. If there exists an a as asserted, then necessarily

$$a = \frac{\log \|y\|_2}{\log \|y\|_1}.$$

We will show that the proposition holds for this a . Let $x \in K^*$. Then $\|x\|_1 = \|y\|_1^b$ for some $b \in \mathbb{R}$. Now choose a monotone decreasing sequence $\frac{m_i}{n_i}$ ($i = 1, 2, 3, \dots$) in \mathbb{Q} , where $m_i \in \mathbb{Z}$, $n_i \in \mathbb{N}^*$ and such that $\lim_{i \rightarrow \infty} \frac{m_i}{n_i} = b$. Then

$$\|x\|_1 = \|y\|_1^b < \|y\|_1^{m_i/n_i} \quad \text{for all } i.$$

Hence

$$\left\| \frac{x^{n_i}}{y^{m_i}} \right\|_1 < 1 \quad \text{for all } i$$

and, because the absolute values are equivalent, also

$$\left\| \frac{x^{n_i}}{y^{m_i}} \right\|_2 < 1 \quad \text{for all } i,$$

or equivalently

$$\|x\|_2 < \|y\|_2^{m_i/n_i} \quad \text{for all } i$$

and this implies

$$\|x\|_2 \leq \|y\|_2^b.$$

Similarly, using an ascending sequence in \mathbb{Q} , we have $\|x\|_2 \geq \|y\|_2^b$. Hence

$$a = \frac{\log\|y\|_2}{\log\|y\|_1} = \frac{\log\|x\|_2}{\log\|x\|_1} \quad \text{for all } x \in K^*,$$

and so $\|x\|_1^a = \|x\|_2$ for all $x \in K$. □

The \mathfrak{p} -adic absolute value on the field of fractions of a Dedekind domain satisfies a stronger version of the triangle inequality. This property depends only on the behavior of the absolute value on the least subring of the field:

10.6 Proposition. *Let $\|\cdot\|$ be a nontrivial absolute value on a field K . Then the following are equivalent:*

- a) $\|n \cdot 1\| \leq 1$ for all $n \in \mathbb{Z}$;
- b) there is an $n \in \mathbb{N}$ with $n \geq 2$ such that $\|n \cdot 1\| \leq 1$;
- c) $\|x + y\| \leq \max(\|x\|, \|y\|)$ for all $x, y \in K$.

PROOF.

a) \Rightarrow b) Trivial.

b) \Rightarrow a) Suppose that some $n \geq 2$ satisfies $\|n \cdot 1\| \leq 1$. Let $m \in \mathbb{N}^*$ and represent m n -adically:

$$m = a_0 + a_1n + a_2n^2 + \cdots + a_rn^r$$

with $a_i \in \mathbb{N}$, $a_i < n$ and $a_r \neq 0$. For all $a \in \mathbb{N}$ with $a < n$ we have

$$\|a \cdot 1\| = \|\overbrace{1 + \cdots + 1}^a\| \leq \|\overbrace{1 + \cdots + 1}^a\| = a < n.$$

So

$$\|m \cdot 1\| \leq \|a_0 \cdot 1\| + \|a_1 \cdot 1\| \|n \cdot 1\| + \cdots + \|a_r \cdot 1\| \|n \cdot 1\|^r \leq n(r + 1).$$

Since $n^r \leq m$, we have $r \leq \frac{\log m}{\log n}$ and so for all $m \in \mathbb{N}^*$:

$$\|m \cdot 1\| \leq n \left(1 + \frac{\log m}{\log n} \right).$$

Replace m by m^s , where $s \in \mathbb{N}^*$:

$$\|m \cdot 1\|^s \leq n \left(1 + \frac{s \log m}{\log n} \right) \quad \text{for all } s, m \in \mathbb{N}^*.$$

Hence

$$\|m \cdot 1\| \leq \sqrt[s]{n} \cdot \sqrt[s]{1 + s \frac{\log m}{\log n}} \rightarrow 1 \quad \text{if } s \rightarrow \infty.$$

Therefore,

$$\|m \cdot 1\| \leq 1 \quad \text{for all } m \in \mathbb{N}^*$$

and thereby for all $m \in \mathbb{Z}$ as well.

c) \Rightarrow a) This follows from

$$\|n \cdot 1\| = \|1 + \cdots + 1\| \leq \|1\| = 1 \quad \text{for all } n \in \mathbb{N}^*.$$

a) \Rightarrow c) We may assume that $\|x\| \geq \|y\|$. Then to prove that $\|x + y\| \leq \|x\|$. For all $n \in \mathbb{N}^*$ we have

$$\begin{aligned} \|x + y\|^n &= \|(x + y)^n\| = \left\| \sum_{k=0}^n \binom{n}{k} x^{n-k} y^k \right\| \leq \sum_{k=0}^n \binom{n}{k} \|x\|^{n-k} \|y\|^k \\ &\leq \sum_{k=0}^n \|x\|^{n-k} \|y\|^k \leq (n+1) \|x\|^n. \end{aligned}$$

So for all $n \in \mathbb{N}^*$ we have $\|x + y\| \leq \sqrt[n]{n+1} \cdot \|x\|$, which implies $\|x + y\| \leq \|x\|$, because $\lim_{n \rightarrow \infty} \sqrt[n]{n+1} = 1$. \square

10.7 Definition. An absolute value $\|\cdot\|$ on a field K is called *archimedean* if there is an $n \in \mathbb{N}^*$ such that $\|n \cdot 1\| > 1$. An absolute value $\|\cdot\|$ is called *nonarchimedean* if it is nontrivial and $\|n \cdot 1\| \leq 1$ for all $n \in \mathbb{Z}$. A place of K is called (non)archimedean if it consists of (non)archimedean absolute values.

Thus we have three types of absolute values: trivial, archimedean and nonarchimedean.

The field \mathbb{Q} has a unique archimedean place:

10.8 Theorem. Let $\|\cdot\|$ be an archimedean absolute value on \mathbb{Q} . Then $\|\cdot\|$ is equivalent to the ordinary absolute value $|\cdot|$ on \mathbb{Q} .

PROOF. By Proposition 10.6 we have $\|n\| > 1$ for all $n \geq 2$. Let m, n be integers ≥ 2 . Represent m n -adically:

$$m = a_0 + a_1 n + a_2 n^2 + \cdots + a_r n^r \quad \text{with } 0 \leq a_i < n \text{ and } a_r \neq 0.$$

Then

$$\|m\| \leq n(1 + \|n\| + \cdots + \|n\|^r) \leq n(r+1)\|n\|^r \leq n \left(1 + \frac{\log m}{\log n}\right) \|n\|^{\frac{\log m}{\log n}}.$$

Replace m by m^s , where $s \in \mathbb{N}^*$:

$$\|m\| \leq \sqrt[s]{n} \cdot \sqrt[s]{1 + \frac{s \log m}{\log n}} \cdot \|n\|^{\frac{\log m}{\log n}} \rightarrow \|n\|^{\frac{\log m}{\log n}} \quad \text{if } s \rightarrow \infty.$$

Hence

$$\|m\|^{\frac{1}{\log m}} \leq \|n\|^{\frac{1}{\log n}} \quad \text{for all } m, n \geq 2$$

and so by symmetry

$$\|m\|^{\frac{1}{\log m}} = \|n\|^{\frac{1}{\log n}} \quad \text{for all } m, n \geq 2.$$

So there is an $a \in \mathbb{R}$ such that $\|n\|^{\frac{1}{\log n}} = e^a$ for all $n \geq 2$, that is

$$\|n\| = e^{a \log n} = n^a \quad \text{for all } n \geq 2.$$

It follows that $\|x\| = |x|^a$ for all $x \in \mathbb{Q}$. □

In section 10.3 a classification of the archimedean places of a number field will be derived: they correspond to real and (pairs of) complex embeddings of the number field. In this section we derive a classification of the nonarchimedean places of a number field. For discrete valuations we have the notion of discrete valuation ring. More generally, we have for a nonarchimedean absolute value a valuation ring:

10.9 Proposition. *Let $\|\cdot\|$ be a nonarchimedean absolute value on a field K . Then*

$$R = \{x \in K \mid \|x\| \leq 1\}$$

is a local ring with

$$\mathfrak{m} = \{x \in K \mid \|x\| < 1\}$$

as its maximal ideal.

PROOF. From Proposition 10.6 follows that R is a subring of K and also that \mathfrak{m} is an ideal of R . Clearly $R \setminus \mathfrak{m} = \{x \in K \mid \|x\| = 1\} = R^*$ and this implies that R is a local ring with maximal ideal \mathfrak{m} . □

10.10 Definition. Let $\|\cdot\|$ be a nonarchimedean absolute value on a field K . The the local ring R described in Proposition 10.9 is called the *valuation ring* of $\|\cdot\|$.

10.11 Proposition. *Let $\|\cdot\|$ be a nonarchimedean absolute value on a number field K . Then $\|\cdot\|$ is equivalent to the \mathfrak{p} -adic absolute value $\|\cdot\|_{\mathfrak{p}}$ for some $\mathfrak{p} \in \text{Max}(\mathcal{O}_K)$.*

PROOF. Consider

$$R = \{x \in K \mid \|x\| \leq 1\} \quad \text{and} \quad \mathfrak{m} = \{x \in K \mid \|x\| < 1\}.$$

By Proposition 10.9 R is a local ring with maximal ideal \mathfrak{m} .

First we prove that $\mathcal{O}_K \subseteq R$. Choose a \mathbb{Z} -basis $(\alpha_1, \dots, \alpha_n)$ of \mathcal{O}_K . Then for $a_1, \dots, a_n \in \mathbb{Z}$:

$$\|a_1\alpha_1 + \dots + a_n\alpha_n\| \leq \max_i \|a_i\alpha_i\| \leq \max_i \|a_i\|.$$

It follows that the set $\{\|\alpha\| \mid \alpha \in \mathcal{O}_K\}$ is a bounded and multiplicatively closed subset of $\mathbb{R}^{\geq 0}$. So this subset is contained in $[0, 1]$. This means that $\mathcal{O}_K \subseteq R$.

Put $\mathfrak{p} = \mathcal{O}_K \cap \mathfrak{m}$. Then \mathfrak{p} is a prime ideal of \mathcal{O}_K . Also the localization $(\mathcal{O}_K)_{\mathfrak{p}}$ is contained in R : for $\alpha \in \mathcal{O}_K$ and $\beta \in \mathcal{O}_K \setminus \mathfrak{p}$ we have $\|\frac{\alpha}{\beta}\| = \|\alpha\| \leq 1$, since $\beta \in R \setminus \mathfrak{m}$. The prime ideal \mathfrak{p} of \mathcal{O}_K differs from the zero ideal, since otherwise $(\mathcal{O}_K)_{\mathfrak{p}} = K$ and this would imply that the absolute value is trivial.

Now choose $\pi \in \mathcal{O}_K$ with $v_{\mathfrak{p}}(\pi) = 1$. It follows from $(\mathcal{O}_K)_{\mathfrak{p}}^* \subseteq R^* = R \setminus \mathfrak{m}$ that for all $\alpha \in K^*$

$$\|\alpha\| = \|\alpha\pi^{-v_{\mathfrak{p}}(\alpha)}\| \|\pi\|^{v_{\mathfrak{p}}(\alpha)} = \|\pi\|^{v_{\mathfrak{p}}(\alpha)}.$$

Since also

$$\|\alpha\|_{\mathfrak{p}} = \|\pi\|_{\mathfrak{p}}^{v_{\mathfrak{p}}(\alpha)},$$

we have $\|\alpha\|^c = \|\alpha\|_{\mathfrak{p}}$ for all $\alpha \in K^*$, where c is determined by $\|\pi\|^c = \|\pi\|_{\mathfrak{p}}$. \square

Now it follows easily that we have a classification of the nonarchimedean places of a number field.

10.12 Theorem. *Let K be a number field. Then the map $\mathfrak{p} \mapsto \text{class of } \|\cdot\|_{\mathfrak{p}}$ from $\text{Max}(\mathcal{O}_K)$ to the set of nonarchimedean places of K is a bijection.*

PROOF. By Proposition 10.11 the map is surjective. For injectivity, let $\mathfrak{p}_1, \mathfrak{p}_2 \in \text{Max}(\mathcal{O}_K)$ with $\mathfrak{p}_1 \neq \mathfrak{p}_2$. Then there is an $\alpha \in \mathfrak{p}_1 \setminus \mathfrak{p}_2$. This implies $\|\alpha\|_{\mathfrak{p}_1} \neq 0$ and $\|\alpha\|_{\mathfrak{p}_2} = 0$. \square

So for \mathbb{Q} we have now a classification of its places.

10.13 Theorem (Ostrowski). *The nontrivial places of \mathbb{Q} are its archimedean place and the p -adic places, one for each prime p .* \square

10.2 Completions

An absolute valuation on a field K determines a metric on K and there is a standard way to complete the metric space. Since the metric comes from an absolute value, the completion will be a field as well.

10.14 Definitions. Let K be a field with an absolute value $\|\cdot\|$ on K . A sequence (a_n) in K is called a *Cauchy sequence* with respect to $\|\cdot\|$ if for each $\varepsilon > 0$ there is an $N \in \mathbb{N}$ such that $\|a_m - a_n\| < \varepsilon$ for all $m, n \geq N$. The sequence is said to *converge* to $a \in K$ if for each $\varepsilon > 0$ there is an $N \in \mathbb{N}$ such that $\|a - a_n\| < \varepsilon$ for all $n > N$, that is if $\lim_{n \rightarrow \infty} \|a - a_n\| = 0$. If a sequence (a_n) converges to a , the (necessarily unique) element a is called the *limit* of the sequence; notation: $a = \lim_{n \rightarrow \infty} a_n$. Sequences converging to 0 are called *null sequences*.

As is well-known, converging sequences are Cauchy sequences, but not necessarily visa versa.

10.15 Definition. Let K be a field with an absolute value $\|\cdot\|$. Then K is called *complete* (w.r.t. $\|\cdot\|$) if every Cauchy sequence with respect to $\|\cdot\|$ in K converges.

10.16 Definition. The *completion* of a valued field K is an embedding $\iota: K \rightarrow \hat{K}$ of the valued field K into a complete valued field \hat{K} such that for each valued field embedding $\sigma: K \rightarrow L$ with L complete there is a unique valued field embedding $\hat{\sigma}: \hat{K} \rightarrow L$ such that the diagram

$$\begin{array}{ccc}
 K & \xrightarrow{\iota} & \hat{K} \\
 \sigma \searrow & & \swarrow \hat{\sigma} \\
 & L &
 \end{array}$$

commutes.

This definition of the completion is a definition by a universal construction. The completion is thus defined up to a canonical isomorphism. Such a definition guarantees uniqueness, but not existence. For the existence usually an explicit construction is needed.

10.17 Construction of the completion of a valued field. Let K be a valued field, \mathfrak{C} the set of Cauchy sequences in K and \mathfrak{N} the set of null sequences in K . By standard arguments we see that \mathfrak{C} is a ring under termwise operations and \mathfrak{N} is an ideal of \mathfrak{C} , in fact a maximal ideal: a Cauchy sequence which is not a null sequence is modulo \mathfrak{N} congruent to an invertible Cauchy sequence. Define \hat{K} to be the field $\mathfrak{C}/\mathfrak{N}$. Let's write the class of a Cauchy sequence (a_n) temporarily as $[(a_n)]$. The embedding $\iota: K \rightarrow \hat{K}$ is defined by sending $a \in K$ to the class of the constant sequence (a) , so $\iota(a) = [(a)]$. The absolute value $\|\cdot\|$ is extended to \hat{K} by

$$\|[(a_n)]\| = \lim_{n \rightarrow \infty} \|a_n\|.$$

Note that the $\|a_n\|$ form a Cauchy sequence in the complete valued field \mathbb{R} . We now have an embedding $\iota: K \rightarrow \hat{K}$ of valued fields. It remains to prove that \hat{K} is complete and that $\iota: K \rightarrow \hat{K}$ satisfies the definition of completion.

10.18 Proposition. *Let K be a valued field. Then the valued field \hat{K} as constructed in 10.17 is complete.*

PROOF. Let $(a_n)_n$ be a Cauchy sequence in K . Then for each $\varepsilon > 0$ there is an N such that $\|a_m - a_n\| \leq \varepsilon$ for all $m, n \geq N$. Let $\alpha = [(a_n)] \in \hat{K}$. For fixed m we have $[(a_m - a_n)_n] = \iota(a_m) - \alpha$. So $\|\iota(a_m) - \alpha\| < \varepsilon$ for each $m \geq N$. This means that the sequence $(\iota(a_m)_m)$ converges to α .

Now let $(\alpha_n)_n$ be a Cauchy sequence in \hat{K} . For each n choose a $b_n \in K$ such that $\|\alpha_n - \iota(b_n)\| < \frac{1}{n}$. Then $(b_n)_n$ is a Cauchy sequence in K and it follows that the sequence $(\alpha_n)_n$ converges to $[(b_n)_n] \in \hat{K}$. \square

10.19 Theorem. *Let K be a valued field. Then $\iota: K \rightarrow \hat{K}$ as defined in 10.17 is a completion of K .*

PROOF. Let L be a complete valued field and $\sigma: K \rightarrow L$ an embedding of valued fields. Then define an embedding $\hat{\sigma}: \hat{K} \rightarrow L$ as follows. Let (a_n) be a Cauchy sequence in K . Then $(\sigma(a_n))$ is a Cauchy sequence in L . Since L is complete, this sequence converges to an element $\beta \in L$. Define $\hat{\sigma}(\alpha)$, where $\alpha = [(a_n)]$, to be β . One easily verifies that $\hat{\sigma}$ is an embedding of valued fields. \square

So each valued field has a completion and since equivalent absolute values determine the same completion, the completions of a field K correspond to the places of K .

We will often identify a valued field K with its image in \hat{K} . Thus, \hat{K} is a complete valued field and its elements are limits of Cauchy sequences in K : for each α there is a sequence (a_n) in K such that

$$\alpha = \lim_{n \rightarrow \infty} a_n$$

and such sequences differ by a null sequence.

10.3 Complete archimedean fields

Theorem 10.12 classifies the nonarchimedean places of a number field. The classification of the archimedean places of a number field follows from another theorem of Ostrowski (Theorem 10.21) which states that \mathbb{R} and \mathbb{C} are essentially the only complete archimedean fields.

10.20 Lemma. *Let $\|\cdot\|$ be an absolute value on \mathbb{C} , whose restriction to \mathbb{R} is equivalent to the absolute value $|\cdot|$ on \mathbb{R} . Then $\|\cdot\|$ is equivalent to the absolute value $|\cdot|$ on \mathbb{C} .*

PROOF. There is a $c > 0$ such that $\|a\| = |a|^c$ for all $a \in \mathbb{R}$. We will prove that $\|\alpha\| = |\alpha|^c$ for all $\alpha \in \mathbb{C}$. From $i^2 = -1$ it follows that $\|i\| = 1$. For $\alpha = a + bi \in \mathbb{C}$ with $a, b \in \mathbb{R}$ we have

$$\|\alpha\| = \|a + bi\| \leq \|a\| + \|b\| = |a|^c + |b|^c \leq |\alpha|^c + |\alpha|^c = 2|\alpha|^c.$$

For $\alpha \in \mathbb{C}^*$ put $f(\alpha) = \|\alpha\|/|\alpha|^c$. Then $0 < f(\alpha) \leq 2$. For a fixed $\alpha \in \mathbb{C}^*$ we then have for all $n \in \mathbb{N}^*$: $f(\alpha)^n = f(\alpha^n) \leq 2$, and so $f(\alpha) \leq \sqrt[n]{2}$. Hence $f(\alpha) \leq 1$. Since $f(\alpha^{-1}) = f(\alpha)^{-1}$, also $f(\alpha) \geq 1$. Therefore, $f(\alpha) = 1$. It follows that $\|\alpha\| = |\alpha|^c$ for all $\alpha \in \mathbb{C}^*$. \square

10.21 Theorem (Ostrowski). *Let K be a field, complete with respect to an archimedean absolute value $\|\cdot\|$ on K . Then $K \cong \mathbb{R}$ or $K \cong \mathbb{C}$ and $\|\cdot\|$ is equivalent to the ordinary absolute value $|\cdot|$ on \mathbb{R} or \mathbb{C} .*

PROOF. Since $\|\cdot\|$ is archimedean, K is of characteristic 0. So we can assume that \mathbb{Q} is a subfield of K . The restriction of $\|\cdot\|$ to \mathbb{Q} is an archimedean absolute value on \mathbb{Q} and is, by Theorem 10.8, equivalent to the ordinary absolute value on \mathbb{Q} . Since K is complete we can assume, by the universal property for completions, that \mathbb{R} is a subfield of K and that the restriction of $\|\cdot\|$ to \mathbb{R} is equivalent to the ordinary absolute value on \mathbb{R} .

We will show that each $\alpha \in K$ is the zero of a polynomial over \mathbb{R} of degree 2. If $\alpha \in \mathbb{R}$ for all $\alpha \in K$, then $K = \mathbb{R}$. Otherwise there is an α such that $K = \mathbb{R}(\alpha) = \mathbb{C}$ and by Lemma 10.20 the absolute value $\|\cdot\|$ is equivalent to the ordinary absolute value on \mathbb{C} .

Let $\alpha \in K$. Consider the function

$$\psi: \mathbb{C} \rightarrow \mathbb{R}, \quad z \mapsto \|\alpha^2 + (z + \bar{z})\alpha + z\bar{z}\|.$$

This is a continuous function and $\lim_{z \rightarrow \infty} \psi(z) = \infty$. It follows that the subset $\{\psi(z) \mid z \in \mathbb{C}\}$ of \mathbb{R} has a least element $a \geq 0$. If $a = 0$, then α is a zero of a polynomial over \mathbb{R} of degree 2.

Suppose $a > 0$ and let $\varepsilon \in \mathbb{R}$ with $\|\varepsilon\| = \frac{a}{2}$. Let $A = \{z \in \mathbb{C} \mid \psi(z) = a\} = \psi^{-1}(a)$. This is a nonempty compact subset of \mathbb{C} . Take $z_0 \in A$ with $|z_0|$ maximal. Consider the following polynomials over \mathbb{R} :

$$\begin{aligned} f(X) &= X^2 + (z_0 + \bar{z}_0)X + z_0\bar{z}_0 + \varepsilon, \\ g(X) &= (f(X) - \varepsilon)^n - (-\varepsilon)^n. \end{aligned}$$

Since $\text{disc}(f) = (z_0 + \bar{z}_0)^2 - 4z_0\bar{z}_0 - 4\varepsilon = (z_0 - \bar{z}_0)^2 - 4\varepsilon \leq -4\varepsilon < 0$, the zeros of f are not real. Let $w \in \mathbb{C}$ such that $f(w) = 0$, then the other zero of f is \bar{w}

and $w\bar{w} = z_0\bar{z}_0 + \varepsilon$. So $|w| > |z_0|$. Therefore, $w \notin A$, that is $\psi(w) > a$. Put $g(X) = \prod_{i=1}^{2n} (X - w_i)$ with $w_1, \dots, w_{2n} \in \mathbb{C}$ and $w_1 = w$. Then

$$\begin{aligned} \|g(\alpha)\|^2 &= \left(\prod_{i=1}^{2n} \|\alpha - w_i\| \right)^2 = \prod_{i=1}^{2n} \|\alpha - w_i\| \cdot \prod_{i=1}^{2n} \|\alpha - \bar{w}_i\| \\ &= \prod_{i=1}^{2n} \|(\alpha - w_i)(\alpha - \bar{w}_i)\| = \prod_{i=1}^{2n} \psi(w_i) = \psi(w) \prod_{i=2}^{2n} \psi(w_i) \geq \psi(w) a^{2n-1} \end{aligned}$$

and

$$\|g(\alpha)\| \leq \|f(\alpha) - \varepsilon\|^n + \|\varepsilon\|^n = \psi(z_0)^n + \|\varepsilon\|^n = a^n + \frac{a^n}{2^n} = a^n \left(1 + \frac{1}{2^n}\right).$$

It follows that

$$1 < \frac{\psi(w)}{a} \leq \frac{\|g(\alpha)\|^2}{a^{2n}} \leq \left(1 + \frac{1}{2^n}\right)^2$$

for all $n \in \mathbb{N}^*$. Contradiction. \square

10.22 Corollary. *Let $\|\cdot\|$ be an archimedean absolute value on a number field K . Then there is an embedding $\sigma: K \rightarrow \mathbb{C}$ such that $\|\cdot\|$ is equivalent to the absolute value $K \rightarrow \mathbb{R}$, $\alpha \mapsto |\sigma(\alpha)|$.*

PROOF. Let $\iota: K \rightarrow \hat{K}$ be a completion of the valued field K . Then \hat{K} is a complete archimedean valued field. So either there is an isomorphism $\tau: \hat{K} \xrightarrow{\sim} \mathbb{R}$ or an isomorphism $\tau: \hat{K} \xrightarrow{\sim} \mathbb{C}$. Hence the absolute value $\|\cdot\|$ on K is equivalent to $\alpha \mapsto |\tau(\alpha)|$. \square

So the archimedean places of a number field K are the places represented by the archimedean absolute values described in the second item of Examples 10.2.

10.4 Primes of a number field

For a number field K we have a classification of its places:

- a) Nonarchimedean places represented by $\|\cdot\|_{\mathfrak{p}}$, where $\mathfrak{p} \in \text{Max}(\mathcal{O}_K)$ (Theorem 10.12).
- b) Archimedean places represented by $\|\cdot\|_{\sigma}$, where σ is a real or complex embedding (Corollary 10.22).

Number fields have much in common with finite extensions of the field $k(T)$ of rational functions over a finite field k . The field $k(T)$ is the field of fractions of the polynomial ring $k[T]$, which is a Euclidean domain. Places of $k(T)$ correspond to the discrete valuations of $k(T)$. There is one discrete valuation on $k(T)$ which does not come from a prime ideal of $k[T]$: the valuation v_{∞} given by $v_{\infty}(f) = -\deg(f)$,

see exercise 2 of chapter 6. The field $k(T)$ is the field of fractions of $k[\frac{1}{T}]$ as well and the valuation v_∞ comes from the prime ideal $(\frac{1}{T})$. The ‘infinite’ places for this type of function fields are not of a special kind. For number fields, however, the situation is different. Their archimedean places are thought of being infinite places of the number field. More on the places of a function field $k(T)$ in the exercises 1–5. For another example, the function field of rational functions on a circle, see exercise 6.

10.23 Definitions and notations. Places of a number field are called *primes* of the number field. The nonarchimedean places are called *finite* primes and the archimedean ones *infinite* primes. The infinite prime determined by a real or complex embedding σ will be denoted by \mathfrak{p}_σ . It is called a *real* infinite prime if σ is a real embedding and a *complex* infinite prime if σ is a complex embedding. The collection of primes of a number field K will be denoted by $\mathcal{P}(K)$. It is the disjoint union of $\mathcal{P}_0(K)$, the collection of finite primes, and $\mathcal{P}_\infty(K)$, the collection of infinite primes of K . Each $\mathfrak{p} \in \mathcal{P}(K)$ comes with an embedding $\sigma_\mathfrak{p}: K \rightarrow K_\mathfrak{p}$, where $K_\mathfrak{p}$ is the completion of K with respect to \mathfrak{p} . It is customary to refer to nonzero prime ideals as being finite primes, although formally a finite prime is an equivalence class of absolute values. For $\mathfrak{p} \in \mathcal{P}_\infty(K)$ we always take $K_\mathfrak{p}$ to be either \mathbb{R} or \mathbb{C} . For a complex infinite prime \mathfrak{p} the embedding $\sigma_\mathfrak{p}: K \rightarrow \mathbb{C}$ is one of the corresponding pair of embeddings. For finite primes \mathfrak{p} we choose

$$\|\alpha\|_\mathfrak{p} = \frac{1}{N(\mathfrak{p})^{v_\mathfrak{p}(\alpha)}},$$

see Examples 10.2. We also use the notation $\|\cdot\|_\mathfrak{p}$ for infinite primes \mathfrak{p} . For $\alpha \in K$ the real number $\|\alpha\|_\mathfrak{p}$ is defined as follows

$$\|\alpha\|_\mathfrak{p} = \begin{cases} \|\alpha\|_{\sigma_\mathfrak{p}} & \text{if } \mathfrak{p} \text{ is real,} \\ \|\alpha\|_{\sigma_\mathfrak{p}}^2 & \text{if } \mathfrak{p} \text{ is complex.} \end{cases}$$

Note that for \mathfrak{p} a complex infinite prime $\|\cdot\|_\mathfrak{p}$ is not an absolute value; however, its square root is one. The choices for the $\|\cdot\|_\mathfrak{p}$ are such that the following *product formula* holds.

10.24 Proposition. *Let K be a number field and $\alpha \in K$. Then*

$$\prod_{\mathfrak{p}} \|\alpha\|_\mathfrak{p} = 1,$$

where the product is over all primes \mathfrak{p} of K .

PROOF. Since $\|\alpha\|_\mathfrak{p} \neq 1$ for only a finite number of primes \mathfrak{p} , the infinite product makes sense. The product over the infinite primes:

$$\prod_{\mathfrak{p} \text{ infinite}} \|\alpha\|_\mathfrak{p} = \prod_{\mathfrak{p} \text{ real}} |\sigma_\mathfrak{p}(\alpha)| \cdot \prod_{\mathfrak{p} \text{ complex}} |\sigma_\mathfrak{p}(\alpha)|^2 = \prod_{\sigma} |\sigma(\alpha)| = |N_{\mathbb{Q}}^K(\alpha)|,$$

where the last product is over all embeddings of K in \mathbb{C} . This product is the inverse of the product over the finite primes:

$$\begin{aligned} \prod_{\mathfrak{p} \text{ finite}} \|\alpha\|_{\mathfrak{p}} &= \prod_{\mathfrak{p} \in \text{Max}(\mathcal{O}_K)} N(\mathfrak{p})^{-v_{\mathfrak{p}}(\alpha)} = N\left(\prod_{\mathfrak{p} \in \text{Max}(\mathcal{O}_K)} \mathfrak{p}^{-v_{\mathfrak{p}}(\alpha)}\right) \\ &= N(\alpha \mathcal{O}_K)^{-1} = |N_{\mathbb{Q}}^K(\alpha)|^{-1}. \end{aligned} \quad \square$$

For the splitting of finite primes in a number field extension we have the notions of ramification index and residue class degree. We extend these notions to the infinite case.

10.25 Definition. Let $L : K$ be a number field extension, \mathfrak{q} an infinite prime of L and \mathfrak{p} an infinite prime of K , say $\mathfrak{q} = \mathfrak{p}_{\tau}$ and $\mathfrak{p} = \mathfrak{p}_{\sigma}$, where τ and σ are embeddings in \mathbb{C} of respectively L and K . Then \mathfrak{q} is said to be *above* \mathfrak{p} if τ is a prolongation of σ . The *residue class degree* $f_K(\mathfrak{q})$ of \mathfrak{q} over K is defined to be 1 in all cases. The *ramification index* of \mathfrak{q} over K is defined by

$$e_K(\mathfrak{q}) = \begin{cases} 2 & \text{if } \mathfrak{q} \text{ is complex and } \mathfrak{p} \text{ is real,} \\ 1 & \text{otherwise.} \end{cases}$$

If a complex infinite prime lies above a real infinite prime, the complex infinite prime of L is said to be *ramified* over K and the real infinite prime of K is said to *ramify* in L .

The definitions of the ramification index and the residue class degree for infinite primes are such that the relation with the degree of the field extension is the same as in the finite case:

10.26 Proposition. Let $L : K$ be a number field extension and $\mathfrak{q}_1, \dots, \mathfrak{q}_r$ the different infinite primes of L above a given infinite prime of K . Then

$$\sum_{i=1}^r e_K(\mathfrak{q}_i) f_K(\mathfrak{q}_i) = [L : K].$$

PROOF. There are $[L : K]$ prolongations to L of an embedding of K in \mathbb{C} . The number on the left hand side is precisely the number of prolongations. \square

The formula also holds when we interchange here the notions of ramification index and residue class degree. The choice is somehow a matter of taste. In the classification of abelian extensions of number fields, as described in chapter 15, there is an important role for the ramifying primes, including the infinite ramifying primes as defined above. If the other choice is made, as is done in [31], this leads to another, but equivalent, description of the classification.

The action of the Galois group of a Galois extension $L : K$ on the collection of primes should be compatible with its action on the corresponding embeddings in the completions, meaning that the following diagram commutes:

$$\begin{array}{ccc}
 L & \xrightarrow{\sigma_{\mathfrak{q}}} & L_{\mathfrak{q}} \\
 \rho \downarrow & & \downarrow \\
 L & \xrightarrow{\sigma_{\rho \cdot \mathfrak{q}}} & L_{\rho(\mathfrak{q})}
 \end{array}$$

The vertical map on the right is the map induced by the embedding $\sigma_{\rho \cdot \mathfrak{q}}$. For $\mathfrak{q} \in \mathcal{P}_{\infty}(L)$ we take the map on the right to be the identity on \mathbb{R} or \mathbb{C} . This determines the action of the Galois group on infinite primes:

10.27 Definition. Let $L : K$ be a Galois extension of number fields, \mathfrak{q} an infinite prime of L and $\rho \in \text{Gal}(L : K)$. The action of ρ on \mathfrak{q} is given by

$$\sigma_{\rho \cdot \mathfrak{q}} = \sigma_{\mathfrak{q}} \rho^{-1}.$$

As in the finite case the Galois group acts transitively on the primes above a given prime.

10.28 Proposition. Let $L : K$ be a Galois extension of number fields and \mathfrak{p} an infinite prime of K . Then $\text{Gal}(L : K)$ acts transitively on the set of primes above \mathfrak{p} .

PROOF. The action of $\text{Gal}(L : K)$ on the set of prolongations to L of an embedding σ of K in \mathbb{C} is transitive. Hence the induced action on the set of infinite primes above \mathfrak{p}_{σ} is transitive as well. \square

Also the notions of inertia group and decomposition group can be extended to include the case of infinite primes.

10.29 Definition. Let $L : K$ be a Galois extension of number fields and \mathfrak{q} an infinite prime of L . The *decomposition group* of \mathfrak{q} over K is the stabilizer of \mathfrak{q} :

$$Z_K(\mathfrak{q}) = \{ \rho \in \text{Gal}(L : K) \mid \rho \cdot \mathfrak{q} = \mathfrak{q} \}.$$

The *inertia group* is defined to be equal to the decomposition group:

$$T_K(\mathfrak{q}) = Z_K(\mathfrak{q}).$$

10.30 Proposition. Let $L : K$ be a Galois extension of number fields, \mathfrak{q} an infinite prime of L and $\rho \in \text{Gal}(L : K)$. Then $Z_K(\rho \cdot \mathfrak{q}) = \rho Z_K(\mathfrak{q}) \rho^{-1}$.

PROOF. For $\tau \in \text{Gal}(L : K)$ the following are equivalent:

$$\tau \in Z_K(\rho \cdot \mathfrak{q}),$$

$$\sigma_{\rho \cdot \mathfrak{q}} \tau^{-1} = \sigma_{\rho \cdot \mathfrak{q}},$$

$$\sigma_{\mathfrak{q}} \rho^{-1} \tau^{-1} = \sigma_{\mathfrak{q}} \rho^{-1},$$

$$\sigma_{\mathfrak{q}} \rho^{-1} \tau^{-1} \rho = \sigma_{\mathfrak{q}},$$

$$\rho^{-1} \tau \rho \in Z_K(\mathfrak{q}),$$

$$\tau \in \rho Z_K(\mathfrak{q}) \rho^{-1}. \quad \square$$

10.31 Notation. Let $L : K$ be an abelian extension of number fields and \mathfrak{p} an infinite prime of K . Then $Z_{\mathfrak{p}}^{(L)}$ denotes the decomposition group over K of any of the infinite primes of L above \mathfrak{p} .

For an infinite prime \mathfrak{p} the group $Z_{\mathfrak{p}}^{(L)}$ is nontrivial if and only if \mathfrak{p} is real and the infinite primes of L above \mathfrak{p} are complex. In this case this group is of order 2.

10.5 Completions of discretely valued fields

In this section K is a field with a discrete valuation v . We fix a positive real number $c < 1$. The discrete valuation determines a nonarchimedean absolute value $\|\cdot\|$:

$$\|x\| = c^{v(x)} \quad \text{for } x \in K.$$

The field K is the field of fractions of the discrete valuation ring

$$R = \{x \in K \mid v(x) \geq 0\} = \{x \in K \mid \|x\| \leq 1\}.$$

The maximal ideal of R is

$$\mathfrak{p} = \{x \in K \mid v(x) > 0\} = \{x \in K \mid \|x\| < 1\}$$

and its group of units is

$$R^* = \{x \in K \mid v(x) = 0\} = \{x \in K \mid \|x\| = 1\}.$$

Let \hat{K} be the completion of the valued field K . The elements of \hat{K} are limits of sequences in K .

Let $\alpha \in \hat{K}$. Then $\alpha = \lim_{n \rightarrow \infty} a_n$ for a Cauchy sequence (a_n) in K and $\|\alpha\| = \lim_{n \rightarrow \infty} \|a_n\|$. If $\alpha \neq 0$, then there is an N such that $\|a_n\| \neq 0$ for all $n \geq N$. Since $\{\|\alpha\| \mid \alpha \in K^*\} = \langle c \rangle$, a discrete subgroup of \mathbb{R}^* , there is an $m \in \mathbb{Z}$ such that eventually $\|a_n\| = c^m$. This defines

$$v: \hat{K}^* \rightarrow \mathbb{Z}, \quad \alpha \mapsto m.$$

It easily follows that v is a discrete valuation of \hat{K} and that this v is a prolongation of the discrete valuation of K . Accordingly, for the prolongation of $\|\cdot\|$ to \hat{K} we have

$$\|\alpha\| = c^{v(\alpha)} \quad \text{for } \alpha \in \hat{K}.$$

We now have a discrete valuation ring

$$\hat{R} = \{x \in \hat{K} \mid v(x) \geq 0\} = \{x \in \hat{K} \mid \|x\| \leq 1\}$$

with maximal ideal

$$\hat{\mathfrak{p}} = \{x \in \hat{K} \mid v(x) > 0\} = \{x \in \hat{K} \mid \|x\| < 1\}.$$

10.32 Terminology. Let F be a complete discretely valued field and v the discrete valuation on F . A *uniformizer* of F is a $\pi \in F$ such that $v(\pi) = 1$. (So the uniformizer of F is the uniformizer of the discrete valuation v in the sense of Definition 6.9.)

Completion doesn't affect the residue class rings:

10.33 Proposition. *The inclusion $R \rightarrow \hat{R}$ induces for each $n \in \mathbb{N}$ an isomorphism $R/\mathfrak{p}^n \xrightarrow{\sim} \hat{R}/\hat{\mathfrak{p}}^n$.*

PROOF. Let $n \in \mathbb{N}^*$. The kernel of the composition $R \rightarrow \hat{R} \rightarrow \hat{R}/\hat{\mathfrak{p}}^n$ is $R \cap \hat{\mathfrak{p}}^n = \{x \in R \mid v(x) \geq n\} = \mathfrak{p}^n$. So the homomorphism $R/\mathfrak{p}^n \rightarrow \hat{R}/\hat{\mathfrak{p}}^n$ is injective. For each $\alpha \in \hat{R}$ there is an $a \in R$ such that $v(\alpha - a) \geq n$. Hence $\hat{R} = R + \hat{\mathfrak{p}}^n$ and this implies surjectivity. \square

In particular the residue class fields are canonically isomorphic: $R/\mathfrak{p} \xrightarrow{\sim} \hat{R}/\hat{\mathfrak{p}}$.

If a series $\sum_{n=1}^{\infty} a_n$ converges in a valued field, then the terms form a null sequence:

$$\lim_{n \rightarrow \infty} a_n = \lim_{n \rightarrow \infty} \left(\sum_{i=1}^n a_i - \sum_{i=1}^{n-1} a_i \right) = \lim_{n \rightarrow \infty} \sum_{i=1}^n a_i - \lim_{n \rightarrow \infty} \sum_{i=1}^{n-1} a_i = 0.$$

If $\lim_{n \rightarrow \infty} a_n = 0$ the series may diverge even when the field is complete, e.g. the series in \mathbb{R} given by $a_n = \frac{1}{n}$. In a complete discretely valued field, however, the converse holds as well:

10.34 Proposition. *Let F be a complete discretely valued field and (a_n) a null sequence in F . Then the series $\sum_{n=1}^{\infty} a_n$ converges in F .*

PROOF. The series is a Cauchy sequence: for $n < m$ we have

$$\left\| \sum_{i=n+1}^m a_i \right\| \leq \max_{n < i \leq m} \|a_i\|$$

and $\|a_n\| \rightarrow 0$ for $n \rightarrow \infty$. \square

The completion \hat{K} of the discretely valued field K is a complete discretely valued field, so this proposition applies in particular to such a completion.

10.35 Theorem. *Let F be a complete discretely valued field, R its valuation ring, \mathfrak{p} the maximal ideal of R , π a uniformizer of F and $S \subseteq R$ a system of representatives of R/\mathfrak{p} . Then for each $x \in R$ there is a unique sequence $(s_n)_{n \geq 0}$ in S such that*

$$x = \sum_{n=0}^{\infty} s_n \pi^n.$$

PROOF. By Proposition 6.18 for each $k \in \mathbb{N}^*$ there are unique $s_0, \dots, s_{k-1} \in S$ such that

$$x \equiv \sum_{n=0}^{k-1} s_n \pi^n \pmod{\mathfrak{p}^k}. \quad \square$$

10.36 Corollary. *Let F be a complete discretely valued field, R its valuation ring and \mathfrak{p} the maximal ideal of R , π a uniformizer of F and $S \subseteq R$ a system of representatives of R/\mathfrak{p} . Then for each $x \in F^*$ there is a unique $N \in \mathbb{Z}$ and a unique sequence $(s_n)_{n \geq N}$ in S such that*

$$x = \sum_{n=N}^{\infty} s_n \pi^n \quad \text{and} \quad s_N \notin \mathfrak{p}.$$

The number N is equal to the valuation of x .

PROOF. F is the field of fractions of R . Apply the Theorem 10.35 to $x\pi^{-v(x)}$. \square

10.37 Alternative construction. A more algebraic way of constructing the completion of a discretely valued field is as follows. First construct the valuation ring \hat{R} . It is the inverse limit of the R/\mathfrak{p}^n . More precisely, it is the inverse limit of the diagram

$$\dots \rightarrow R/\mathfrak{p}^{n+1} \rightarrow R/\mathfrak{p}^n \rightarrow \dots \rightarrow R/\mathfrak{p},$$

where the maps $R/\mathfrak{p}^{n+1} \rightarrow R/\mathfrak{p}^n$ are induced by the identity on R . So we can take

$$\hat{R} = \{(\dots, x_{n+1}, x_n, \dots, x_1) \mid x_n \in R/\mathfrak{p}^n \text{ and } x_{n+1} \mapsto x_n \text{ for all } n \in \mathbb{N}^*\}.$$

This kind of limits is treated in general in chapter 19. The connection with the construction in this chapter is as follows: put $x_n = \overline{b_n}$ with $b_n \in R$, then $b_{n+1} - b_n \in \mathfrak{p}^n$, so (b_n) converges and the element $(\dots, x_{n+1}, x_n, \dots, x_1)$ corresponds to $\lim_{n \rightarrow \infty} b_n$. The field \hat{K} is then obtained as the field of fractions of \hat{R} .

10.38 Notations.

1. For a complete discretely valued field F the discrete valuation is often denoted by v_F , the valuation ring by \mathcal{O}_F and the residue class field by k_F .

2. Let K be a discretely valued field, R its valuation ring with maximal ideal \mathfrak{p} . The completion of K will be denoted by $K_{\mathfrak{p}}$. It is a complete discretely valued field. Its valuation ring will be denoted by $R_{\mathfrak{p}}$. The notation $\hat{\mathfrak{p}}$ for the maximal ideal of $R_{\mathfrak{p}}$ will be used for distinction from \mathfrak{p} . It is the ideal of $R_{\mathfrak{p}}$ generated by \mathfrak{p} : for $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$ we have

$$\mathfrak{p}R_{\mathfrak{p}} = \pi R_{\mathfrak{p}} = \hat{\mathfrak{p}}.$$

3. For K a number field and $\mathfrak{p} \in \text{Max}(\mathcal{O}_K)$, $K_{\mathfrak{p}}$ is the completion of K with respect to the discrete valuation $v_{\mathfrak{p}}$. The valuation ring of $K_{\mathfrak{p}}$ will be denoted by $\mathcal{O}_{\mathfrak{p}}$.

10.39 Example. Let p be a prime number. The completion of \mathbb{Q} w.r.t. the discrete valuation $v_p: \mathbb{Q}^* \rightarrow \mathbb{Z}$ is the field \mathbb{Q}_p of p -adic numbers. The set $S = \{0, 1, \dots, p-1\}$ is a system of representatives of \mathbb{Z}/p . The valuation ring is denoted by \mathbb{Z}_p and is called the ring of p -adic integers. By Corollary 10.36 a nonzero p -adic number x has a unique representation

$$x = \sum_{n=N}^{\infty} s_n p^n$$

with $s_n \in S$, $N = v_p(x)$ and $s_N \neq 0$. This representation, or the sequence of the s_n , is called the p -adic expansion of x . A p -adic integer x has a p -adic expansion

$$x = \sum_{n=0}^{\infty} s_n p^n.$$

For $x \neq 0$, the valuation of x is the least $N \in \mathbb{N}$ with $s_N \neq 0$.

10.6 Extensions of complete discretely valued fields

The main result in this section is that a finite extension of a complete discretely valued field has again the structure of a complete discretely valued field (Theorem 10.40). This will be used in the next chapter, where it is shown that a finite extension of \mathbb{Q}_p is the completion of some number field (Corollary 11.5).

10.40 Theorem. *Let F be a complete discretely valued field and $E : F$ a finite separable field extension. Then the integral closure of \mathcal{O}_F in E is a discrete valuation ring and E is complete with respect to the discrete absolute value determined by the valuation.*

PROOF. Put $d = [E : F]$ and let S be the integral closure of \mathcal{O}_F in E . By Theorem 2.45 the ring S is a Dedekind domain and since this ring is semi-local it is a principal ideal domain (Proposition 2.21). Moreover, because \mathcal{O}_F is a principal ideal domain, S is a free \mathcal{O}_F -module of rank d (Corollary 1.38). Let β_1, \dots, β_d be an \mathcal{O}_F -basis of S . On the F -vector space E we have a norm $\|\cdot\|$ defined as follows:

$$\|a_1\beta_1 + \dots + a_d\beta_d\| = \max_{1 \leq j \leq d} \|a_j\|_F \quad (\text{for } a_1, \dots, a_d \in F).$$

Then for all indices j with $1 \leq j \leq d$ we have $\|a_j\|_F \leq \|a_1\beta_1 + \dots + a_d\beta_d\|$. So a sequence $(a_1n\beta_1 + \dots + a_dn\beta_d)_n$ with all a_jn in F is a Cauchy sequence with respect to $\|\cdot\|$ if and only if the sequences $(a_jn)_n$ converge in F . Put $a_j = \lim_n a_jn$. Then $(a_j - a_jn)_n$ is a null sequence in F and we have

$$\|(a_1 - a_1n)\beta_1 + \dots + (a_d - a_dn)\beta_d\| = \max_j \|a_j - a_jn\|_F.$$

It follows that the sequence $(a_1n\beta_1 + \dots + a_dn\beta_d)_n$ converges to $a_1\beta_1 + \dots + a_d\beta_d$ with respect to the norm $\|\cdot\|$. Hence the vector space E is complete with respect to this norm.

Next we show that the Dedekind domain S has only one maximal ideal. Let \mathfrak{q} be a maximal ideal of S . Then $\mathfrak{p}_F S = \mathfrak{q}^e \mathfrak{a}$ with e the ramification index of \mathfrak{q} over F and $\mathfrak{q} \nmid \mathfrak{a}$. By the Chinese Remainder Theorem there exists for each $n \in \mathbb{N}$ an $\varepsilon_n \in S$ such that

$$\varepsilon_n \equiv \begin{cases} 1 & (\text{mod } \mathfrak{q}^{en}), \\ 0 & (\text{mod } \mathfrak{a}^n). \end{cases}$$

Then $\varepsilon_n^{n+1} - \varepsilon_n \in \mathfrak{q}^{en} \mathfrak{a}^n = \mathfrak{p}_F^n S = \mathfrak{p}_F^n \beta_1 + \dots + \mathfrak{p}_F^n \beta_d$. So ε_n is a Cauchy sequence with respect to $\|\cdot\|$. Put $\varepsilon = \lim_n \varepsilon_n$. Since $\varepsilon_n^2 - \varepsilon_n \in \mathfrak{q}^{en} \mathfrak{a}^n$ is a null sequence with respect to $\|\cdot\|$, it follows that $\varepsilon^2 = \varepsilon$. The image of $\varepsilon \in S$ in the residue field S/\mathfrak{q} is 1, so $\varepsilon \neq 0$ and since E is a field we have $\varepsilon = 1$. The image of ε in S/\mathfrak{a} is both 1 and 0, so $\mathfrak{a} = S$.

It remains to show that E is complete with respect to $\|\cdot\|_{\mathfrak{q}}$. Let $(\alpha_n)_n$ be a Cauchy sequence in E with respect to $\|\cdot\|_{\mathfrak{q}}$. Then for each $M \in \mathbb{N}$ there is an $N \in \mathbb{N}$ such that $\alpha_n - \alpha_m \in \mathfrak{q}^{em} = \mathfrak{p}^M S$ for all $m, n \geq N$. So $(\alpha_n)_n$ is a Cauchy sequence with respect to $\|\cdot\|$. Put $\alpha_n = a_1n\beta_1 + \dots + a_dn\beta_d$ with the a_jn in F . The sequences $(a_jn)_n$ converge in F with respect to $\|\cdot\|_F$ as well as with respect to $\|\cdot\|_{\mathfrak{q}}$. Hence the sequence $(\alpha_n)_n$ converges with respect to $\|\cdot\|_{\mathfrak{q}}$. \square

So a finite extension of a complete discretely valued field is in a unique way a complete discrete valued field with the topology of the base field induced by the topology on the extension. On the other hand, such extensions are necessarily finite; more precisely:

10.41 Theorem. *Let $E : F$ be an extension of complete discrete valued fields such that the absolute value on F induced by the absolute value on E is non-trivial and that F is complete w.r.t. this absolute value. Let the extension of the residue class fields be finite of degree f . Then \mathcal{O}_E is a free \mathcal{O}_F -module of rank ef and $[E : F] = ef$, where $e = (\mathbb{Z} : v_E(F^*))$.*

PROOF. The second assertion follows from the first, so we prove the first. Let $\beta_1, \dots, \beta_f \in \mathcal{O}_E$ be such that $\overline{\beta}_1, \dots, \overline{\beta}_f$ is a k_F -basis of k_E . Let ρ and π be uniformizers of F and E respectively. We will show that the elements

$$\beta_i \pi^j \quad (i = 1, \dots, f \text{ and } j = 0, \dots, e - 1)$$

form an \mathcal{O}_F -basis of \mathcal{O}_E . Let X be a set of representatives of $k_F = \mathcal{O}_F/\mathfrak{p}_F$. Then $Y = X\beta_1 + \dots + X\beta_f$ is a set of representatives of $k_E = \mathcal{O}_E/\mathfrak{p}_E$. Instead of using powers π^k when representing elements of \mathcal{O}_E we can also use the elements $\rho^i \pi^j$ with $i \in \mathbb{N}$ and $0 \leq j < e$. Note that $v_E(\rho^j \pi^i) = ie + j$. For elements of \mathcal{O}_E we have the unique representation

$$\alpha = \sum_{i=0}^{\infty} \sum_{j=0}^{e-1} \gamma_{ij} \rho^i \pi^j,$$

where the γ_{ij} are unique elements of Y . Put $\gamma_{ij} = \sum_{k=1}^f c_{ijk} \beta_k$, where $c_{ijk} \in X$. Then

$$\alpha = \sum_{i=0}^{\infty} \sum_{j=0}^{e-1} \gamma_{ij} \rho^i \pi^j = \sum_{i=0}^{\infty} \sum_{j=0}^{e-1} \sum_{k=1}^f c_{ijk} \beta_k \rho^i \pi^j = \sum_{j=0}^{e-1} \sum_{k=1}^f \left(\sum_{i=0}^{\infty} c_{ijk} \rho^i \right) \beta_k \pi^j.$$

Since $\sum_{i=0}^{\infty} c_{ijk} \rho^i \in \mathcal{O}_F$, the $\beta_k \pi^j$ generate the \mathcal{O}_F -module \mathcal{O}_E . It is straightforward to show their independence over \mathcal{O}_F . So \mathcal{O}_E is a free \mathcal{O}_F -module of rank ef . \square

10.42 Notation and terminology. Let $E : F$ be as in the above theorem. The ramification index of \mathfrak{p}_E over F is called the *ramification index* of $E : F$ and is denoted by $e_F^{(E)}$. Similarly we have the *residue class degree* $f_F^{(E)}$ of $E : F$.

10.7 Completions of field extensions

Completion of an extension of valued fields yields an extension of complete fields. In case of discretely valued fields the result is an extension of complete discretely valued fields as considered in the previous section. Here we study the connection between the extension and its completion. In this section:

R	a Dedekind domain,
K	the field of fractions of R ,
$L : K$	a finite separable field extension,
n	$= [L : K]$, the degree of $L : K$,
S	the integral closure of R in L ,
\mathfrak{p}	a maximal ideal of R ,
\mathfrak{q}	a maximal ideal of S above \mathfrak{p} ,
e	$= e_K(\mathfrak{q})$, the ramification index of \mathfrak{q} over K ,
f	$= f_K(\mathfrak{q})$, the residue class degree of \mathfrak{q} over K .

We study the effect of completing the field L with respect to the nonarchimedean valuation $\|\cdot\|_{\mathfrak{q}}$.

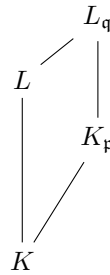
The discrete valuations with respect to \mathfrak{p} and \mathfrak{q} of K and L respectively, are related by

$$v_{\mathfrak{q}}(\alpha) = e \cdot v_{\mathfrak{p}}(\alpha) \quad \text{for all } \alpha \in K.$$

So the absolute value on L given by $\|\cdot\|_{\mathfrak{q}} = c^{v_{\mathfrak{q}}(\cdot)}$ for some c with $0 < c < 1$, satisfies

$$\|\alpha\|_{\mathfrak{q}} = c^{e \cdot v_{\mathfrak{p}}(\alpha)} = \|\alpha\|_{\mathfrak{p}} \quad \text{for all } \alpha \in K,$$

where $\|\cdot\|_{\mathfrak{p}}$ is taken to be $(c^e)^{v_{\mathfrak{p}}(\cdot)}$. It follows that we can assume that the completion $K_{\mathfrak{p}}$ of K is a subfield of $L_{\mathfrak{q}}$.



10.43 Proposition. $K_{\mathfrak{p}}L = L_{\mathfrak{q}}$.

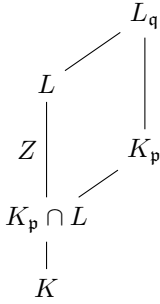
PROOF. The composition $K_{\mathfrak{p}}L$ is a composition of subfields of $L_{\mathfrak{q}}$ and so $L_{\mathfrak{q}} \supseteq K_{\mathfrak{p}}L$. Choose $\vartheta \in L$ such that $L = K(\vartheta)$ and consider the subfield $K_{\mathfrak{p}}(\vartheta)$ of $L_{\mathfrak{q}}$. Since ϑ is algebraic over $K_{\mathfrak{p}}$ the extension $K_{\mathfrak{p}}(\vartheta) : K_{\mathfrak{p}}$ is finite and so by Theorem 10.40 $K_{\mathfrak{p}}(\vartheta)$ is complete w.r.t. (the restriction of) the absolute value $\|\cdot\|_{\mathfrak{q}}$ on $L_{\mathfrak{q}}$. The field $L_{\mathfrak{q}}$ is the completion of L w.r.t. $\|\cdot\|_{\mathfrak{q}}$ and L is a subfield of $K_{\mathfrak{p}}(\vartheta)$. Hence $K_{\mathfrak{p}}L = K_{\mathfrak{p}}K(\vartheta) = K_{\mathfrak{p}}(\vartheta) \supseteq L_{\mathfrak{q}}$. \square

10.44 Proposition. *The ring $S_{\mathfrak{q}}$ is a free $R_{\mathfrak{p}}$ -module of rank ef and $[L_{\mathfrak{q}} : K_{\mathfrak{p}}] = ef$.*

PROOF. Apply Theorem 10.40: for $E : F$ take the extension $L_{\mathfrak{q}} : K_{\mathfrak{p}}$. By Theorem 7.7 the integral domain $S_{\mathfrak{q}}$ is the integral closure of $R_{\mathfrak{p}}$ in $L_{\mathfrak{q}}$. Note that $\hat{\mathfrak{p}}S_{\mathfrak{q}} = \mathfrak{p}R_{\mathfrak{p}}S_{\mathfrak{q}} = \mathfrak{p}S_{\mathfrak{q}} = \mathfrak{p}SS_{\mathfrak{q}} = \mathfrak{q}^eS_{\mathfrak{q}} = \hat{\mathfrak{q}}^e$ and that $[S_{\mathfrak{q}}/\hat{\mathfrak{q}} : R_{\mathfrak{p}}/\hat{\mathfrak{p}}] = [S/\mathfrak{q} : R/\mathfrak{p}] = f$. \square

For Galois extensions we have:

10.45 Theorem. *Let $L : K$ be a Galois extension. Then $L_{\mathfrak{q}} : K_{\mathfrak{p}}$ is a Galois extension and the restriction of $K_{\mathfrak{p}}$ -automorphisms of $L_{\mathfrak{q}}$ to L induces an isomorphism $\text{Gal}(L_{\mathfrak{q}} : K_{\mathfrak{p}}) \xrightarrow{\sim} Z_K(\mathfrak{q})$.*



PROOF. From $L_{\mathfrak{q}} = K_{\mathfrak{p}}L$ follows that $L_{\mathfrak{q}} : K_{\mathfrak{p}}$ is a Galois extension and $\text{Gal}(L_{\mathfrak{q}} : K_{\mathfrak{p}}) \cong \text{Gal}(L : (K_{\mathfrak{p}} \cap L))$. Put $Z = Z_K(\mathfrak{q})$. If $\sigma \in Z$, then $\sigma(\mathfrak{q}) = \mathfrak{q}$ and so $\|\sigma(\alpha)\|_{\mathfrak{q}} = \|\alpha\|_{\mathfrak{q}}$ for all $\alpha \in L$. By the definition of completion σ extends uniquely to an automorphism of $L_{\mathfrak{q}}$, its restriction to $K_{\mathfrak{p}}$ being the identity, because it is the unique extension of the identity on K . From $L_{\mathfrak{q}} = K_{\mathfrak{p}}L$ follows that we thus have an injective group homomorphism $Z \rightarrow \text{Gal}(L_{\mathfrak{q}} : K_{\mathfrak{p}})$, which is an isomorphism since the orders of both groups are equal. Otherwise put: $L^Z = K_{\mathfrak{p}} \cap L$. \square

Finally, we relate the ‘global’ norm N_K^L and trace Tr_K^L to the ‘local’ norm $N_{K_{\mathfrak{p}}}^{L_{\mathfrak{q}}}$ and trace $\text{Tr}_{K_{\mathfrak{p}}}^{L_{\mathfrak{q}}}$. The last notations will be abbreviated to $N_{\mathfrak{p}}^{\mathfrak{q}}$ and $\text{Tr}_{\mathfrak{p}}^{\mathfrak{q}}$. We now consider the extensions $L_{\mathfrak{q}} : K_{\mathfrak{p}}$ for all $\mathfrak{q} \mid \mathfrak{p}S$ together. The embeddings $L \rightarrow L_{\mathfrak{q}}$ induce a homomorphism of $K_{\mathfrak{p}}$ -algebras

$$\psi_{\mathfrak{p}} : K_{\mathfrak{p}} \otimes_K L \rightarrow \prod_{\mathfrak{q} \mid \mathfrak{p}S} L_{\mathfrak{q}}, \quad \alpha \otimes \beta \mapsto (\alpha\beta)_{\mathfrak{q}}.$$

10.46 Proposition. *The $K_{\mathfrak{p}}$ -algebra homomorphism $\psi_{\mathfrak{p}}$ is an isomorphism.*

PROOF. The map $\psi_{\mathfrak{p}}$ is obtained by applying the exact functor $K_{\mathfrak{p}} \otimes_K -$ to the diagonal embedding $L \rightarrow \prod_{\mathfrak{q} \mid \mathfrak{p}S} L_{\mathfrak{q}}$. Hence $\psi_{\mathfrak{p}}$ is injective. Since L is an n -dimensional K -vector space, the algebra $K_{\mathfrak{p}} \otimes_K L$ is n -dimensional over $K_{\mathfrak{p}}$. The $K_{\mathfrak{p}}$ -dimension of $\prod_{\mathfrak{q} \mid \mathfrak{p}S} L_{\mathfrak{q}}$ is equal to n as well: $\sum_{\mathfrak{q} \mid \mathfrak{p}S} e_K(\mathfrak{q})f_K(\mathfrak{q}) = n$. \square

10.47 Corollary. *For $\alpha \in L$ and \mathfrak{p} a prime of K*

$$N_K^L(\alpha) = \prod_{\mathfrak{q} \mid \mathfrak{p}S} N_{\mathfrak{p}}^{\mathfrak{q}}(\alpha) \quad \text{and} \quad \text{Tr}_K^L(\alpha) = \sum_{\mathfrak{q} \mid \mathfrak{p}S} \text{Tr}_{\mathfrak{p}}^{\mathfrak{q}}(\alpha).$$

PROOF. By Proposition 10.46 for both algebras $K_{\mathfrak{p}} \otimes_K L$ and $\prod_{\mathfrak{q} \mid \mathfrak{p}S} L_{\mathfrak{q}}$ multiplication by α has the same characteristic polynomial. So for $K_{\mathfrak{p}} \otimes_K L$ this polynomial is $\Delta_{\alpha}^{L:K}$. Hence

$$\Delta_{\alpha}^{L:K}(X) = \prod_{\mathfrak{q} \mid \mathfrak{p}S} \Delta_{\alpha}^{L_{\mathfrak{q}}:K_{\mathfrak{p}}}(X).$$

The identities for the norms and the traces are obtained by comparing coefficients. \square

EXERCISES

- Let k be a field and $\|\cdot\|$ a nontrivial absolute value on the field $k(T)$ of rational functions such that its restriction to k is the trivial absolute value. Show that $\|\cdot\|$ is a nonarchimedean absolute value on $k(T)$.
- Let k and $\|\cdot\|$ be as in exercise 1.
 - Prove that $\|\cdot\|$ is equivalent to $\|\cdot\|_{\mathfrak{p}}$ for some $\mathfrak{p} \in \text{Max}(k[T])$ if $\|T\| \leq 1$.
 - Assume that $\|T\| > 1$. Prove that $\|\cdot\|$ is equivalent to the absolute value $\|\cdot\|_{v_\infty}$ determined by the discrete valuation v_∞ described in exercise 2 of chapter 6:

$$\|f\|_{v_\infty} = c^{-\deg(f)} \quad \text{for } f \in k(T)^*,$$

where c such that $0 < c < 1$.

- Show that the $v_{\mathfrak{p}}$ with $\mathfrak{p} \in \text{Max}(k[T]) \cup \{\infty\}$ are all discrete valuations on $k(T)$ which vanish on k^* .

The symbol ∞ can be thought of as an infinite prime of $k(T)$. However, this field is the field of fractions of other Dedekind domains as well, including Dedekind domains for which ∞ is one of the prime ideals, e.g. the Dedekind domain $k[\frac{1}{T}]$. This is best understood when considering $k(T)$ geometrically as the field of rational functions on the projective line.

- Let k be a field and let V be the set of all discrete valuations on $k(T)$ which vanish on k^* . So by part (iii) of exercise 2:

$$V = \{v_{\mathfrak{p}} \mid \mathfrak{p} \in \text{Max}(k[T]) \text{ or } \mathfrak{p} = \infty\}.$$

Denote the residue class field w.r.t. a valuation v by k_v . Then $k_v : k$ is a finite field extension: $k_{v_\infty} = k$ and for $v = v_{\mathfrak{p}}$ with $\mathfrak{p} \in \text{Max}(k[T])$ we have $k_v = k[T]/\mathfrak{p}$. Define $\deg(v) = [k_v : k]$.

- Prove that $\sum_{v \in V} \deg(v)v(f) = 0$ for all $f \in k(T)^*$.
- Show that we have an exact sequence

$$1 \longrightarrow k^* \longrightarrow k(T)^* \xrightarrow{(v)_v} \bigoplus_{v \in V} \mathbb{Z} \xrightarrow{(\deg(v))_v} \mathbb{Z} \longrightarrow 0.$$

- Let k and V be as in exercise 3. Put $V_\infty = V \setminus \{v_{(T)}\}$ and $V_0 = V \setminus \{v_\infty\}$. Show that for each subset W of V with $\emptyset \neq W \neq V$ the ring

$$\{f \in k(T) \mid v(f) \geq 0 \text{ for all } v \in W\}$$

is a Dedekind domain: it is a localization of $k[T]$ or of $k[\frac{1}{T}]$.

- Let k be a finite field.
 - Show that the places of $k(T)$ correspond to the discrete valuations of $k(T)$.
 - For each discrete valuation v of $k(T)$ choose a c_v with $0 < c_v < 1$. Then the places of $k(T)$ are represented by the absolute values $\|\cdot\|_v$ defined by

$$\|f\|_v = c_v^{v(f)} \quad \text{for } f \in k(T)^*.$$

Let k_v be the residue class field of the discrete valuation v . Show that if we choose $c_v = \#(k_v)^{-1}$ the following product formula holds:

$$\prod_v \|f\|_v = 1 \quad \text{for all } f \in k(T)^*.$$

6. Let k be a field in which -1 is not a square. Then k is not of characteristic 2. Let R be the ring $k[X, Y]/(X^2 + Y^2 - 1) = k[x, y]$. (The elements x and y are the classes of X and Y respectively and so $x^2 + y^2 = 1$.) Its field of fractions is $k(x, y)$, a quadratic extension of $k(x)$.

(i) Show that intersecting the line $y = t(x + 1)$ by the circle $x^2 + y^2 = 1$ yields an isomorphism $\varphi: k(x, y) \xrightarrow{\sim} k(T)$. Compute this isomorphism.

(ii) Let V be the set of all discrete valuations of $k(T)$ and put $W = V \setminus \{v_{\mathfrak{q}}\}$, where $\mathfrak{q} = (T^2 + 1)$.

(iii) Prove that

$$\varphi(R) = \{f \in k(T) \mid v(f) \geq 0 \text{ for all } v \in W\}.$$

So, in particular, by exercise 4 the ring R is a Dedekind domain.

(iv) Compute R^* and $\mathcal{C}(R)$ for $k = \mathbb{R}$.

(Use the ker-coker exact sequence of $k(T)^* \rightarrow \bigoplus_v \mathbb{Z} \rightarrow \bigoplus_{v \in V_0} \mathbb{Z}$.)

7. Let p be a prime number and x a nonzero p -adic number. Show that x is a rational number if and only if its p -adic expansion, as described in Example 10.39, is eventually periodic. Determine the p -adic expansion of -1 .

8. Let K_1 and K_2 be number fields. Put $L = K_1 K_2$ and $K = K_1 \cap K_2$. Let \mathfrak{q} be a prime of L and $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}$ the primes under \mathfrak{q} of respectively K_1, K_2, K .

(i) We can assume that the completions $(K_1)_{\mathfrak{p}_1}, (K_2)_{\mathfrak{p}_2}$ and $K_{\mathfrak{p}}$ are subfields of $L_{\mathfrak{q}}$. Show that $L_{\mathfrak{q}} = (K_1)_{\mathfrak{p}_1} (K_2)_{\mathfrak{p}_2}$.

(ii) Show that $K_{\mathfrak{p}} \subseteq (K_1)_{\mathfrak{p}_1} \cap (K_2)_{\mathfrak{p}_2}$, but that equality does not hold in general.

11 Local Fields

The completion of a number field with respect to a nonarchimedean absolute value is a complete discretely valued field with a finite residue field. Such fields are called local fields. In section 11.1 it is shown that all local fields of characteristic zero are completions of number fields. A powerful property of local fields is the similarity between (parts of) their additive and multiplicative structure given by the logarithm and the exponential function. This is well-known for the complete archimedean fields \mathbb{R} and \mathbb{C} . In section 11.4 the logarithm and exponential function for the completions at finite primes are introduced.

11.1 Local fields of characteristic 0

The completion at a finite prime of a number field is a complete discretely valued field of characteristic 0 with a finite residue class field. It will be shown that all such fields are completions of some number field.

11.1 Definition. A complete discretely valued field with a finite residue class field is called a *local field*.

The p -adic completion of a number field is a local field of characteristic 0. We will show that conversely every local field of characteristic 0 is the completion at a finite prime of some number field. The following lemma is crucial.

11.2 Krasner's Lemma. *Let p be a prime number, $F : \mathbb{Q}_p$ a Galois extension and let $\alpha, \beta \in F$ satisfy*

$$\|\alpha - \beta\| < \|\sigma(\alpha) - \alpha\| \quad \text{for all } \sigma \in \text{Gal}(F : \mathbb{Q}_p) \text{ with } \sigma(\alpha) \neq \alpha,$$

where $\|\cdot\|$ is the unique prolongation of $\|\cdot\|_p$ to F . Then $\alpha \in \mathbb{Q}_p(\beta)$.

PROOF. Let $\tau \in \text{Gal}(F : \mathbb{Q}_p(\beta))$. The uniqueness of $\|\cdot\|$ implies that automorphisms of $F : \mathbb{Q}_p$ preserve the absolute value. So

$$\|\tau(\alpha) - \beta\| = \|\alpha - \beta\|$$

and, therefore,

$$\|\tau(\alpha) - \alpha\| = \|\tau(\alpha) - \beta + \beta - \alpha\| \leq \max(\|\tau(\alpha) - \beta\|, \|\alpha - \beta\|) = \|\alpha - \beta\|.$$

11 Local Fields

The condition on α and β implies that $\tau(\alpha) = \alpha$. Since this holds for all $\tau \in \text{Gal}(F : \mathbb{Q}_p(\beta))$, we have $\alpha \in \mathbb{Q}_p(\beta)$. \square

11.3 Lemma. *Let K be a field with absolute value $\|\cdot\|$ and $\alpha \in K$ a zero of $f = X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n \in K[X]$. Then*

$$\|\alpha\| \leq \max\left(1, \sum_{i=1}^n \|a_i\|\right).$$

PROOF. If $\|\alpha\| \geq 1$, then

$$\|\alpha\| = \left\| a_1 + \frac{a_2}{\alpha} + \cdots + \frac{a_n}{\alpha^{n-1}} \right\| \leq \sum_{i=1}^n \|a_i\|. \quad \square$$

11.4 Proposition. *Let p be a prime number, $F : \mathbb{Q}_p$ a finite field extension and $\alpha \in F$. Then $\mathbb{Q}_p(\alpha) = \mathbb{Q}_p(\beta)$ for some $\beta \in F$ which is algebraic over \mathbb{Q} .*

PROOF. By Theorem 10.40 F is a local field. Put $n = [\mathbb{Q}_p(\alpha) : \mathbb{Q}_p]$. Let $f \in \mathbb{Q}_p[X]$ be the minimal polynomial of α over \mathbb{Q}_p . Set $f = X^n + a_1X^{n-1} + \cdots + a_n$ and $C = \max(1, \sum_{i=1}^n \|a_i\|)$. Let $\varepsilon > 0$, to be specified later, and put

$$\delta = \varepsilon^n / \sum_{i=0}^{n-1} C^i.$$

Choose $g = X^n + b_1X^{n-1} + \cdots + b_n \in \mathbb{Q}[X]$ with $\|a_i - b_i\| < \delta$ for $i = 1, \dots, n$. Then by Lemma 11.3

$$\|g(\alpha)\| = \|g(\alpha) - f(\alpha)\| \leq \sum_{i=1}^n \|b_i - a_i\| \|\alpha\|^{n-i} < \delta \sum_{i=0}^{n-1} C^i = \varepsilon^n.$$

Let E be a splitting field of fg over F and $\|\cdot\|$ the unique prolongation of $\|\cdot\|_p$ to E . Over E we have

$$g = \prod_{i=1}^n (X - \beta_i) \quad \text{with } \beta_1, \dots, \beta_n \in E.$$

From

$$\|g(\alpha)\| = \prod_{i=1}^n \|\alpha - \beta_i\| < \varepsilon^n$$

follows that $\|\alpha - \beta\| < \varepsilon$ for some zero β of g . Take

$$\varepsilon = \min_{\substack{\sigma \in \text{Gal}(E:\mathbb{Q}_p) \\ \sigma(\alpha) \neq \alpha}} \|\sigma(\alpha) - \alpha\|.$$

Then by Krasner's Lemma $\alpha \in \mathbb{Q}_p(\beta)$ and so $\mathbb{Q}_p(\alpha) \subseteq \mathbb{Q}_p(\beta)$. Because $n = [\mathbb{Q}_p(\alpha) : \mathbb{Q}_p] \leq [\mathbb{Q}_p(\beta) : \mathbb{Q}_p] \leq n$, we have $\mathbb{Q}_p(\alpha) = \mathbb{Q}_p(\beta)$. \square

11.5 Corollary. *Let p be a prime number and $F : \mathbb{Q}_p$ a finite field extension. Then F is the local field of some number field K at a finite prime of K above p .*

PROOF. Choose a primitive element α of the extension $F : \mathbb{Q}_p$. By Proposition 11.4 there is a $\beta \in \mathbb{Q}_p(\alpha)$ which is algebraic over \mathbb{Q} such that $\mathbb{Q}_p(\alpha) = \mathbb{Q}_p(\beta)$. Take $K = \mathbb{Q}(\beta) \subset F$ and $\mathfrak{p} = \mathfrak{p}_F \cap K \in \text{Max}(\mathcal{O}_K)$. Then $K_{\mathfrak{p}} \subseteq F$ and $F = \mathbb{Q}_p(\beta) \subseteq K_{\mathfrak{p}}$. \square

Summarizing, we have the following.

11.6 Theorem. *Equivalent are:*

- a) F is a local field of characteristic 0,
- b) F is a finite extension of \mathbb{Q}_p for some prime number p ,
- c) F is the \mathfrak{p} -adic completion of a number field at a finite prime \mathfrak{p} .

PROOF.

a) \Rightarrow b) Since F is of characteristic 0, its prime field is \mathbb{Q} . The discrete valuation on F induces a discrete valuation on \mathbb{Q} , which by Theorem 10.12 is the p -adic valuation for some prime number p . So F is an extension of \mathbb{Q}_p . By Theorem 10.41 the extension $F : \mathbb{Q}_p$ is finite: take $F : \mathbb{Q}_p$ for the extension $E : F$ in the theorem.

b) \Rightarrow c) Corollary 11.5.

c) \Rightarrow a) The \mathfrak{p} -adic completion of a number field is a complete discretely valued field (cf. section 10.5) with a finite residue class field (Proposition 10.33). \square

11.2 The multiplicative group

In this section we study the multiplicative structure of a local field and, in particular, its roots of unity. It will be shown that the roots of unity of the residue field of a local field can be lifted to the field itself in a canonical way. The completion of a number field often has many more roots of unity than the number field itself.

11.7 Lemma. *Let F be a local field. Then for $\alpha \in \mathcal{O}_F^*$ and $q = \#(k_F)$ the sequence $(\alpha^{q^n})_n$ converges to a $(q - 1)$ -st root of unity congruent to α modulo \mathfrak{p}_F .*

PROOF. Put $\alpha_n = \alpha^{q^n}$. For the convergence of $(\alpha_n)_n$ it suffices by Proposition 10.34 to show that $(\alpha_{n+1} - \alpha_n)_n$ is a null sequence. Since $\alpha \in \mathcal{O}_F^*$ we have $\|\alpha\| = 1$ and

$$\|\alpha_{n+1} - \alpha_n\| = \|\alpha^{q^{n+1}} - \alpha^{q^n}\| = \|\alpha^{(q-1)q^n} - 1\|.$$

From

$$\alpha^{(q-1)q^{n+1}} - 1 = (\alpha^{(q-1)q^n} - 1)(\alpha^{(q-1)q^n(q-1)} + \dots + \alpha^{(q-1)q^n} + 1)$$

and $\alpha^{q-1} \equiv 1 \pmod{\mathfrak{p}}$ follows that

$$v_F(\alpha^{(q-1)q^{n+1}} - 1) > v_F(\alpha^{(q-1)q^n} - 1).$$

Hence $(\alpha_{n+1} - \alpha_n)_n$ is a null sequence. All terms of the sequence $(\alpha_n)_n$ are congruent to α modulo \mathfrak{p}_F , so this holds for the limit as well. For $\zeta = \lim_{n \rightarrow \infty} \alpha_n$ we have

$$\zeta = \lim_{n \rightarrow \infty} \alpha^{q^{n+1}} = \left(\lim_{n \rightarrow \infty} \alpha^{q^n} \right)^q = \zeta^q. \quad \square$$

By this lemma we have for a local field F a map

$$\lambda_F: \mathcal{O}_F^* \rightarrow \mu_{q-1}(F), \quad \alpha \mapsto \lim_{n \rightarrow \infty} \alpha^{q^n}.$$

It clearly is a group homomorphism and for $\zeta \in \mu_{q-1}(F)$ the sequence $(\zeta^{q^n})_n$ is constant, so λ_F is a retract of \mathcal{O}_F^* to its subgroup $\mu_{q-1}(F)$. For $\alpha \equiv 1 \pmod{\mathfrak{p}_F}$ we have $\lambda_F(\alpha) = 1$. Hence λ_F induces a homomorphism

$$\omega_F: k_F^* \rightarrow \mu_{q-1}(F), \quad \bar{\alpha} \mapsto \lambda_F(\alpha).$$

The map λ_F is surjective and so is this induced map. Since both groups k_F^* and $\mu_{q-1}(F)$ are of order $q - 1$, the homomorphism ω_F is an isomorphism. It follows that we have a split short exact sequence

$$1 \longrightarrow 1 + \mathfrak{p}_F \longrightarrow \mathcal{O}_F^* \longrightarrow k_F^* \longrightarrow 1.$$

We have shown the first part of the following theorem.

11.8 Theorem. *Let F be a local field and $q = \#(k_F)$, a power of a prime number p . Then \mathcal{O}_F^* is the direct product of the subgroups $\mu_{q-1}(F)$ and $1 + \mathfrak{p}_F$. The kernel of the restriction of λ_F to $\mu(F)$ is the p -primary part of $\mu(F)$.*

PROOF. Let $\zeta \in \mu(F)$. Write $\zeta = \eta\xi$ with $\eta, \xi \in \mu(F)$, $p \nmid o(\xi)$ and $o(\eta)$ a power of p . Let m be the order of ξ . The m -th cyclotomic polynomial splits over F and, therefore, over k_F as well. Since $p \nmid m$, the finite field k_F has a primitive m -th root of unity. Hence $m \mid q - 1$, that is $\xi \in \mu_{q-1}(F)$. So we have

$$\lambda_F(\zeta) = \lambda_F(\eta)\lambda_F(\xi) = \lambda_F(\xi) = \xi$$

and hence $\zeta = \eta$, if $\lambda_F(\zeta) = 1$. □

If the local field is of nonzero characteristic, then it is of the same characteristic as the residue class field. In this case the p -primary part of $\mu(F)$ is trivial and so $\mu(F) \cong k_F^*$.

The multiplicative group of a local field F is the direct product of \mathcal{O}_F^* and the infinite cyclic subgroup generated by a uniformizer. So for this multiplicative group we have:

11.9 Corollary. *Let F be a local field, π a uniformizer of F and $q = \#(k_F)$. Then*

$$F^* = (1 + \mathfrak{p}_F) \cdot \mu_{q-1}(F) \cdot \langle \pi \rangle,$$

a direct product of subgroups. □

So for a determination of the multiplicative structure a local field F we can now focus on the group $1 + \mathfrak{p}_F$. This will be done in section 11.5.

11.3 Extensions

For cyclotomic extensions of local fields we have:

11.10 Lemma. *Let F be a local field of characteristic 0 with residue class field of characteristic p , $m \in \mathbb{N}^*$ and $E : F$ the m -th cyclotomic extension of F . Suppose that $p \nmid m$. Then:*

- (i) $\mathcal{O}_E = \mathcal{O}_F[\zeta]$, where ζ is a primitive m -th root of unity.
- (ii) *The extension $E : F$ is unramified and the canonical map $\text{Gal}(E : F) \rightarrow \text{Gal}(k_E : k_F)$ is an isomorphism. In particular $E : F$ is a cyclic extension.*

PROOF.

- (i) This follows from Corollary 7.26 as well as from Proposition 1.36.
- (ii) We have $E = F(\zeta)$ for a primitive m -th root of unity. Let g be the minimal polynomial of ζ over F . Then $g \mid X^m - 1$ (in $\mathcal{O}_F[X]$). So $\text{disc}(g) \mid \text{disc}(X^m - 1)$ in \mathcal{O}_F . Because $p \nmid m$, it follows that $v_F(\text{disc}(g)) = 0$. So $v_F(\mathfrak{d}_F(E)) = 0$. □

For a complete local field of characteristic $p \neq 0$ the m -th cyclotomic extension is the m' -th cyclotomic extension, where $m = p^k m'$ with $p \nmid m'$. It easily follows that in this case all cyclotomic extensions are unramified.

An extension of local fields is a totally ramified extension on top of an unramified extension:

11.11 Theorem. *Let $E : F$ be an extension of local fields and $q = \#(k_E)$. Then $E : F(\mu_{q-1})$ is a totally ramified extension and $F(\mu_{q-1}) : F$ is the maximal unramified subextension of $E : F$.*

PROOF. By Theorem 11.8 E contains a primitive $(q - 1)$ -st root of unity ζ . Consider the intermediate field $F' = F(\zeta)$ of the extension $E : F$. By Lemma 11.10 the extension $F' : F$ is unramified. The residue class field of F' has a primitive $(q - 1)$ -st root of unity. So $f_{F'}^{(E)} = 1$ and hence $[E : F'] = e_{F'}^{(E)} f_{F'}^{(E)} = e_{F'}^{(E)}$. By Theorem 7.50 the composition of unramified extensions is unramified. So $F' : F$ is the maximal unramified subextension. \square

Let e be the ramification index and f the residue class degree. If $\alpha_1, \dots, \alpha_f \in \mathcal{O}_{F'}$ are such that $\bar{\alpha}_1, \dots, \bar{\alpha}_f$ is an k_F -basis of $k_{F'}$, then $\alpha_1, \dots, \alpha_f$ is an F -base of F' . For $\pi \in E$ with $v_E(\pi) = 1$ the elements $1, \pi, \dots, \pi^{e-1}$ form an F' -basis of E . Thus we obtain an F -basis of E : all $\alpha_i \pi^j$ with $1 \leq i \leq f$ and $0 \leq j \leq e - 1$. For an extension of local fields this gives an extra meaning to the basis described in Theorem 10.41.

11.12 Corollary. *Let $E : F$ be a finite extension of local fields and $q = \#(k_E)$. Then $E : F$ is unramified if and only if it is contained in the $(q - 1)$ -st cyclotomic extension of F .* \square

11.13 Corollary. *Let F be a local field of characteristic 0 and \bar{F} an algebraic closure of K . Then for each $n \in \mathbb{N}^*$ there is a unique intermediate field E of $\bar{F} : F$ with $E : F$ unramified of degree n .*

PROOF. Suppose the residue class field of F has q elements. Let $n \in \mathbb{N}^*$ and $\zeta \in \bar{F}$ a primitive $(q^n - 1)$ -st root of unity. Take $E = F(\zeta)$. Then $k_E : k_F$ is the $(q^n - 1)$ -st cyclotomic extension of k_F . By Lemma 11.3 $E : F$ is cyclic of degree n , the order of \bar{q} in $(\mathbb{Z}/q^n - 1)^*$. If $E' : F$ is unramified and of degree n , then $f_F^{(E')} = n$. By Theorem 11.11 $E' : F$ is the $(q^n - 1)$ -st cyclotomic extension of F . \square

11.14 Example. Let p be a prime. The field \mathbb{Q}_p has a unique unramified quadratic extension $E : \mathbb{Q}_p$, the $(p^2 - 1)$ -st cyclotomic extension. For $p = 2$ we have $E = \mathbb{Q}_2(\zeta_3) = \mathbb{Q}_2(\sqrt{-3})$. For odd p and a squarefree $m \in \mathbb{Z}$ such that $\left(\frac{m}{p}\right) = -1$, set $K = \mathbb{Q}(\sqrt{m})$ and $\mathfrak{p} = p\mathcal{O}_K$. Then $E = \mathbb{Q}(\sqrt{m})_{\mathfrak{p}} = \mathbb{Q}_p(\sqrt{m})$.

Integral primitive elements

Let $E : F$ be an extension of local fields. The following proposition will be used in chapter 17 when studying further properties of higher ramification groups.

11.15 Proposition. *There exists a $\gamma \in \mathcal{O}_E$ such that $\mathcal{O}_E = \mathcal{O}_F[\gamma]$.*

PROOF. Let $\alpha \in \mathcal{O}_E$ be such that $\bar{\alpha} \in k_E$ is a primitive element of $k_E : k_F$ and $f \in \mathcal{O}_F[X]$ a monic polynomial such that $\bar{f} \in k_F[X]$ is the minimal polynomial of $\bar{\alpha}$ over k_F . Then $f(\alpha) \in \mathfrak{p}_F$ and so $v_E(\alpha) \geq 1$. If $v_E(\alpha) = 1$, then we can take $\gamma = \alpha$: by the proof of Theorem 10.41, or the remark following Theorem 11.11, \mathcal{O}_E

is generated by products $\alpha^i f(\alpha)^j$ and this implies $\mathcal{O}_E = \mathcal{O}_F[\alpha]$. So we will assume that $v_E(\alpha) \geq 2$. Let π be a uniformizer of v_E . Then by Taylor's formula

$$f(\alpha + \pi) = f(\alpha) + \pi f'(\alpha) + \pi^2 \beta,$$

where $\beta \in \mathcal{O}_E$. The irreducible polynomial $\bar{f} \in k_F[X]$ has no multiple roots, so $f'(\alpha) \in \mathcal{O}_E^*$. It follows that $v_E(\alpha + \pi) = 1$ and in this case $\gamma = \alpha + \pi$ will do. \square

11.4 Exponential function and logarithm

In the sequel we will need more knowledge of the structure of the multiplicative group of a local field than we already derived in the previous sections. For complete archimedean fields the exponential function connects the additive structure to the multiplicative structure: e.g. on \mathbb{R} the exponential function is an isomorphism from the additive group \mathbb{R} to the multiplicative group $\mathbb{R}^{>0}$, the logarithm being its inverse. Usually the additive structure is easier to deal with than the multiplicative structure. The German mathematician Hensel introduced the exponential and logarithmic function on local fields. The starting points are the power series representations of these functions just as they are in the archimedean case.

In this section F is a local field of characteristic 0 with a residue class field of characteristic p . For simplicity we put $v = v_F$, $\mathfrak{p} = \mathfrak{p}_F$, $e = v(p) = e_{\mathbb{Q}_p}^{(F)}$ and $f = f_{\mathbb{Q}_p}^{(F)} = [k_F : \mathbb{F}_p]$.

Over a field of characteristic 0 we have formal power series

$$\exp x = \sum_{n=0}^{\infty} \frac{x^n}{n!} \quad \text{and} \quad \log(1+x) = \sum_{n=1}^{\infty} (-1)^{n-1} \frac{x^n}{n}.$$

The following relations hold, say in the formal power series ring $\mathbb{Q}[[T]]$, and where x and y are formal power series in T with constant term 0:

$$\begin{aligned} \exp(x+y) &= \exp x \cdot \exp y, & \exp \log(1+x) &= 1+x, \\ \log(1+x)(1+y) &= \log(1+x) + \log(1+y), & \log \exp x &= x. \end{aligned}$$

First we consider the exponential function.

11.16 Definition. The *exponential function* \exp on F is given by a series:

$$\exp(\alpha) = \sum_{n=0}^{\infty} \frac{\alpha^n}{n!}$$

for all $\alpha \in F$ for which the series converges.

11 Local Fields

By Proposition 10.34 the series converges if and only if the valuation of the n -th term tends to infinity for $n \rightarrow \infty$. We need to know the valuation of $n!$. Hensel gave a nice computation of its value. It goes as follows. Use the base p for a representation of n :

$$n = a_0 + a_1p + a_2p^2 + \cdots + a_kp^k \quad \text{with } 0 \leq a_i < p \text{ and } a_k \neq 0. \quad (11.1)$$

Let s_n be the p -adic digit sum of n , i.e. $s_n = a_0 + a_1 + \cdots + a_k$.

11.17 Lemma. *Let $n \in \mathbb{N}^*$. Then $v_p(n!) = \frac{n - s_n}{p - 1}$.*

PROOF. Let the p -adic notation of n be as in (11.1). Then

$$\begin{aligned} v_p(n!) &= \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots + \left\lfloor \frac{n}{p^k} \right\rfloor \\ &= (a_1 + \cdots + a_kp^{k-1}) + (a_2 + \cdots + a_kp^{k-2}) + \cdots + (a_{k-1} + a_kp) + a_k \\ &= a_1 + a_2(1+p) + a_3(1+p+p^2) + \cdots + a_k(1+p+\cdots+p^{k-1}) \\ &= a_1 \frac{p-1}{p-1} + a_2 \frac{p^2-1}{p-1} + \cdots + a_k \frac{p^k-1}{p-1} \\ &= \frac{1}{p-1} (a_0 + a_1p + a_2p^2 + \cdots + a_kp^k - (a_0 + a_1 + a_2 + \cdots + a_k)) \\ &= \frac{n - s_n}{p-1}. \end{aligned} \quad \square$$

11.18 Proposition. *Let $\alpha \in F$. Then:*

- (i) *the series $\sum_{n=0}^{\infty} \frac{\alpha^n}{n!}$ converges if and only if $v(\alpha) > \frac{e}{p-1}$;*
- (ii) *$v(\exp \alpha - 1) = v(\alpha)$ for each α with $v(\alpha) > \frac{e}{p-1}$;*
- (iii) *for each $t > \frac{e}{p-1}$ the map*

$$\exp: \mathfrak{p}^t \rightarrow 1 + \mathfrak{p}^t$$

is an injective group homomorphism from the additive group \mathfrak{p}^t to the multiplicative group $1 + \mathfrak{p}^t$.

It will turn out that the homomorphism in (iii) is in fact an isomorphism. The logarithm will be its inverse.

PROOF.

(i) By lemma 11.17

$$\begin{aligned} v\left(\frac{\alpha^n}{n!}\right) &= n \cdot v(\alpha) - e \cdot v_p(n!) = n \cdot v(\alpha) - \frac{e}{p-1}(n - s_n) \\ &= n\left(v(\alpha) - \frac{e}{p-1}\right) + \frac{e \cdot s_n}{p-1} \geq n\left(v(\alpha) - \frac{e}{p-1}\right). \end{aligned}$$

So the n -th term tends to infinity if $v(\alpha) > \frac{e}{p-1}$. If $v(\alpha) \leq \frac{e}{p-1}$, then the series diverges, since $s_n = 1$ for infinitely many n .

(ii) $\exp \alpha - 1 = \alpha + \sum_{n=2}^{\infty} \frac{\alpha^n}{n!} = \alpha + \alpha \sum_{n=2}^{\infty} \frac{\alpha^{n-1}}{n!}$ and for each $n \geq 2$ we have $s_n \geq 1$.

So

$$v\left(\frac{\alpha^{n-1}}{n!}\right) = (n-1)v(\alpha) - e \frac{n - s_n}{p-1} \geq (n-1)\left(v(\alpha) - \frac{e}{p-1}\right) > 0.$$

(iii) By (ii) the map $\exp: \mathfrak{p}^t \rightarrow 1 + \mathfrak{p}^t$ is defined. The formal properties of \exp imply that $\exp(\alpha_1 + \alpha_2) = \exp \alpha_1 \cdot \exp \alpha_2$ for $\alpha_1, \alpha_2 \in \mathfrak{p}^t$. From (i) it follows that $\exp(\alpha) \neq 1$ for $\alpha \neq 0$, so the group homomorphism is injective. \square

The logarithm on F is defined as follows.

11.19 Definition. The *logarithm* on F is given by a series:

$$\log(\alpha) = \sum_{n=1}^{\infty} (-1)^{n-1} \frac{(\alpha - 1)^n}{n}$$

for all $\alpha \in F$ for which the series converges.

11.20 Proposition. Let $\alpha \in F$. Then

(i) the series $\sum_{n=1}^{\infty} (-1)^{n-1} \frac{(\alpha - 1)^n}{n}$ converges if and only if $\alpha \in 1 + \mathfrak{p}$;

(ii) $v(\log \alpha) = v(\alpha - 1)$ for each $\alpha \in F$ with $v(\alpha - 1) > \frac{e}{p-1}$.

(iii) the map

$$\log: 1 + \mathfrak{p} \rightarrow F$$

is a homomorphism from the multiplicative group $1 + \mathfrak{p}$ to the additive group F . For each $t > \frac{e}{p-1}$ it induces by restriction a homomorphism

$$\log: 1 + \mathfrak{p}^t \rightarrow \mathfrak{p}^t.$$

PROOF.

$$(i) \ v\left(\frac{(\alpha-1)^n}{n}\right) = n \cdot v(\alpha-1) - v(n) \geq n \cdot v(\alpha-1) - \frac{e \log n}{\log p} \rightarrow \infty \text{ if } n \rightarrow \infty.$$

$$(ii) \ \log \alpha = (\alpha-1) + (\alpha-1) \sum_{n=2}^{\infty} (-1)^n \frac{(\alpha-1)^{n-1}}{n}. \text{ It suffices to show that}$$

$$v\left(\frac{(\alpha-1)^{n-1}}{n}\right) = (n-1) \cdot v(\alpha-1) - v(n) > 0 \text{ for } n \geq 2. \text{ For } p \nmid n \text{ we have } v(n) = 0, \text{ so assume that } p \mid n. \text{ Then } n \geq p \text{ and}$$

$$v\left(\frac{(\alpha-1)^{n-1}}{n}\right) \geq (n-1)v(\alpha-1) - \frac{e \log n}{\log p} > \frac{e(n-1)}{p-1} - \frac{e \log n}{\log p}.$$

We have to show that $\frac{n-1}{p-1} \geq \frac{\log n}{\log p}$ or, since $n \geq p$ and $p \geq 2$, that $\frac{n-1}{\log n} \geq \frac{p-1}{\log p}$. This follows from $\frac{x-1}{\log x}$ being monotone increasing for $x > 1$, which is easily seen by substitution of the monotonic increasing e^y for x :

$$\frac{x-1}{\log x} = \frac{e^y-1}{y} = \sum_{n=1}^{\infty} \frac{y^{n-1}}{n!}.$$

(iii) By (ii) the map $\log: 1 + \mathfrak{p}^t \rightarrow \mathfrak{p}^t$ is defined and the formal properties of \log imply that it is a homomorphism. \square

Since \exp and \log are formally inverses of each other, the preceding propositions imply the following.

11.21 Theorem. *Let $t \in \mathbb{N}$ with $t > \frac{e}{p-1}$. The maps*

$$\log: 1 + \mathfrak{p}^t \rightarrow \mathfrak{p}^t \quad \text{and} \quad \exp: \mathfrak{p}^t \rightarrow 1 + \mathfrak{p}^t$$

are group isomorphisms and inverses of each other. \square

The subgroups \mathfrak{p}^t and $1 + \mathfrak{p}^t$ of respectively \mathcal{O}_F and \mathcal{O}_F^* are of finite index. So the groups \mathcal{O}_F and \mathcal{O}_F^* have much in common. An important consequence concerns the group F^n of n -th powers of F^* .

11.22 Theorem. *Let $n \in \mathbb{N}^*$. Then $1 + \mathfrak{p}^t \subseteq F^{*n}$ for $t > e \cdot v_p(n) + \frac{e}{p-1}$.*

PROOF. Let $\alpha \in 1 + \mathfrak{p}^t$. Then $\log \alpha \in \mathfrak{p}^t$ because $t > \frac{e}{p-1}$. So $v(\frac{1}{n} \log \alpha) \geq t - v(n) = t - e \cdot v_p(n) > \frac{e}{p-1}$ and for $\beta = \exp(\frac{1}{n} \log \alpha) \in 1 + \mathfrak{p}^{t-v(n)}$ we have $\beta^n = \exp(\log \alpha) = \alpha$. Hence $\alpha \in F^{*n}$. \square

11.23 Corollary. *For each $n \in \mathbb{N}^*$ the index of F^{*n} in F^* is finite.*

PROOF. Let $n \in \mathbb{N}^*$. By the theorem there is a $t \in \mathbb{N}^*$ such that $1 + \mathfrak{p}^t \subseteq F^{*n} \cap \mathcal{O}_F^* = \mathcal{O}_F^{*n}$. The split short exact sequence

$$1 \longrightarrow \mathcal{O}_F^* \longrightarrow F^* \xrightarrow{v} \mathbb{Z} \longrightarrow 1$$

induces a split short exact sequence

$$1 \longrightarrow \mathcal{O}_F^*/\mathcal{O}_F^{*n} \longrightarrow F^*/F^{*n} \xrightarrow{v} \mathbb{Z}/n \longrightarrow 1.$$

So $F^*/F^{*n} \cong \mathcal{O}_F^*/\mathcal{O}_F^{*n} \times \mathbb{Z}/n$. The index of $1 + \mathfrak{p}^t$ in \mathcal{O}_F^* is finite: $\mathcal{O}_F^*/(1 + \mathfrak{p}^t) \cong (\mathcal{O}_F/\mathfrak{p}^t)^*$. From $1 + \mathfrak{p}^t \subseteq \mathcal{O}_F^{*n} \subseteq \mathcal{O}_F^*$ follows that the index of \mathcal{O}_F^{*n} in \mathcal{O}_F^* is finite as well. \square

11.5 The multiplicative group

Let F be a local field with k_F of characteristic p and $\mathfrak{p} = \mathfrak{p}_F$. First we show that $1 + \mathfrak{p}$ is a \mathbb{Z}_p -module in a natural way. Writing operators of this multiplicative group as exponents, we will define α^z for $\alpha \in 1 + \mathfrak{p}$ and $z \in \mathbb{Z}_p$. Its definition rests on the following lemma.

11.24 Lemma. *Let $\alpha \in 1 + \mathfrak{p}$ and $z = \lim_{n \rightarrow \infty} z_n$ with $z_n \in \mathbb{Z}$ for all $n \in \mathbb{N}^*$. Then the sequence $(\alpha^{z_n})_n$ converges in $1 + \mathfrak{p}$. If also $z = \lim_{n \rightarrow \infty} z'_n$ with $z'_n \in \mathbb{Z}$ for all $n \in \mathbb{N}^*$, then*

$$\lim_{n \rightarrow \infty} \alpha^{z'_n} = \lim_{n \rightarrow \infty} \alpha^{z_n}.$$

PROOF. For each $m \in \mathbb{N}^*$ the group $(1 + \mathfrak{p}^m)/(1 + \mathfrak{p}^{m+1})$ is of order $q = \#(k_F/\mathfrak{p})$. It follows that for each $m \in \mathbb{N}^*$ the group $(1 + \mathfrak{p})/(1 + \mathfrak{p}^{m+1})$ is of order q^m , that is

$$\alpha^{p^m} \equiv 1 \pmod{\mathfrak{p}^{m+1}} \quad \text{for all } m \in \mathbb{N}^*.$$

Put $v_{\mathfrak{p}}(z_{n+1} - z_n) = a_n$ and $v_{\mathfrak{p}}(z'_n - z_n) = b_n$. Then $\lim_{n \rightarrow \infty} a_n = \infty$ and $\lim_{n \rightarrow \infty} b_n = \infty$. Then

$$\frac{\alpha^{z_{n+1}}}{\alpha^{z_n}} = \alpha^{z_{n+1} - z_n} \equiv 1 \pmod{\mathfrak{p}^{a_n+1}} \quad \text{and} \quad \frac{\alpha^{z'_n}}{\alpha^{z_n}} = \alpha^{z'_n - z_n} \equiv 1 \pmod{\mathfrak{p}^{b_n+1}}.$$

And so

$$\alpha^{z_{n+1}} \equiv \alpha^{z_n} \pmod{\mathfrak{p}^{a_n+1}} \quad \text{and} \quad \alpha^{z'_n} \equiv \alpha^{z_n} \pmod{\mathfrak{p}^{b_n+1}}.$$

It follows that the sequence $(\alpha^{z_n})_n$ converges and that the limit does not depend on the choice of the sequence $(z_n)_n$. \square

11.25 Definition. Let F be a local field with k_F of characteristic p , $\alpha \in 1 + \mathfrak{p}_F$ and $z \in \mathbb{Z}_p$. Then the power α^z is defined by

$$\alpha^z = \lim_{n \rightarrow \infty} \alpha^{z_n},$$

where $(z_n)_n$ is a sequence in \mathbb{Z} converging to z .

11.26 Lemma. For each $m \in \mathbb{N}^*$ the abelian group $1 + \mathfrak{p}^m$ is a \mathbb{Z}_p -module under

$$\mathbb{Z}_p \times (1 + \mathfrak{p}^m) \longrightarrow 1 + \mathfrak{p}^m, \quad (z, \alpha) \mapsto \alpha^z.$$

PROOF. Let $z = \lim_{n \rightarrow \infty} z_n$ with $z_n \in \mathbb{Z}$ and $\alpha \in 1 + \mathfrak{p}^m$. Then $\alpha^{z_n} \in 1 + \mathfrak{p}^m$ for all n , because $1 + \mathfrak{p}^m$ is a subgroup of F^* . Hence $\alpha^z \in 1 + \mathfrak{p}^m$. Let also $\beta \in 1 + \mathfrak{p}^m$ and $w = \lim_{n \rightarrow \infty} w_n$ with $w_n \in \mathbb{Z}$. Then for each n :

$$(\alpha\beta)^{z_n} = \alpha^{z_n} \beta^{z_n}, \quad \alpha^{z_n + w_n} = \alpha^{z_n} \alpha^{w_n} \quad \text{and} \quad \alpha^{z_n w_n} = (\alpha^{z_n})^{w_n}.$$

So by the well-known rules for limits we obtain

$$(\alpha\beta)^z = \alpha^z \beta^z, \quad \alpha^{z+w} = \alpha^z \alpha^w \quad \text{and} \quad \alpha^{zw} = (\alpha^z)^w.$$

This means that under $(z, \alpha) \mapsto \alpha^z$ the group $1 + \mathfrak{p}^m$ is a \mathbb{Z}_p -module. □

We can now determine the structure of the multiplicative group of a local field of characteristic 0.

11.27 Theorem. Let F be a local field of characteristic 0 with k_F of characteristic p , $[F : \mathbb{Q}_p] = d$ and $w = \#(\mu(F))$. Then

$$F^* \cong \mathbb{Z} \oplus (\mathbb{Z}/w) \oplus \mathbb{Z}_p^d.$$

PROOF. Let π be a uniformizer of v_F and $\#(k_F) = q$. Then by Corollary 11.9

$$F^* = \langle \pi \rangle \cdot \mu_{q-1}(F) \cdot (1 + \mathfrak{p}_F).$$

Since \mathbb{Z}_p is a principal ideal domain the ring \mathcal{O}_F is a free \mathbb{Z}_p -module of rank d . For n sufficiently large the map $\log: 1 + \mathfrak{p}_F^n \rightarrow \mathfrak{p}_F^n$ is an isomorphism of \mathbb{Z}_p -modules (Theorem 11.21). So $1 + \mathfrak{p}_F^n \cong \pi^n \mathcal{O}_F \cong \mathcal{O}_F \cong \mathbb{Z}_p^d$. The index of $1 + \mathfrak{p}_F^n$ in $1 + \mathfrak{p}_F$ is finite, so the \mathbb{Z}_p -module $1 + \mathfrak{p}_F$ is of rank d as well. Its torsion subgroup consists of the roots of unity of F of order a power of p . By Theorem 11.8 this subgroup is the kernel of $\lambda_F: \mu(F) \rightarrow \mu_{q-1}(F)$. □

EXERCISES

- Let p be a prime number. By Corollary 11.9

$$\mathbb{Q}_p^* = (1 + p\mathbb{Z}_p) \cdot \mu_{p-1} \cdot \langle p \rangle.$$

- Show that $(1 + p\mathbb{Z}_p)^2 = 1 + p\mathbb{Z}_p$ if p is odd.
- Show that for odd p the group $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ is noncyclic of order 4, its elements being represented by 1, p , u and pu , where $u \in \mathbb{Z}$ represents a generator of the cyclic group \mathbb{F}_p^* .

- (iii) Show that $(1 + 2\mathbb{Z}_2)^2$ has index 2 in $1 + 2\mathbb{Z}_2$.
2. Let p be a prime number, $r \in \mathbb{N}^*$, $K = \mathbb{Q}(\zeta_{p^r})$ and \mathfrak{p} the prime of K above p . Compute $\mu(K)$ and $\mu(K_{\mathfrak{p}})$.
 3. Let $E : F$ be a totally tamely ramified Galois extension of local fields, v the discrete valuation of E and $[E : F] = n$. Show that there is a $\pi \in E$ with $v(\pi) = 1$ and $\pi^n \in F$. (Use exercise 17 of chapter 7.)
 4. Let m and n be different squarefree integers $\neq 1$. Put $k = mn / \gcd(m, n)^2$ and let p be an odd prime such that $p \mid m$, $p \mid n$ and $\left(\frac{k}{p}\right) = -1$. Show that the completions of the fields $\mathbb{Q}(\sqrt{m})$ and $\mathbb{Q}(\sqrt{n})$ with respect to the prime above p are not isomorphic.
 5.
 - (i) Let p be an odd prime. Show that the group $1 + p\mathbb{Z}_p$ is a subgroup of the group \mathbb{Q}_p^{*2} of squares in \mathbb{Q}_p^* .
 - (ii) Show that $\mathbb{Q}_p^* / \mathbb{Q}_p^{*2}$ is a noncyclic group of order 4.
 - (iii) Prove that inside a given algebraic closure of \mathbb{Q}_p there are exactly 3 quadratic extensions of \mathbb{Q}_p .
 6.
 - (i) Show that the group $1 + 8\mathbb{Z}_2$ is a subgroup of the group \mathbb{Q}_2^{*2} of squares in \mathbb{Q}_2^* .
 - (ii) Show that $\mathbb{Q}_2^* / \mathbb{Q}_2^{*2}$ is 2-elementary group of order 8.
 - (iii) Prove that inside a given algebraic closure of \mathbb{Q}_2 there are exactly 7 quadratic extensions of \mathbb{Q}_2 .
 - (iv) Give for each of the seven quadratic extensions of \mathbb{Q}_2 a primitive element. Which one is unramified?

12 Galois Modules

Galois theory is a powerful tool when investigating field extensions. The Galois group of a Galois extension $L : K$ is a group of automorphisms of L and as such it acts on the field L . The Galois group acts on many structures associated to L as well, e.g. it acts on the multiplicative group L^* , the ring \mathcal{O}_L , the group \mathcal{O}_L^* and the group $\mathbb{I}(L)$ of fractional ideals. Group cohomology applies in these cases and is usually referred to as *Galois cohomology*. It will be used in the next chapters, however, not in full generality. Only the special case of the cohomology of cyclic groups will be used. It is described in section 12.2. In section 12.3 many examples of Galois cohomology groups for cyclic number field extensions are given. These examples will be used in later chapters. The action of a Galois group often comes with extra structure. This is formalized in section 12.4 and is particularly interesting when dealing with noncyclic Galois groups. Special cases are studied in the last two sections.

12.1 Modules over a group

Modules over a group are essentially modules over the group ring of the group.

12.1 Terminology. Let G be a group. If G operates on an abelian group A via automorphisms of A , then A , equipped with this action, is called a *G -module*. Equivalently, a G -module A consists of an abelian group A together with a group homomorphism $G \rightarrow \text{Aut}(A)$. If, more generally, for a commutative ring R the group G acts on an R -module A via R -automorphisms, the action corresponds to a group homomorphism $G \rightarrow \text{Aut}_R(A)$, where Aut_R stands for the group of R -automorphisms. For K a field and V a K -vector space, a group homomorphism $G \rightarrow \text{Aut}_K(V)$ is usually called a *representation* over K of G . If V is of finite dimension, then the dimension of V is called the *degree* of the representation.

In section 18.4 representations over \mathbb{C} will be used for Artin's generalization of the L -functions as defined for abelian number fields in chapter 9.

Using the multiplicative notation for G and the additive notation for A , a G -action on A comes down to a map

$$G \times A \rightarrow A, \quad (\sigma, a) \mapsto \sigma a$$

such that for all $a, b \in A$ and $\sigma, \tau \in G$:

$$\begin{aligned}(\sigma\tau)a &= \sigma(\tau a), \\ \sigma(a + b) &= \sigma a + \sigma b, \\ 1a &= a.\end{aligned}$$

12.2 Definition. Let G be a (multiplicative) group. The *group ring* $\mathbb{Z}[G]$ of G is the free abelian group with G as basis equipped with the multiplication induced by the group multiplication in G :

$$\sum_{\sigma} n_{\sigma}\sigma \cdot \sum_{\tau} m_{\tau}\tau = \sum_{\sigma,\tau} n_{\sigma}m_{\tau}\sigma\tau,$$

where $n_{\sigma}, m_{\tau} \in \mathbb{Z}$. More generally, the *group algebra* $R[G]$ over a commutative ring R is the free R -module on G equipped with the ring multiplication induced by the group multiplication on the basis elements. Its elements are $\sum_{\sigma} a_{\sigma}\sigma$ with $a_{\sigma} \in R$ for all $\sigma \in G$.

For A a G -module, the group homomorphism $G \rightarrow \text{Aut}(A)$ extends to a ring homomorphism $\mathbb{Z}[G] \rightarrow \text{End}(A)$, where $\text{End}(A)$ is the ring of endomorphisms of the abelian group A . Thus A becomes a $\mathbb{Z}[G]$ -module. On the other hand a $\mathbb{Z}[G]$ -module A is a G -module by restriction of the operations to the basis G of $\mathbb{Z}[G]$. We will switch freely between the notions of G -module and $\mathbb{Z}[G]$ -module. A $\mathbb{Z}[G]$ -module homomorphism $f: A \rightarrow B$ corresponds to a G -module homomorphism in the sense that it is a homomorphism of abelian groups satisfying

$$f(\sigma a) = \sigma f(a) \quad \text{for all } a \in A \text{ and } \sigma \in G.$$

For R a commutative ring $R[G]$ -modules A are R -modules equipped with an action of G on A by R -linear maps. In particular, representations over \mathbb{C} of a group G correspond to $\mathbb{C}[G]$ -modules.

12.3 Definitions and notations.

- a) The *norm element* of a finite group G is the element $\sum_{\sigma \in G} \sigma$ of $\mathbb{Z}[G]$. It is denoted by N_G . If G is generated by a subset X of G , then also the notation N_X is used and if $X = \{\sigma\}$, a one element set, then we may write N_{σ} .
- b) Let A be a G -module. Then the G -module of G -invariants of A is the G -submodule

$$A^G = \{ a \in A \mid \sigma a = a \text{ for all } \sigma \in G \} = \bigcap_{\sigma \in G} \text{Ker}(1 - \sigma: A \rightarrow A).$$

It is the largest G -submodule with trivial G -action. Notations like A^X and A^{σ} for X and σ as above are used as well.

- c) Let A be a G -module. Then the G -module of G -co-invariants of A is the quotient G -module of A by the G -submodule generated by all $a - \sigma a$ with $a \in A$ and $\sigma \in G$:

$$A_G = A / \sum_{\sigma \in G} (1 - \sigma)A.$$

It is the largest quotient G -module with trivial G -action. The class of $a \in A$ in the quotient module A_G will often be denoted by \bar{a} . Again we have notations A_X and A_σ .

Trivial but important identities for norm elements are:

12.4 Lemma. *Let H, H_1 and H_2 be subgroups of a finite group G . Then:*

- (i) *If $H_1 \leq H_2$, then $N_{H_1}N_{H_2} = \#(H_1) \cdot N_{H_2}$.*
- (ii) $(N_H)^2 = \#(H) \cdot N_H$.
- (iii) *If H_1H_2 is a subgroup of G , then $N_{H_1}N_{H_2} = \#(H_1 \cap H_2) \cdot N_{H_1H_2}$.*

PROOF. (ii) follows from (i), and (i) follows from $\sigma N_{H_2} = N_{H_2}$ for all $\sigma \in H_1$, or, alternatively, apply (iii) to $H_1 \leq H_1H_2$. For (iii) note that the $\#(H_1)\#(H_2)$ terms in $N_{H_1}N_{H_2}$ correspond to the elements of $H_1 \times H_2$, whereas $\text{Ker}(H_1 \times H_2 \rightarrow H_1H_2) \cong H_1 \cap H_2$. \square

The following will be frequently used when studying group actions on abelian groups.

12.5 Lemma. *Let G be a group of order n acting on an abelian group A . Then multiplication by N_G induces a homomorphism*

$$\bar{N}_G: A_G \longrightarrow A^G, \quad \bar{a} \mapsto N_G a$$

of abelian groups. The kernel and the cokernel of this homomorphism are killed¹ by n . In particular the homomorphism is an isomorphism if multiplication by n is an automorphism of A .

PROOF. It follows from $\sigma N_G = N_G = N_G \sigma$ that multiplication by N_G induces a homomorphism $A_G \rightarrow A^G$. For $\bar{a} \in A_G$ with $N_G a = 0$ one has $\bar{n}\bar{a} = \overline{N_G a} = 0$. And for $a \in A^G$ we have $na = N_G a$. \square

Associated to a group module are series of abelian groups: the homology groups and the cohomology groups. Here a short description in terms of derived functors is given. *In this book no use is made of the full theory of group (co)homology.*

Let G be a group. The functor $A \mapsto A_G$ is a right exact functor from G -modules to abelian groups. For $m \in \mathbb{N}$ its m -th left derived functor is denoted by $H_m(G, -)$.

¹Terminology: an abelian group A is killed by n if $na = 0$ for all $a \in A$; a not necessarily abelian multiplicative group G has exponent n if $g^n = 1$ for all $g \in G$.

The group $H_m(G, A)$ is called the m -th homology group of G with coefficients in A . In particular we have $H_0(G, A) = A_G$.

The functor $A \mapsto A^G$ is a left exact functor from G -modules to abelian groups. For $m \in \mathbb{N}$ its m -th right derived functor is denoted by $H^m(G, -)$. The group $H^m(G, A)$ is called the m -th cohomology group of G with coefficients in A . In particular we have $H^0(G, A) = A^G$.

The Tate cohomology groups $\hat{H}^m(G, A)$ of a finite group G with coefficients in a G -module A are defined for all $m \in \mathbb{Z}$:

$$\hat{H}^m(G, A) = \begin{cases} H^m(G, A) & \text{if } m \geq 1, \\ \text{Coker}(A_G \xrightarrow{\overline{N}_G} A^G) & \text{if } m = 0, \\ \text{Ker}(A_G \xrightarrow{\overline{N}_G} A^G) & \text{if } m = -1, \\ H_{-m-1}(G, A) & \text{if } m \leq -2. \end{cases}$$

By definition we have the exact sequence

$$0 \longrightarrow \hat{H}^{-1}(G, A) \longrightarrow A_G \xrightarrow{\overline{N}_G} A^G \longrightarrow \hat{H}^0(G, A) \longrightarrow 0.$$

By Lemma 12.5 the groups $\hat{H}^m(G, A)$ are killed by $n = \#(G)$ for $m = -1, 0$. In fact this holds for all $m \in \mathbb{Z}$. In particular, if multiplication by n is an automorphism of A , then $\hat{H}^m(G, A) = 0$ for all $m \in \mathbb{Z}$.

For G cyclic one shows that $\hat{H}^m(G, A) = \hat{H}^{m+2}(G, A)$, so for such G the above exact sequence can be written as

$$0 \longrightarrow \hat{H}^1(G, A) \longrightarrow A_G \xrightarrow{\overline{N}_G} A^G \longrightarrow \hat{H}^0(G, A) \longrightarrow 0$$

and can be used as a definition of $\hat{H}^0(G, A)$ and $\hat{H}^1(G, A)$, as will be done in the next section. In this context it is customary to delete the $\hat{}$ in the notation.

12.2 Cohomology of cyclic groups

The Tate cohomology groups of a cyclic group have a simple description. This description is taken here to be their definition. The general notion of group cohomology is not used in this book.

12.6 Definition and notation. Let G be a cyclic group of order n generated by σ . Then elements Δ and N of $\mathbb{Z}[G]$ are defined as follows

$$\Delta = 1 - \sigma \quad \text{and} \quad N = 1 + \sigma + \cdots + \sigma^{n-1}.$$

For A a G -module the homomorphisms $a \mapsto \Delta a$ and $a \mapsto Na$ are denoted by Δ_A and N_A respectively. So $N = N_G$ and in the notation N_A the group G is understood. Similarly for Δ , in which case, moreover, the generator σ is not specified.

12.7 Lemma. *Let G be a finite cyclic group and A a G -module. Then $\text{Im}(\Delta_A) \subseteq \text{Ker}(N_A)$ and $\text{Im}(N_A) \subseteq \text{Ker}(\Delta_A)$.*

PROOF. This follows from $N\Delta = \Delta N = 1 - \sigma^n = 0$. □

12.8 Definition. Let G be a cyclic group, generated by an element σ of order n . Then the 0-th and the 1-st *cohomology group* of a G -module A are defined respectively as follows:

$$H^0(A) = \text{Ker}(\Delta_A) / \text{Im}(N_A) \quad \text{and} \quad H^1(A) = \text{Ker}(N_A) / \text{Im}(\Delta_A).$$

(Clearly, these groups do not depend on the choice of the generator σ .)

There is some variation in the terminology. For cyclic G , the ' i -th cohomology group (for $i = 0, 1$) of A ' stands for the ' i -th Tate cohomology group of G with values in A '. Here the emphasis is on the module, not on the group.

A direct consequence of the definition is the following.

12.9 Proposition. *Let G be a cyclic group of order n generated by σ and A a G -module. Then we have exact sequences*

$$0 \longrightarrow H^1(A) \longrightarrow \text{Coker}(\Delta_A) \xrightarrow{\overline{N}_A} \text{Ker}(\Delta_A) \longrightarrow H^0(A) \longrightarrow 0$$

and

$$0 \longrightarrow H^0(A) \longrightarrow \text{Coker}(N_A) \xrightarrow{\overline{\Delta}_A} \text{Ker}(N_A) \longrightarrow H^1(A) \longrightarrow 0. \quad \square$$

The first exact sequence is the same sequence as

$$0 \longrightarrow H^1(A) \longrightarrow A_G \xrightarrow{\overline{N}_G} A^G \longrightarrow H^0(A) \longrightarrow 0,$$

which shows that indeed the cohomology groups are the Tate cohomology groups $\hat{H}^0(G; A)$ and $\hat{H}^{-1}(G; A)$, see the remarks at the end of section 12.1.

Cohomology theories give rise to long exact sequences of cohomology groups. Due to the fact that in the cyclic case the cohomology is periodic with period 2, these long exact sequences wind up as a hexagon.

12.10 Theorem (The Exact Hexagon). *Let G be a finite cyclic group and let*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

be a short exact sequence of G -modules. Then an exact hexagon of cohomology groups is induced:

$$\begin{array}{ccc}
 & H^0(A) \longrightarrow H^0(B) & \\
 & \nearrow & \searrow \\
 H^1(C) & & H^0(C) \\
 & \nwarrow & \swarrow \\
 & H^1(B) \longleftarrow H^1(A) &
 \end{array}$$

PROOF. The Snake Lemma applied to the commutative diagram

$$\begin{array}{ccccccc}
 0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C \longrightarrow 0 \\
 & & \downarrow \Delta_A & & \downarrow \Delta_B & & \downarrow \Delta_C \\
 0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C \longrightarrow 0
 \end{array}$$

yields an exact sequence of kernels and cokernels

$$\begin{aligned}
 0 &\longrightarrow \text{Ker}(\Delta_A) \longrightarrow \text{Ker}(\Delta_B) \longrightarrow \text{Ker}(\Delta_C) \\
 &\longrightarrow \text{Coker}(\Delta_A) \longrightarrow \text{Coker}(\Delta_B) \longrightarrow \text{Coker}(\Delta_C) \longrightarrow 0.
 \end{aligned}$$

There is a similar exact sequence for N instead of Δ . Applying the Snake Lemma to the commutative diagram

$$\begin{array}{ccccccc}
 \text{Coker}(N_A) & \longrightarrow & \text{Coker}(N_B) & \longrightarrow & \text{Coker}(N_C) & \longrightarrow & 0 \\
 & & \overline{\Delta}_A \downarrow & & \overline{\Delta}_B \downarrow & & \overline{\Delta}_C \downarrow \\
 0 & \longrightarrow & \text{Ker}(N_A) & \longrightarrow & \text{Ker}(N_B) & \longrightarrow & \text{Ker}(N_C)
 \end{array}$$

yields an exact sequence

$$H^0(A) \longrightarrow H^0(B) \longrightarrow H^0(C) \longrightarrow H^1(A) \longrightarrow H^1(B) \longrightarrow H^1(C).$$

Interchanging the role of N and Δ yields a similar exact sequence and these two together form the exact hexagon. \square

A tool for making computations is the Herbrand quotient:

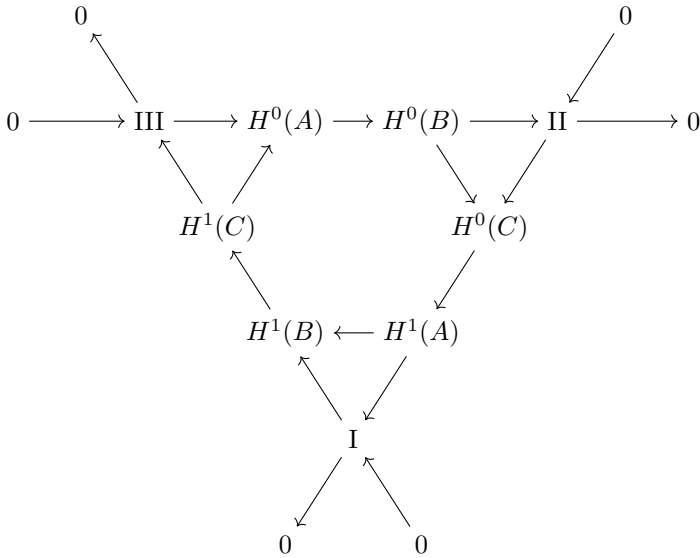
12.11 Definition. Let G be a finite cyclic group and A a G -module such that $H^0(A)$ and $H^1(A)$ are finite. Then the *Herbrand quotient* of A is the rational number

$$q(A) = \frac{\#(H^1(A))}{\#(H^0(A))}.$$

12.12 Proposition. Let G be a finite cyclic group and $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ a short exact sequence of G -modules. If for two of the three modules the Herbrand quotient is defined, then so for the third and

$$q(B) = q(A)q(C).$$

PROOF. The associated exact hexagon leads to a diagram with exact sequences:



If the Herbrand quotient of two of the modules A , B and C is defined, then four of the six abelian groups in the exact hexagon are finite and so are the remaining two. Because the alternating product of the orders in an exact sequence equals 1, we have

$$\frac{q(A)q(C)}{q(B)} = \frac{\#(H^1(A)) \cdot \#(H^0(B)) \cdot \#(H^1(C))}{\#(H^0(A)) \cdot \#(H^1(B)) \cdot \#(H^0(C))} = \frac{\#(\text{II}) \cdot \#(\text{I}) \cdot \#(\text{III})}{\#(\text{III}) \cdot \#(\text{II}) \cdot \#(\text{I})} = 1. \quad \square$$

12.13 Proposition. *Let G be a finite cyclic group and A a finite G -module. Then $q(A) = 1$.*

PROOF. From the exact sequence

$$0 \longrightarrow \text{Ker}(\text{N}_A) \longrightarrow A \xrightarrow{\text{N}_A} A \longrightarrow \text{Coker}(\text{N}_A) \longrightarrow 0$$

follows that $\#(\text{Ker}(\text{N}_A)) = \#(\text{Coker}(\text{N}_A))$ and together with the exactness of

$$0 \longrightarrow H^0(A) \longrightarrow \text{Coker}(\text{N}_A) \xrightarrow{\overline{\Delta_A}} \text{Ker}(\text{N}_A) \longrightarrow H^1(A) \longrightarrow 0$$

this implies that $\#(H^1(A)) = \#(H^0(A))$. □

12.14 Corollary. *Let G be a finite cyclic group and let A be a G -submodule of finite index in the G -module B . If one of the Herbrand quotients of A and B is defined, then so is the other and, moreover, $q(A) = q(B)$.*

PROOF. Apply Proposition 12.12 to the short exact sequence $0 \rightarrow B \rightarrow A \rightarrow B/A \rightarrow 0$ and use that $q(B/A) = 1$ by Proposition 12.13. □

The following proposition describes the cohomology of a type of module which will occur frequently.

12.15 Proposition. *Let $G = \langle \sigma \rangle$ be a cyclic group of order n and d a divisor of n , say $n = dm$. Let B be a torsion free abelian group and $A = \bigoplus_{i=1}^d B$ the G -module with the G -action*

$$\sigma(b_1, \dots, b_d) = (b_2, \dots, b_d, b_1).$$

Then $H^1(A) = 0$ and $H^0(A) \cong B/mB$.

PROOF. We have for $a = (b_1, \dots, b_d)$:

$$\begin{aligned} \Delta a &= (b_1 - b_2, b_2 - b_3, \dots, b_d - b_1), \\ \text{N}a &= m(b_1 + \dots + b_d, \dots, b_1 + \dots + b_d) \end{aligned}$$

and an easy calculation shows that

$$\begin{aligned} \text{Ker}(\Delta_A) &= \{ (b, \dots, b) \mid b \in B \} \cong B, \\ \text{Im}(\Delta_A) &= \{ (b_1, \dots, b_d) \in A \mid \sum b_i = 0 \} = \text{Ker}(\text{N}_A), \\ \text{Im}(\text{N}_A) &= \{ m(b, \dots, b) \mid b \in B \} \cong mB. \end{aligned} \quad \square$$

12.3 Galois cohomology of cyclic groups

This section contains computations of cohomology groups of some modules over the Galois group of a cyclic extension. Since the group is a Galois group it is customary to speak of Galois cohomology in such cases.

The cohomology groups of L and L^*

In this subsection $L : K$ is a Galois extension of degree n with $\text{Gal}(L : K) = G = \langle \sigma \rangle$. The additive group L and the multiplicative group L^* both are G -modules: the action of σ is given by $\sigma\alpha = \sigma(\alpha)$.

12.16 Theorem. $H^0(L) = 0$ and $H^1(L) = 0$.

PROOF. The action of Δ and N is given by

$$\Delta\alpha = \alpha - \sigma(\alpha) \quad \text{and} \quad N\alpha = \alpha + \sigma(\alpha) + \cdots + \sigma^{n-1}(\alpha) = \text{Tr}_K^L(\alpha).$$

The maps $\Delta_L, N_L : L \rightarrow L$ are K -linear. The trace map $\text{Tr}_K^L : L \rightarrow K$ is surjective (Corollary 1.30). So by the Main Theorem of Galois Theory

$$K = \text{Im}(\text{Tr}_K^L) = \text{Im}(N_L) \subseteq \text{Ker}(\Delta_L) = L^\sigma = K.$$

It follows that $H^0(L) = 0$ and also that $\text{Ker}(N_L) = \text{Im}(\Delta_L)$, since both are of dimension $n - 1$. \square

Alternatively, by the Normal Basis Theorem of Galois theory there is an $\alpha \in L$ such that $\alpha, \sigma(\alpha), \dots, \sigma^{n-1}(\alpha)$ is a K -basis of L . Apply Proposition 12.15. For fields of characteristic 0 the theorem follows directly from the fact that the map $L_G \rightarrow L^G$ induced by N_L is an isomorphism.

12.17 Theorem. $H^0(L^*) = K^*/N_K^L(L^*)$ and $H^1(L^*) = 1$.

PROOF. The action of Δ and N is given by

$$\Delta\alpha = \frac{\alpha}{\sigma(\alpha)} \quad \text{and} \quad N\alpha = \alpha \cdot \sigma(\alpha) \cdots \sigma^{n-1}(\alpha) = N_K^L(\alpha).$$

We have, again by the Main Theorem of Galois Theory

$$\begin{aligned} \text{Ker}(\Delta_{L^*}) &= \{ \alpha \in L^* \mid \sigma(\alpha) = \alpha \} = L^* \cap L^G = L^* \cap K = K^*, \\ \text{Im}(N_{L^*}) &= N_K^L(L^*). \end{aligned}$$

Hence $H^0(L^*) = K^*/N_K^L(L^*)$.

The group $\text{Im}(\Delta_{L^*})$ consists of all $\frac{\beta}{\sigma(\beta)}$ with $\beta \in L^*$ and the group $\text{Ker}(N_{L^*})$ is the subgroup of all $\alpha \in L^*$ with $N_K^L(\alpha) = 1$. We have to show that each such α is of the form $\frac{\beta}{\sigma(\beta)}$. Let $\alpha \in L^*$ such that $N_K^L(\alpha) = 1$. For $\gamma \in L^*$ we consider the element

$$\beta = \sum_{k=0}^{n-1} \left(\sigma^k(\gamma) \prod_{j=0}^k \sigma^j(\alpha) \right) = \sigma^{n-1}(\gamma) + \sum_{k=0}^{n-2} \left(\sigma^k(\gamma) \prod_{j=0}^k \sigma^j(\alpha) \right).$$

Apply σ :

$$\sigma(\beta) = \gamma + \sum_{k=0}^{n-2} \left(\sigma^{k+1}(\gamma) \prod_{j=0}^k \sigma^{j+1}(\alpha) \right) = \gamma + \sum_{k=1}^{n-1} \left(\sigma^k(\gamma) \prod_{j=1}^k \sigma^j(\alpha) \right).$$

So $\alpha\sigma(\beta) = \beta$. Is there a γ such that $\beta \neq 0$? Choose a $\vartheta \in L$ such that $L = K(\vartheta)$ and consider the elements $\beta = \beta_j$ for $\gamma = \vartheta^{j-1}$ for $j = 1, \dots, n$. They form the column vector Av , where

$$A = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \vartheta & \sigma(\vartheta) & \cdots & \sigma^{n-1}(\vartheta) \\ \vdots & \vdots & \ddots & \vdots \\ \vartheta^{n-1} & \sigma(\vartheta)^{n-1} & \cdots & \sigma^{n-1}(\vartheta)^{n-1} \end{pmatrix} \quad \text{and} \quad v = \begin{pmatrix} \alpha \\ \alpha\sigma(\alpha) \\ \vdots \\ \alpha\sigma(\alpha) \cdots \sigma^{n-1}(\alpha) \end{pmatrix}.$$

Since ϑ is primitive, the elements $\vartheta, \sigma(\vartheta), \dots, \sigma^{n-1}(\vartheta)$ are different. So the Vandermonde matrix A is invertible. Because $v \neq 0$ it follows that $Av \neq 0$. So $\beta_j \neq 0$ for some j . Therefore, $\alpha = \frac{\beta_j}{\sigma(\beta_j)}$. \square

The formula $H^1(L^*) = 1$ is known as *Hilbert's Theorem 90*.

The cohomology groups of $\mathbb{I}(S)$

Let R be a Dedekind domain, K the field of fractions of R , $L : K$ a cyclic extension, $G = \text{Gal}(L : K)$ and S the integral closure of R in L . The discrete valuations $v_{\mathfrak{q}}$ on L constitute an isomorphism

$$\mathbb{I}(S) \xrightarrow{\sim} \bigoplus_{\mathfrak{p}} \bigoplus_{\mathfrak{q}|\mathfrak{p}S} \mathbb{Z}$$

of G -modules, the direct sums being over the maximal ideals \mathfrak{p} of R and the maximal ideals \mathfrak{q} of S dividing $\mathfrak{p}S$. By Proposition 12.15 we have

$$H^1(\bigoplus_{\mathfrak{q}|\mathfrak{p}S} \mathbb{Z}) = 0 \quad \text{and} \quad H^0(\bigoplus_{\mathfrak{q}|\mathfrak{p}S} \mathbb{Z}) = \mathbb{Z}/e_{\mathfrak{p}}f_{\mathfrak{p}}.$$

Hence

$$H^1(\mathbb{I}(S)) = 1 \quad \text{and} \quad H^0(\mathbb{I}(S)) \cong \bigoplus_{\mathfrak{p}} \mathbb{Z}/e_{\mathfrak{p}}f_{\mathfrak{p}}.$$

For the norm N_K^L of fractional ideals we have by Proposition 7.67 a commutative diagram

$$\begin{array}{ccc} \mathbb{I}(S) & \xrightarrow{\sim} & \bigoplus_{\mathfrak{p} \in P} \bigoplus_{\mathfrak{q}|\mathfrak{p}S} \mathbb{Z} \\ \text{N}_K^L \downarrow & & \downarrow (f_{\mathfrak{p}} \cdot)_{\mathfrak{p}} \\ \mathbb{I}(R) & \xrightarrow{\sim} & \bigoplus_{\mathfrak{p} \in P} \mathbb{Z} \end{array}$$

where $f_{\mathfrak{p}} \cdot : \mathbb{Z} \rightarrow \mathbb{Z}$ is multiplication by $f_{\mathfrak{p}}$ for each $\mathfrak{p} \in \text{Max}(S)$. In particular we have:

12.18 Proposition. $H^1(\mathbb{I}(S)) = 1$ and if no prime ideal of R ramifies in L , then $H^0(\mathbb{I}(S)) = \mathbb{I}(R)/N_K^L(\mathbb{I}(S))$ (identifying $\mathbb{I}(R)$ with a subgroup of $\mathbb{I}(S)$). \square

So in the number field case we have in the terminology of section 6.4:

12.19 Corollary. Let $L : K$ be a cyclic extension of number fields, P a collection of nonzero prime ideals of \mathcal{O}_K and Q the collection of prime ideals of \mathcal{O}_L above P . Then $H^1(\mathbb{I}_Q(L)) = 1$. If P does not contain the in L ramifying primes, then $H^0(\mathbb{I}_Q(L)) = \mathbb{I}_P(K)/N_K^L(\mathbb{I}_Q(L))$.

PROOF. Take $R = \mathcal{O}_P$ and $S = \mathcal{O}_Q$. \square

The cohomology groups of \mathcal{O}_E and \mathcal{O}_E^* (E a local field)

Let $E : F$ be a cyclic Galois extension of local fields, p the characteristic of the residue class fields, e the ramification index and f the residue class degree. Put $G = \text{Gal}(E : F) = \langle \sigma \rangle$. Then $\#(G) = n = ef$.

12.20 Proposition. $q(\mathcal{O}_E) = 1$.

PROOF. Choose a normal basis $(\beta, \sigma(\beta), \dots, \sigma^{n-1}(\beta))$ of $E : F$. We can assume that $\beta \in \mathcal{O}_E$. Put $\delta = \text{disc}(\beta, \sigma(\beta), \dots, \sigma^{n-1}(\beta))$. Then $\delta \in \mathcal{O}_F \setminus \{0\}$ and

$$T := \mathcal{O}_F\beta + \mathcal{O}_F\sigma(\beta) + \dots + \mathcal{O}_F\sigma^{n-1}(\beta) \subseteq \mathcal{O}_E \subseteq \frac{1}{\delta}T.$$

So $\delta\mathcal{O}_E \subseteq T \subseteq \mathcal{O}_E$. The ideal $\delta\mathcal{O}_E$ of the ring \mathcal{O}_E is of finite index: if $v_E(\delta) = m$, then $\mathcal{O}_E/\delta\mathcal{O}_E = \mathcal{O}_E/\mathfrak{p}_E^m$. By Corollary 12.14 $q(\mathcal{O}_E) = q(T)$ and by Proposition 12.15 $q(T) = 1$. \square

The exponential function defined in section 11.3 relates the multiplicative structure to the additive structure.

12.21 Proposition. $q(\mathcal{O}_E^*) = 1$.

PROOF. Put $t = \lfloor \frac{e}{p-1} \rfloor + 1$. By Theorem 11.21 we have an isomorphism

$$\exp: \mathfrak{p}_E^t \xrightarrow{\sim} 1 + \mathfrak{p}_E^t.$$

It is an isomorphism of G -modules:

$$\exp(\sigma(\alpha)) = \sum_{j=0}^{\infty} \frac{\sigma(\alpha)^j}{j!} = \sigma \left(\sum_{j=0}^{\infty} \frac{\alpha^j}{j!} \right) = \sigma(\exp \alpha).$$

Because $1 + \mathfrak{p}_E^t$ and \mathfrak{p}_E^t are of finite index in respectively \mathcal{O}_E^* and \mathcal{O}_E , we have

$$q(\mathcal{O}_E^*) = q(1 + \mathfrak{p}_E^t) = q(\mathfrak{p}_E^t) = q(\mathcal{O}_E) = 1. \quad \square$$

12.22 Theorem. $F^*/N_F^E(E^*)$ is of order $n = [E : F]$.

PROOF. Consider the following short exact sequence of G -modules

$$1 \longrightarrow \mathcal{O}_E^* \longrightarrow E^* \xrightarrow{v_E} \mathbb{Z} \longrightarrow 0,$$

where \mathbb{Z} has trivial G -action. Then $q(\mathbb{Z}) = \frac{1}{n}$ and

$$q(E^*) = q(\mathcal{O}_E^*)q(\mathbb{Z}) = \frac{1}{n}.$$

Since $H^1(E^*) = 1$ (Hilbert's Theorem 90), it follows that $\#(H^0(E^*)) = n$. \square

12.23 Theorem. $\#(H^0(\mathcal{O}_E^*)) = \#(H^1(\mathcal{O}_E^*)) = e$.

PROOF. By Proposition 12.21 $\#(H^0(\mathcal{O}_E^*)) = \#(H^1(\mathcal{O}_E^*))$, so it suffices to show that $\#(H^0(\mathcal{O}_E^*)) = e$. We have

$$\text{Ker}(\Delta_{\mathcal{O}_E^*}) = \mathcal{O}_F^* \quad \text{and} \quad \text{Im}(N_{\mathcal{O}_E^*}) = N_F^E(\mathcal{O}_E^*).$$

So $H^0(\mathcal{O}_E^*) = \mathcal{O}_F^*/N_F^E(\mathcal{O}_E^*)$. The norm map N_F^E induces the following commutative diagram with exact rows:

$$\begin{array}{ccccccc} 1 & \longrightarrow & \mathcal{O}_E^* & \longrightarrow & E^* & \xrightarrow{v_E} & \mathbb{Z} \longrightarrow 0 \\ & & \downarrow & & N_F^E \downarrow & & f \downarrow \\ 1 & \longrightarrow & \mathcal{O}_F^* & \longrightarrow & F^* & \xrightarrow{v_F} & \mathbb{Z} \longrightarrow 0 \end{array}$$

The cokernels of the vertical maps form a short exact sequence. From Theorem 12.22 it follows that the group $\mathcal{O}_F^*/N_F^E(\mathcal{O}_E^*)$ is of order e . \square

The Herbrand quotient of \mathcal{O}_L^*

Let $L : K$ be a cyclic Galois extension of number fields of degree n . Put $G = \text{Gal}(L : K) = \langle \sigma \rangle$. The group G acts on the infinite primes of L via $\tau \cdot \sigma_{\mathfrak{q}} = \sigma_{\mathfrak{q}}\tau^{-1}$, where $\tau \in G$ and $\sigma_{\mathfrak{q}}$ a real or complex embedding corresponding to \mathfrak{q} . The orbits of this action are the collections of primes above the same infinite prime of L . Let \mathfrak{p} be an infinite prime of K . If \mathfrak{p} does not ramify in L , then the orbit of primes of L above \mathfrak{p} has n elements, and if \mathfrak{p} does ramify it has $n/2$ elements. In the last case the decomposition group of \mathfrak{p} in L is of order 2 with $\sigma^{n/2}$ as its nontrivial element.

The structure of the group \mathcal{O}_L^* is given by the Dirichlet Unit Theorem. By Lemma 5.32 there is for each infinite prime \mathfrak{q} of L a unit $\varepsilon_{\mathfrak{q}} \in \mathcal{O}_L^*$ such that $\|\varepsilon_{\mathfrak{q}}\|_{\mathfrak{q}} > 1$ and $\|\varepsilon_{\mathfrak{q}}\|_{\mathfrak{q}'} < 1$ for all infinite primes $\mathfrak{q}' \neq \mathfrak{q}$ of L .

Now choose for each infinite prime \mathfrak{p} of K an infinite prime \mathfrak{q} of L above \mathfrak{p} and an $\varepsilon_{\mathfrak{q}}$ as above. In case \mathfrak{p} does not ramify, define for each $\tau(\mathfrak{q})$ in the same orbit a unit

$$\varepsilon_{\tau(\mathfrak{q})} = \tau(\varepsilon_{\mathfrak{q}}).$$

Then

$$\|\tau(\varepsilon_{\mathfrak{q}})\|_{\mathfrak{q}'} = |\sigma_{\mathfrak{q}'}\tau(\varepsilon_{\mathfrak{q}})| = |\sigma_{\tau^{-1}(\mathfrak{q}')}(\varepsilon_{\mathfrak{q}})| > 1 \text{ if } \mathfrak{q}' = \tau(\mathfrak{q}), \text{ and } < 1 \text{ otherwise.}$$

If \mathfrak{p} ramifies, replace $\varepsilon_{\mathfrak{q}}$ by $\varepsilon_{\mathfrak{q}}\sigma^{n/2}(\varepsilon_{\mathfrak{q}})$ and define $\varepsilon_{\tau(\mathfrak{q})}$ as in the nonramifying case. Thus we have a set of units $\varepsilon_{\mathfrak{q}}$, one for each of the $r + s$ infinite primes of L , which is invariant under the action of G and which by Proposition 5.34 is of rank $r + s - 1$. Let B be the subgroup of \mathcal{O}_L^* generated by the $r + s$ units $\varepsilon_{\mathfrak{q}}$ and let A be a free abelian group with $r + s$ basis elements $a_{\mathfrak{q}}$, one for each infinite prime \mathfrak{q} of L . Since A is free of rank $r + s$ and B is of rank $r + s - 1$, we thus have a short exact sequence of G -modules

$$0 \longrightarrow \mathbb{Z} \longrightarrow A \longrightarrow B \longrightarrow 1$$

with \mathbb{Z} a trivial G -module.

12.24 Theorem. $q(\mathcal{O}_L^*) = \frac{[L : K]}{2^t}$, where t is the number of infinite primes of K that ramify in L .

PROOF. Because \mathcal{O}_L^*/B is finitely generated and of rank 0, this group is finite. So $q(\mathcal{O}_L^*) = q(B)$. We compute $q(B)$. Let $A(\mathfrak{p})$ be the free abelian group on the $a_{\mathfrak{q}}$ with \mathfrak{q} above \mathfrak{p} . Then $A = \bigoplus_{\mathfrak{p}} A(\mathfrak{p})$, $q(A(\mathfrak{p})) = 1$ if \mathfrak{p} does not ramify and $q(A(\mathfrak{p})) = \frac{1}{2}$ if \mathfrak{p} does ramify. So $q(A) = \frac{1}{2^t}$ and since $q(\mathbb{Z}) = \frac{1}{[L : K]}$, we have

$$q(B) = \frac{q(A)}{q(\mathbb{Z})} = \frac{[L : K]}{2^t}. \quad \square$$

12.4 Galois modules and transfers

If the Galois group G of a Galois extension $L : K$ induces an action on an abelian group A associated to L , the G -module is often referred to as a *Galois module*. Such a Galois module often comes with extra structure. This situation is formalized in the Definitions 12.26 and 12.34.

12.25 Notation. Let $L : K$ be a Galois extension. The category of all intermediate fields of $L : K$ and their K -embeddings is denoted by $\mathcal{G}(L : K)$. (A K -embedding is an embedding which fixes the elements of K .) Special morphisms in this category are the elements of $\text{Gal}(L : K)$ and the inclusion maps $j_L^{K'} : K' \rightarrow L$, one for each intermediate field K' of $L : K$. Also the notation j^H will be used for $j_L^{L^H} : L^H \rightarrow L$.

12.26 Definition. Let $L : K$ be a Galois extension. A *Galois module* A associated to $L : K$ is a functor

$$A: \mathcal{G}(L : K) \rightarrow \mathcal{A}b.$$

Clearly we have:

12.27 Lemma. Let A be a Galois module associated to a Galois extension $L : K$ of degree n with Galois group G . Then $A(L)$ is a G -module under

$$\sigma \cdot x = A(\sigma)(x) \quad \text{for } \sigma \in G \text{ and } x \in A(L).$$

The map $A(j^G): A(K) \rightarrow A(L)$ is a G -homomorphism from the trivial G -module $A(K)$ to the G -module $A(L)$. \square

For H a subgroup of G , the extension $L : L^H$ is a Galois extension with Galois group H and the category $\mathcal{G}(L : L^H)$ is a subcategory of $\mathcal{G}(L : K)$. So restriction of a Galois module $A: \mathcal{G}(L : K) \rightarrow \mathcal{A}b$ gives a Galois module associated to $L : L^H$.

12.28 Definition. A Galois module A related to a Galois extension $L : K$ with Galois group G is called a *Galois module with descent* if for each subgroup H of G the map $A(j^H): A(L^H) \rightarrow A(L)$ induces an isomorphism $\overline{A(j^H)}: A(L^H) \xrightarrow{\sim} A(L)^H$.

12.29 Examples. Let $L : K$ be a Galois extension of degree n and $G = \text{Gal}(L : K)$. Examples of Galois modules A associated to $L : K$, given by $A(K')$ for intermediate fields K' of $L : K$, are:

$$\text{a) } A(K') = K', \quad \text{b) } A(K') = K'^* \quad \text{and} \quad \text{c) } A(K') = \mu(K').$$

By the Main Theorem of Galois Theory these examples are Galois modules with descent.

For number field extensions there are many interesting examples of Galois modules:

12.30 Examples. Let $L : K$ be a Galois extension of number fields with Galois group G . Examples of Galois modules A associated to $L : K$, given by $A(K')$ for intermediate fields K' of $L : K$ and $A(f)$ for K -embeddings being understood:

- a) $A(K') = \mathcal{O}_{K'}$, a Galois module with descent.
- b) $A(K') = \mathcal{O}_{K'}^*$, also with descent.
- c) $A(K') = \mathbb{I}(K')$. If a prime \mathfrak{p} ramifies in L , then $\prod_{\mathfrak{q}|\mathfrak{p}\mathcal{O}_L} \mathfrak{q} \in \mathbb{I}(L)^G$, but is not in the image of $\mathbb{I}(K) \rightarrow \mathbb{I}(L)^H$. Only if the extension $L : K$ is unramified, this Galois module is a Galois module with descent.

- d) $A(K') = \mathcal{C}(K')$. We have seen that $\mathcal{C}(K) \rightarrow \mathcal{C}(L)$ is not injective in general, so in these cases there is no descent.

12.31 Example. Let $L : K$ be a Galois extension with $G = \text{Gal}(L : K) \cong C_2 \times C_2$, say $G = \langle \sigma, \tau \rangle$, σ and τ being two automorphisms of order 2. In $\mathbb{Z}[G]$ we have

$$N_\sigma + N_\tau + N_{\sigma\tau} = 3 + \sigma + \tau + \sigma\tau = 2 + N_G.$$

So for a G -module A this means that $2x \in A^\sigma + A^\tau + A^{\sigma\tau}$ for all $x \in A$. For a Galois module $A: \mathcal{G}(L : K) \rightarrow \mathcal{A}b$ it implies that for each $x \in A(L)$ we have that $2x$ is in the subgroup generated by the images of $A(L^\sigma)$, $A(L^\tau)$ and $A(L^{\sigma\tau})$ in $A(L)$. If in particular $L : K$ is a number field extension, this applies to the Galois modules of Examples 12.30:

- For each $\alpha \in \mathcal{O}_L$ the integer 2α is in the subgroup $\mathcal{O}_{L^\sigma} + \mathcal{O}_{L^\tau} + \mathcal{O}_{L^{\sigma\tau}}$. This has been used in exercise 9 of chapter 1 for the computation of an integral basis for a biquadratic number field.
- For each $\nu \in \mathcal{O}_L^*$ the unit ν^2 is in the subgroup $\mathcal{O}_{L^\sigma}^* \cdot \mathcal{O}_{L^\tau}^* \cdot \mathcal{O}_{L^{\sigma\tau}}^*$. This has been used for the computation of the unit groups of the biquadratic fields $\mathbb{Q}(\sqrt{-2}, \sqrt{3})$ and $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ (Examples 5.37 and 5.38).
- For each $x \in \mathcal{C}(L)$ the ideal class x^2 is in the subgroup generated by the images of $\mathcal{C}(L^\sigma)$, $\mathcal{C}(L^\tau)$ and $\mathcal{C}(L^{\sigma\tau})$.

12.32 Example. Let $L : K$ be a Galois extension with $G = \text{Gal}(L : K) \cong S_3$, say $G = \langle \sigma, \tau \rangle$, σ an automorphism of order 3 and τ an automorphism of order 2. Then $\tau\sigma\tau = \sigma^{-1}$ and in $\mathbb{Z}[G]$ we have

$$N_\sigma + N_\tau + N_{\sigma\tau} + N_{\sigma^2\tau} = 3 + N_G.$$

For a G -module A this implies that $3x \in A^\sigma + A^\tau + A^{\sigma\tau} + A^{\sigma^2\tau}$ for all $x \in A$. For a Galois module $A: \mathcal{G}(L : K) \rightarrow \mathcal{A}b$ it follows that for each $x \in A(L)$, the element $3x$ is in the subgroup generated by the images of $A(L^\sigma)$, $A(L^\tau)$, $A(L^{\sigma\tau})$ and $A(L^{\sigma^2\tau})$. So, in particular, if $L : K$ is a number field extension:

- For each $\alpha \in \mathcal{O}_L$ the integer 3α is in the subgroup $\mathcal{O}_{L^\sigma} + \mathcal{O}_{L^\tau} + \mathcal{O}_{L^{\sigma\tau}} + \mathcal{O}_{L^{\sigma^2\tau}}$. This has been used for the computation of an integral basis of the field $\mathbb{Q}(\sqrt[3]{\alpha}, \zeta_3)$ in Example 7.17.
- For each $\nu \in \mathcal{O}_L^*$ the unit ν^3 is in the subgroup $\mathcal{O}_{L^\sigma}^* \cdot \mathcal{O}_{L^\tau}^* \cdot \mathcal{O}_{L^{\sigma\tau}}^* \cdot \mathcal{O}_{L^{\sigma^2\tau}}^*$. This also has been used in Example 7.17.
- For each $x \in \mathcal{C}(L)$ the ideal class x^3 is in the subgroup generated by the images of $\mathcal{C}(L^\sigma)$, $\mathcal{C}(L^\tau)$, $\mathcal{C}(L^{\sigma\tau})$ and $\mathcal{C}(L^{\sigma^2\tau})$.

12.33 Example. The ideal class groups of the proper subfields of $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ are trivial. Since $\mathcal{C}: \mathcal{G}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3) : \mathbb{Q}) \rightarrow \mathcal{A}b$ is a Galois module, the group $\mathcal{C}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3))$ is a 3-elementary abelian group. In fact, the group is trivial, see again Example 7.17.

Transfers

In many interesting cases a Galois module is not a Galois module with descent. However, there is a useful weaker notion.

12.34 Definition. Let A be a Galois module associated to a Galois extension $L : K$ with Galois group G and let H be a subgroup of G . A *transfer* tr^H of A is an H -homomorphism

$$\text{tr}^H : A(L) \rightarrow A(L^H)$$

such that the following diagram commutes

$$\begin{array}{ccc}
 A(L) & \xrightarrow{N_H} & A(L) \\
 \text{tr}^H \downarrow & \nearrow A(j^H) & \downarrow \text{tr}^H \\
 A(L^H) & \xrightarrow{m} & A(L^H)
 \end{array}$$

where m and N_H stand for multiplication by $m = \#(H)$ and N_H in $A(L^H)$ and the $\mathbb{Z}[G]$ -module $A(L)$ respectively. A Galois module A with transfers is a Galois module A together with transfers of A for each subgroup H of G .

Note that the square in the above diagram commutes because tr^H is an L^H -homomorphism. By the map $A(j^H)$ the square is subdivided into two commutative triangles.

12.35 Examples.

- a) The examples given in Examples 12.29 are Galois modules with transfers. The transfers are $\text{Tr}_{L^H}^L$, $N_{L^H}^L$ and $N_{L^H}^L$ respectively. In the last two cases the transfer is the norm map restricted to L^* and $\mu(L)$ respectively.
- b) The examples a) and b) given in Examples 12.30 are Galois modules with transfers. The transfers are given by $\text{Tr}_{L^H}^L$ and $N_{L^H}^L$.
- c) Example c) given in Examples 12.30 is a Galois module with transfers. Transfers are the norm maps $N_{L^H}^L$ described in Notations 7.71, see also Definition 7.65 and Proposition 7.69.
- d) Example d) given in Examples 12.30 is a Galois module with transfers. The transfers are described in Notations 7.71 and for their properties see Proposition 7.69 and Corollary 7.70.

12.36 Proposition. *Galois modules with descent are Galois modules with transfers.*

PROOF. If the Galois module has transfers then the diagram in Definition 12.34 induces a commutative diagram

$$\begin{array}{ccc}
 A(L)_H & \xrightarrow{\overline{N}_H} & A(L)^H \\
 \downarrow \text{tr}^H & \nearrow \overline{A(j^H)} & \downarrow \text{tr}^H \\
 A(L^H) & \xrightarrow{m} & A(L^H)
 \end{array}$$

So if the map $\overline{A(j^H)}$ is an isomorphism, then tr^H has to be the composition

$$A(L) \longrightarrow A(L)_H \xrightarrow{\overline{N}_H} A(L)^H \xrightarrow{\overline{A(j^H)}^{-1}} A(L^H).$$

Let this be the definition of the transfer. Then the top triangle in the diagram of Definition 12.34 commutes. The composition of the first two maps is just $N_H: A(L) \rightarrow A(L)^H$. For the commutativity of the bottom triangle we have to show that the composition $\text{tr}^H \overline{A(j^H)}$ is multiplication by m . The image of $\overline{A(j^H)}$ is contained in $A(L)^H$, so this composition is the composition of $\overline{A(j^H)}$ and the restriction of tr^H to $A(L)^H$. So we get

$$A(L^H) \xrightarrow{\overline{A(j^H)}} A(L)^H \xrightarrow[\text{tr}^H]{N_H} A(L)^H \xrightarrow{\overline{A(j^H)}^{-1}} A(L^H)$$

and this is multiplication by m . □

12.37 Definition. Let A be a Galois module associated to a Galois extension $L : K$ of degree n and Galois group G . Then A is called *acyclic* if multiplication by n is an automorphism of $A(L)^H$ for each subgroup H of G . Equivalently, A takes values in the category of $\mathbb{Z}[\frac{1}{n}]$ -modules.

A partial converse of Proposition 12.36:

12.38 Proposition. *Let A be an acyclic Galois module with transfers associated to a Galois extension $L : K$ with Galois group G of order n . Then A is a Galois module with descent. Moreover, for each subgroup H of G the subgroup $A(L)^H$ of $A(L)$ is a direct summand.*

PROOF. The horizontal maps in the diagram in the proof of Proposition 12.36 are isomorphisms and as a consequence all the maps in the diagram are isomorphisms. So, in particular, A is a Galois module with descent. The subgroups $A(L)^H$ of $A(L)$ are direct summands: a left inverse of the inclusion is given by multiplication by $\frac{1}{m}N_H$. □

Of course, from a Galois module A an acyclic one can be obtained by tensoring with $\mathbb{Z}[\frac{1}{n}]$, where n is the order of the Galois group: A is then replaced by the Galois module $\mathbb{Z}[\frac{1}{n}] \otimes A(-)$. More generally, $R \otimes A(-)$ is acyclic if n is invertible in the ring R . Example 12.31 was about Galois modules associated to a Galois extension with Galois group of type $C_2 \times C_2$. The Galois modules have transfers. The Galois module given by $K' \mapsto \mathbb{Z}[\frac{1}{2}] \otimes \mathcal{C}(K')$, that is $K' \mapsto$ odd part of $\mathcal{C}(K')$ is acyclic. It is not hard to show that the structure of the odd part of $\mathcal{C}(L)$ is completely determined by the odd parts of the ideal class groups of the proper intermediate fields. This will be done in detail more generally for the group $C_p \times C_p$ with p a prime in section 12.5.

The group S_3 , considered in Example 12.32, is an example of a metacyclic group. In section 12.6 group modules are studied in detail for a class of metacyclic groups.

12.5 $C_p \times C_p$ -Modules

Let p be a prime number and G the elementary abelian p -group of rank 2: $G = C_p \times C_p$. This group has $p + 1$ subgroups of order p . Let Υ denote this collection of subgroups. For the norm elements of the subgroups of G we have the relation

$$\sum_{H \in \Upsilon} N_H = p + N_G.$$

In $\mathbb{Z}[\frac{1}{p}][G]$ this can be written as

$$\frac{1}{p^2} N_G + \sum_{H \in \Upsilon(G)} \left(\frac{1}{p} N_H - \frac{1}{p^2} N_G \right) = 1. \tag{12.1}$$

Using Lemma 12.4 the following is easily verified:

12.39 Proposition. *The elements $\varepsilon_H = \frac{1}{p} N_H - \frac{1}{p^2} N_G$, one for each subgroup H of order p , form together with $\varepsilon_G = \frac{1}{p^2} N_G$ an orthogonal system of idempotents of $\mathbb{Z}[\frac{1}{p}][G]$. \square*

As a result any $\mathbb{Z}[\frac{1}{p}][G]$ -module A splits as a direct sum

$$A = \varepsilon_G A \oplus \bigoplus_{H \in \Upsilon} \varepsilon_H A.$$

For each H of order p we have $\frac{1}{p} N_H = \varepsilon_H + \varepsilon_G$ and so

$$A^H = N_H A = \varepsilon_H A \oplus \varepsilon_G A = \varepsilon_H A \oplus A^G.$$

Thus we have:

12.40 Proposition. *Let A be a $\mathbb{Z}[\frac{1}{p}][G]$ -module. Then*

$$A^G \oplus \bigoplus_{H \in \Upsilon} A^H/A^G \xrightarrow{\sim} A. \quad \square$$

Combining this result with Theorem 12.38 yields:

12.41 Theorem. *Let p be a prime number, $L : K$ a Galois extension with $\text{Gal}(L : K) \cong C_p \times C_p$ and A an acyclic Galois module with transfers associated to $L : K$. Then*

$$A(L)/A(K) \cong \bigoplus_{H \in \Upsilon} A(L^H)/A(K) \quad \square$$

The Galois group of a biquadratic number field over \mathbb{Q} is isomorphic to $C_2 \times C_2$. So for a biquadratic number field K the odd part of the ideal class group is determined by the ideal class groups of its three quadratic subfields. The class number formulas for biquadratic number fields in 9.57 and 9.58 reduce the computation of the order of the 2-primary part of the abelian group $\mathcal{C}(K)$ to the computation of the full unit group of \mathcal{O}_K .

12.42 Example. Let's again have a look at $K = \mathbb{Q}(\sqrt{-2}, \sqrt{3})$. The odd parts of the ideal class groups form an acyclic Galois module associated to $K : \mathbb{Q}$. The ideal class groups of $\mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(\sqrt{3})$ are trivial and the ideal class group of $\mathbb{Q}(\sqrt{6})$ is of order 2. So the odd part of $\mathcal{C}(K)$ is trivial. This also follows from the computation in Example 9.57, which tells even more: $h(K) = Q(K)$. Since $Q(K) = 2$ (Example 5.49), it follows that $\mathcal{C}(K)$ is of order 2. The group $\mathcal{C}(K)$ has also been computed using the Minkowski bound in Example 5.23: $\mathcal{C}(K)$ is of order 2 and is generated by a prime ideal above 2.

A less trivial case of a biquadratic number field:

12.43 Example. Let $K = \mathbb{Q}(\sqrt{79}, \sqrt{-3})$. Put $K_1 = \mathbb{Q}(\sqrt{79})$, $K_2 = \mathbb{Q}(\sqrt{-3})$ and $K_3 = \mathbb{Q}(\sqrt{-237})$. The class number of K_2 equals 1. The algorithms given in chapter 4 for quadratic number fields can be used for the computation of the ideal class groups of K_1 and K_3 . The group $\mathcal{C}(K_1)$ is of order 3 and is generated by the class of a prime ideal above 3. The structure of $\mathcal{C}(K_3)$ is $C_6 \times C_2$. So by Theorem 12.41 the structure of the odd part of $\mathcal{C}(K)$ is $C_3 \times C_3$. The problem is to compute the 2-primary part. The formula

$$h(K) = \frac{Q(K)}{2} h(K_1) h(K_2) h(K_3)$$

in 9.57 yields $h(K) = 18 \cdot Q(K)$. We show by contradiction that $Q(K) = 2$. Suppose that $Q(K) = 1$. Then there is a $\nu \in \mathcal{O}_K^*$ such that $\nu^2 = -\varepsilon$, where ε is the fundamental unit of K_1 . Then $K = K_1(\nu)$. The discriminant of $(1, \nu)$ over K_1 is -4ε . So $\mathfrak{d}_{K_1}(K) \mid 4\mathcal{O}_{K_1}$. The prime ideals of \mathcal{O}_{K_1} above 3 ramify in K and are,

therefore, divisors of $\mathfrak{d}_{K_1}(K)$. Contradiction. Hence $h(K) = 36$ and therefore, the 2-primary part of $\mathcal{C}(K)$ is of order 4. The prime 3 splits completely in K_1 and ramifies in K_2 and K_3 . The prime 79 splits completely in K_2 and ramifies in K_1 and K_3 . Let \mathfrak{p} be a prime ideal of \mathcal{O}_K above 3 and \mathfrak{q} a prime ideal of \mathcal{O}_K above 79. The ideals $N_{K_3}^K(\mathfrak{p})$ and $N_{K_3}^K(\mathfrak{q})$ represent ideal classes which generate the 2-primary part of $\mathcal{C}(K_3)$. So the map $\text{tr}_{K_3}^K: \mathcal{C}(K) \rightarrow \mathcal{C}(K_3)$ is surjective. It follows that $\mathcal{C}(K) \cong C_6 \times C_6$.

By relation (12.1) the element $1 \in \mathbb{Z}[\frac{1}{p}][G]$ can be written as a combination of N_G and the N_H for $H \in \Upsilon$:

$$1 = -\frac{1}{p}N_G + \frac{1}{p} \sum_{H \in \Upsilon} N_H.$$

In section 18.2 this will be generalized to arbitrary abelian groups G and it will lead to a generalization of Proposition 12.40, see Corollary 18.32.

12.6 $C_p \rtimes C_q$ -Modules

Let p be a prime number and W_p the group generated by an element σ of order p and an element ρ of order $p - 1$ satisfying $\rho\sigma\rho^{-1} = \sigma^g$, where g is a primitive root modulo p . In this section we consider subgroups G of W_p generated by σ and $\tau = \rho^s$, where s is a divisor of $p - 1$ different from $p - 1$. Then G is a metacyclic group $C_p \rtimes C_q$, where $q = \frac{p-1}{s}$. For q prime this is the unique nonabelian group of order pq . In this section q is not necessarily prime.

The group G has exactly p cyclic subgroups of order q : the groups $\langle \sigma^i \tau \rangle$ for $i = 0, \dots, p - 1$. As is easily seen, G is the disjoint union of $\langle \sigma \rangle$ and these subgroups minus their unity element, hence

$$N_G = -p + N_\sigma + \sum_{i=0}^{p-1} N_{\sigma^i \tau}. \tag{12.2}$$

For G -modules A it follows that A modulo the subgroup generated by the A^H for nontrivial $H < G$ has exponent p . In the remaining part of this section we will study the way A is composed of these subgroups A^H when multiplication by p is invertible. The element $\frac{1}{p}N_\sigma$ is a central idempotent of the ring $\mathbb{Z}[\frac{1}{p}][G]$. Hence, a $\mathbb{Z}[\frac{1}{p}][G]$ -module A splits as the direct sum of $N_\sigma A (= A^\sigma)$ and A/A^σ , which is a $\mathbb{Z}[\frac{1}{p}][G]/\mathfrak{a}$ -module, where \mathfrak{a} is the (two-sided) ideal generated by N_σ .

The case $G = W_p$ will be considered first. Let B be a $\mathbb{Z}[\frac{1}{p}][W_p]$ -module satisfying $N_\sigma B = B^\sigma = 0$. Let \mathfrak{b} be the ideal of $\mathbb{Z}[\frac{1}{p}][W_p]$ generated by N_σ . Then B is an

$R := \mathbb{Z}[\frac{1}{p}][W_p]/\mathfrak{b}$ -module. We will construct an orthogonal system consisting of $p-1$ idempotents of R . Since $N_{W_p} = N_\rho N_\sigma$, equation (12.2) for $G = W_p$ gives

$$\sum_{i=0}^{p-1} \frac{1}{p} N_{\sigma^i \rho} \equiv 1 \pmod{\mathfrak{b}}. \quad (12.3)$$

Put $\vartheta = \sigma^{1-g}$. Then for all $j \in \mathbb{Z}$ we have $\sigma^j \rho \sigma^{-j} = \sigma^j \sigma^{-jg} \rho = \vartheta^j \rho$, and so $\sigma^j N_\rho \sigma^{-j} = N_{\vartheta^j \rho}$. For $j = 1, \dots, p-1$ we define

$$\varepsilon_j = \frac{1}{p} N_{\vartheta^j \rho} (1 - \sigma^j) \in \mathbb{Z}[\frac{1}{p}][W_p].$$

We will show that the ε_j modulo \mathfrak{b} form an orthogonal system of idempotents of R . Note that these elements are not central:

$$\rho(\vartheta^j \rho) \rho^{-1} = \vartheta^{jg} \rho$$

and so

$$\rho \varepsilon_j \rho^{-1} = \frac{1}{p} N_{\vartheta^{jg} \rho} (1 - \sigma^{jg}) = \varepsilon_{jg}.$$

Since g is a primitive root modulo p , conjugation by ρ induces a $p-1$ -cycle of the set $\{\varepsilon_1, \dots, \varepsilon_{p-1}\}$. First a lemma.

12.44 Lemma. *For all $i = 1, \dots, p-1$ and all $j = 0, \dots, p-1$ we have $N_{\vartheta^j \rho} \sigma^i N_{\vartheta^j \rho} \equiv -N_{\vartheta^j \rho} \pmod{\mathfrak{b}}$.*

PROOF. Conjugation by a power of σ shows that we can assume that $j = 0$ and subsequent conjugation by ρ shows that we can assume that $i = 1$. We have

$$\begin{aligned} N_\rho \sigma N_\rho &= \sum_{j=0}^{p-1} \sum_{k=0}^{p-1} \rho^j \sigma \rho^k = \sum_{j=0}^{p-1} \sum_{k=0}^{p-1} \sigma^{g^j} \rho^{j+k} = \sum_{j=0}^{p-1} \sum_{l=0}^{p-1} \sigma^{g^j} \rho^l \\ &= \sum_{j=0}^{p-1} \sigma^{g^j} \sum_{l=0}^{p-1} \rho^l = (N_\sigma - 1) N_\rho \equiv -N_\rho \pmod{\mathfrak{b}}. \quad \square \end{aligned}$$

12.45 Proposition. *The elements $\bar{\varepsilon}_j$ for $j = 1, \dots, p-1$ form an orthogonal system of idempotents of the ring R .*

PROOF. For proving that the $\bar{\varepsilon}_j$ are idempotents conjugation by ρ shows that we can assume that $j = 1$. By Lemma 12.4 and Lemma 12.44 we have

$$\begin{aligned} (N_{\vartheta \rho} (1 - \sigma))^2 &= (N_{\vartheta \rho} - N_{\vartheta \rho} \sigma)^2 = N_{\vartheta \rho}^2 - N_{\vartheta \rho} \sigma N_{\vartheta \rho} - N_{\vartheta \rho}^2 \sigma + N_{\vartheta \rho} \sigma N_{\vartheta \rho} \sigma \\ &\equiv (p-1) N_{\vartheta \rho} + N_{\vartheta \rho} - (p-1) N_{\vartheta \rho} \sigma - N_{\vartheta \rho} \sigma \equiv p N_{\vartheta \rho} (1 - \sigma) \pmod{\mathfrak{b}}. \end{aligned}$$

Hence $\varepsilon_1^2 \equiv \varepsilon_1 \pmod{\mathfrak{b}}$. For $i, j \in \{1, \dots, p-1\}$ with $i \neq j$ we have also by Lemma 12.44

$$\begin{aligned} N_{\vartheta^i \rho}(1 - \sigma^i)N_{\vartheta^j \rho} &= N_{\vartheta^i \rho}N_{\vartheta^j \rho} - N_{\vartheta^i \rho}\sigma^i N_{\vartheta^j \rho} = \sigma^i N_{\rho}\sigma^{j-i}N_{\rho}\sigma^{-j} - \sigma^i N_{\rho}\sigma^j N_{\rho}\sigma^{-j} \\ &\equiv -\sigma^i N_{\rho}\sigma^{-j} + \sigma^i N_{\rho}\sigma^j \equiv 0 \pmod{\mathfrak{b}}. \end{aligned}$$

It follows that $\varepsilon_i \varepsilon_j = \frac{1}{p^2} N_{\vartheta^i \rho}(1 - \sigma^i)N_{\vartheta^j \rho}(1 - \sigma^j) \equiv 0 \pmod{\mathfrak{b}}$. Finally, equation (12.2) for $G = W_p$ implies

$$\sum_{i=0}^{p-1} N_{\vartheta^i \rho} = \sum_{i=0}^{p-1} N_{\sigma^i \rho} \equiv p \pmod{\mathfrak{b}}.$$

Since

$$0 \equiv N_{\sigma} N_{\rho} \equiv \sum_{i=0}^{p-1} \sigma^i N_{\rho} \equiv \sum_{i=0}^{p-1} N_{\vartheta^i \rho} \sigma^i \pmod{\mathfrak{b}},$$

it follows that

$$\sum_{i=1}^{p-1} \varepsilon_i = \sum_{i=1}^{p-1} \frac{1}{p} N_{\vartheta^i \rho}(1 - \sigma^i) = \sum_{i=1}^{p-1} \frac{1}{p} N_{\vartheta^i \rho} - \sum_{i=1}^{p-1} \frac{1}{p} N_{\vartheta^i \rho} \sigma^i \equiv 1 \pmod{\mathfrak{b}}. \quad \square$$

Since the element ε is a central idempotent of $\mathbb{Z}[\frac{1}{p}][W_p]$ we have

12.46 Corollary. *Let $\varepsilon = \frac{1}{p} N_{\sigma} \in \mathbb{Z}[\frac{1}{p}][W_p]$. Then the elements*

$$\varepsilon, (1 - \varepsilon)\varepsilon_1, \dots, (1 - \varepsilon)\varepsilon_{p-1}$$

form a system of orthogonal idempotents of the ring $\mathbb{Z}[\frac{1}{p}][W_p]$. \square

The system of orthogonal idempotents gives a direct sum decomposition of $\mathbb{Z}[\frac{1}{p}][W_p]$ -modules and the submodules corresponding to the last $p-1$ idempotents in the system are isomorphic since these idempotents are conjugate. A further simplification of the direct sum decomposition will be obtained using the following well-known lemma for which we give here a direct proof.

12.47 Lemma. *Let C be a cyclic group of order n generated by σ and let A be a $\mathbb{Z}[\frac{1}{n}][C]$ -module satisfying $N_C A = 0$. Then $(1 - \sigma)A = A$.*

PROOF. Clearly, $(1 - \sigma)A \subseteq A$. Let $a \in A$. The element $b = \sum_{i=1}^{n-1} \left(1 - \frac{i}{n}\right) \sigma^{i-1} a$ satisfies $(1 - \sigma)b = a$. \square

12.48 Proposition. *Let B be a $\mathbb{Z}[\frac{1}{p}][W_p]$ -module. Then we have an isomorphism of abelian groups*

$$B/B^{\sigma} \xrightarrow{\sim} (N_{\rho} B / N_{W_p} B)^{p-1}.$$

PROOF. By Corollary 12.46 we have a direct sum decomposition of the abelian group B :

$$B = \varepsilon B \oplus (1 - \varepsilon)\varepsilon_1 B \oplus \cdots \oplus (1 - \varepsilon)\varepsilon_{p-1} B.$$

The subgroup $\langle \rho \rangle$ of W_p acts on $\{(1 - \varepsilon)\varepsilon_j \mid j = 1, \dots, p - 1\}$ by conjugation. Therefore, we have

$$B \xrightarrow{\sim} B^\sigma \oplus ((1 - \varepsilon)\varepsilon_1 B)^{p-1}.$$

It remains to show that $\varepsilon_1(1 - \varepsilon)B \xrightarrow{\sim} N_\rho B / N_{W_p} B$. The inclusion of $(1 - \varepsilon)B$ in B induces an isomorphism of $\mathbb{Z}[\frac{1}{p}][W_p]$ -modules $(1 - \varepsilon)B \xrightarrow{\sim} B/\varepsilon B = B/B^\sigma$. Because $N_\sigma(B/B^\sigma) = 0$, we have by Lemma 12.47 $(1 - \sigma)(B/B^\sigma) = B/B^\sigma$. Hence,

$$\begin{aligned} \varepsilon_1(1 - \varepsilon)B &\xrightarrow{\sim} \varepsilon_1(B/B^\sigma) = N_{\vartheta\rho}(1 - \sigma)(B/B^\sigma) = N_{\vartheta\rho}(B/B^\sigma) \\ &\xrightarrow{\sim} N_{\vartheta\rho}B / N_{\vartheta\rho}N_\sigma B = N_{\vartheta\rho}B / N_{W_p} B \xrightarrow{\sim} N_\rho B / N_{W_p} B, \end{aligned}$$

where the last isomorphism is induced by multiplication with σ^{-1} . \square

Next we consider the general case.

12.49 Proposition. *Let G be the subgroup of W_p is generated by σ and an element of order $q \mid p - 1$ with $q \neq 1$, say the element $\tau = \rho^s$, where $s = \frac{p-1}{q}$. Let A be a $\mathbb{Z}[\frac{1}{pq}][G]$ -module. Then we have isomorphisms of abelian groups*

$$A^s \xrightarrow{\sim} (A^\sigma)^s \oplus (A^\tau / A^G)^{p-1}.$$

and

$$(A/A^G)^s \xrightarrow{\sim} (A^\sigma / A^G)^s \oplus (A^\tau / A^G)^{p-1}.$$

PROOF. Let B be the W_p -module induced by the G -module A , that is

$$B = \mathbb{Z}[W_p] \otimes_{\mathbb{Z}[G]} A = \bigoplus_{i=0}^{s-1} \rho^i \otimes A.$$

It is in fact a $\mathbb{Z}[\frac{1}{pq}][W_p]$ -module and so are $\varepsilon B (= B^\sigma)$ and $(1 - \varepsilon)B (\xrightarrow{\sim} B/B^\sigma)$. By Proposition 12.48 we have

$$B \xrightarrow{\sim} B^\sigma \oplus B/B^\sigma \xrightarrow{\sim} B^\sigma \oplus (N_\rho B / N_{W_p} B)^{p-1}.$$

Since $B \cong A^s$ and $B^\sigma \cong (A^\sigma)^s$ as abelian groups, it remains to prove that $N_\tau A / N_G A \xrightarrow{\sim} N_\rho B / N_{W_p} B$. Consider the injective group homomorphism

$$f: A \rightarrow B, a \mapsto \sum_{j=0}^{s-1} \rho^j \otimes a.$$

For any $a \in A$ the element $N_\tau a$ maps under f to $\sum_{j=0}^{s-1} \rho^j \otimes N_\tau a = \sum_{j=0}^{s-1} \rho^j N_\tau \otimes a = N_\rho \otimes a$. So f restricts to an injective homomorphism

$$f: N_\tau A \rightarrow N_\rho B, N_\tau a \mapsto N_\rho \otimes a.$$

This map is also surjective: $N_\rho(\rho^i \otimes a) = N_\rho \rho^i \otimes a = N_\rho \otimes a = f(N_\tau a)$. Furthermore, $f(N_G A) = N_{W_p} B$: for any $a \in A$ we have $f(N_G a) = f(N_\tau N_\sigma a) = N_\rho \otimes N_\sigma a = N_\rho N_\sigma \otimes a = N_{W_p} \otimes a = N_{W_p}(1 \otimes a)$ and $N_{W_p}(\rho^i \otimes a) = N_{W_p} \rho^i \otimes a = N_{W_p} \otimes a = f(N_G a)$. \square

Since the ideal class groups of fields in a Galois extension of number fields form a Galois module with transfers, we now have for the ideal class group of a Galois extension with Galois group the metacyclic group G the following.

12.50 Theorem. *Let $L : K$ be a Galois extension of number fields with Galois group $G \cong C_p \rtimes C_q$. Then for each prime $l \nmid pq$*

$$\mathcal{C}(L)_l / \mathcal{C}(K)_l \cong \mathcal{C}(L^\sigma)_l / \mathcal{C}(K)_l \times (\mathcal{C}(L^\tau)_l / \mathcal{C}(K)_l)^q. \quad \square$$

12.51 Example. Let $f \in \mathbb{Z}[X]$ be a monic irreducible polynomial of degree 3 and $\alpha \in \mathbb{R}$ a zero of f . Put $K = \mathbb{Q}(\alpha)$. Assume that $d = \text{disc}(f)$ is not a square. Then $K : \mathbb{Q}$ is not a Galois extension. Its normal closure is the splitting field of f . Let L be this splitting field. Then $\text{Gal}(L : \mathbb{Q}) \cong S_3$. For primes $p \neq 2, 3$ the p -components of the ideal class groups form an acyclic Galois module with transfers associated to $L : \mathbb{Q}$. By Theorem 12.50 we have

$$\mathcal{C}(L)_p \cong \mathcal{C}(\mathbb{Q}(\sqrt{d}))_p \times \mathcal{C}(K)_p^2.$$

So the structure of the group $\mathcal{C}(L)$ is up to 2- and 3-torsion determined by the the ideal class groups of K and $\mathbb{Q}(\sqrt{d})$. Furthermore, since $[L : \mathbb{Q}(\sqrt{d})] = 3$, the 2-component of $\mathcal{C}(\mathbb{Q}(\sqrt{d}))$ maps injectively into $\mathcal{C}(L)$. Similarly, the 3-component of $\mathcal{C}(K)$ maps injectively into $\mathcal{C}(L)$.

EXERCISES

1. (i) Let $L : K$ be a quadratic Galois extension and $\alpha \in L$ with $\alpha \neq -1$ and $N_K^L(\alpha) = 1$. Let $\sigma \in \text{Gal}(L : K)$ be of order 2. Show that $\beta = \alpha + 1$ satisfies $\alpha = \frac{\beta}{\sigma(\beta)}$.
- (ii) Let $(x, y, z) \in \mathbb{N}^{*3}$ be a Pythagorean triple. Use (i) applied to $\mathbb{Q}(i) : \mathbb{Q}$ to show that there are $u, v \in \mathbb{N}^*$ such that $(x : y : z) = (u^2 - v^2 : 2uv : u^2 + v^2)$.
2. Let G be a cyclic group of order n and A a G -module. Prove that the groups $H^0(A)$ and $H^1(A)$ are killed by n .

3. Let G be a cyclic group and A a finite G -module such that $\gcd(\#(G), \#(A)) = 1$. Show that $H^0(A) = H^1(A) = 0$.
4. Let A and B be as in Proposition 12.15, but without the condition of B being torsion free. Show² that $H^1(A) \cong_m B$ and $H^0(A) \cong B/mB$.
5. Let $E : F$ be an unramified extension of local fields. Show that the map $N_F^E : E \rightarrow F$ induces a surjective homomorphism $\mathcal{O}_E^* \rightarrow \mathcal{O}_F^*$.
6. Let $L = \mathbb{Q}(\alpha, \zeta_3)$, where $\alpha = \sqrt[3]{7} \in \mathbb{R}$. Put $K = \mathbb{Q}(\alpha)$.
 - (i) Show that the prime number 3 totally ramifies in L .
 - (ii) Show that $\delta := \frac{2(1+2\zeta_3)}{\alpha-1} \in \mathcal{O}_L$, $L = \mathbb{Q}(\delta)$ and $\delta^2 \in \mathbb{Z}[\alpha]$.
 - (iii) Show that $\text{disc}(L) = -3^k 7^4$ for some $k \in \mathbb{N}^*$.
 - (iv) Compute the minimal polynomial f of δ over \mathbb{Q} .
 - (v) Prove that $k = 7$.
 - (vi) Show that $\mathcal{C}(L)$ is an elementary abelian 3-group of 3-rank ≥ 1 .
7. Let p be an odd prime number, $K = \mathbb{Q}(\zeta_p)$, $G = \text{Gal}(K : \mathbb{Q})$ and \mathfrak{p} the unique prime of L above p .
 - (i) Which of the cohomology groups of the following G -modules are finite?

$$K, \quad K^*, \quad \mathcal{O}_K, \quad \mathcal{O}_K^*, \quad \mathbb{I}(K), \quad K_{\mathfrak{p}}, \quad K_{\mathfrak{p}}^*, \quad \mathcal{O}_{\mathfrak{p}}^*$$
 - (ii) Determine the order of each of the finite cohomology groups.
 - (iii) Show that each of the finite cohomology groups is cyclic.

8. Let K be a quadratic number field of discriminant D . Let r be the number of finite primes which ramify in K . So r equals the number of prime divisors of D . In this exercise we show that the 2-rank of the narrow ideal class group $\mathcal{C}^+(K)$ is equal to $r - 1$. See exercise 9 of chapter 6 for the definition of the narrow ideal class group. Or, specifically for quadratic number fields, see exercise 17 of chapter 4. We will use the following notations:

$$\begin{aligned}
 K^+ &= \{ \alpha \in K^* \mid N_{\mathbb{Q}}^K(\alpha) > 0 \}, \\
 \mathcal{O}_K^+ &= \{ \nu \in \mathcal{O}_K^* \mid N_{\mathbb{Q}}^K(\alpha) > 0 \} = \mathcal{O}_K^* \cap K^+, \\
 \Delta(K) &= \{ \alpha \in K^+ \mid \alpha \mathcal{O}_K \in \mathbb{I}(K)^2 \}.
 \end{aligned}$$

Furthermore, a group homomorphism $\varphi : \Delta(K) \rightarrow \mathcal{C}^+(K)$ is defined by $\varphi(\alpha) = [\mathfrak{a}]^+$, where $\alpha \mathcal{O}_K = \mathfrak{a}^2$.

- (i) Show that $\text{Im}(\varphi) = {}_2\mathcal{C}(K)^+$.
- (ii) Show that $\text{Ker}(\varphi) = \mathcal{O}_K^+ \cdot (K^+)^2$.
- (iii) Let $\psi : \mathcal{O}_K^+ \rightarrow \Delta(K)/(K^+)^2$ be the homomorphism induced by the inclusion $\mathcal{O}_K^+ \subseteq \Delta(K)$. So $\psi(\nu) = \nu \cdot (K^+)^2$ for $\nu \in \mathcal{O}_K^+$. Show that $\text{Ker}(\psi) = (\mathcal{O}_K^+)^2$.

²Notation: for A an abelian group and $n \in \mathbb{N}^*$, the subgroup killed by n is denoted by ${}_n A$.

(iv) Conclude that we have a short exact sequence

$$1 \rightarrow \mathcal{O}_K^+ / (\mathcal{O}_K^+)^2 \rightarrow \Delta(K) / (K^+)^2 \rightarrow {}_2\mathcal{C}^+(K) \rightarrow 1.$$

(v) Show that $\mathcal{O}_K^+ / (\mathcal{O}_K^+)^2$ is of order 2.

(vi) Let $\alpha \in \Delta(K)$. Show that $N_{\mathbb{Q}}^K(\alpha) = t^2$, where $t \in \mathbb{Q}^+$.

(vii) Let σ be the nontrivial automorphism of K . Show that there is an element $\beta \in K^+$ such that $\frac{\alpha}{t} = \frac{\beta}{\sigma(\beta)}$. Conclude that $\alpha \equiv q \pmod{(K^+)^2}$ for a unique squarefree $q \in \mathbb{N}^*$.

(viii) Prove that $\Delta(K) / (K^+)^2$ is an elementary abelian 2-group of rank r .

(ix) Finally, show that $\text{rk}_2(\mathcal{C}^+(K)) = r - 1$.

9. In section 4.9 the 2-rank of the ideal class group of a quadratic number field has been computed using the algorithms for the ideal class groups given in the same chapter. Show that the formula for the 2-rank also follows from the computation in the previous exercise.

13 Ray Class Groups and Dirichlet Characters

Global class field theory is about abelian extensions of global fields. In this book mainly number fields are considered. In chapter 9 the absolute case was studied: abelian extensions of \mathbb{Q} . In this special case much can be done without class field theory in full generality. The description of class field theory in this book is from the ideal-theoretic viewpoint, which is in a sense the classical one. In a more modern approach one proceeds from local to global, starting with class field theory for local fields. Then for the global theory all completions of a number field, archimedean and \mathfrak{p} -adic, are considered simultaneously. In our approach local class field theory will follow from the global theory and finally, in the last chapter, the relation with the modern global theory will be established.

In case of an abelian number field the splitting behavior of a prime number is determined modulo some $N \in \mathbb{N}^*$, the conductor of the field. The splitting of a nonramifying prime number is described by its values under Dirichlet characters. If the base field K is an arbitrary number field, the situation is much more complicated: its ring of integers need not to be a principal ideal domain and generally there is more than one infinite prime. Nevertheless, there is a similar regularity: there is a conductor and there are Dirichlet characters. The ‘ray class groups’ take over the role of the groups $(\mathbb{Z}/N)^*$. They are described in the first section. Characters on the ray class groups will determine the (generalized) Dirichlet characters, which in this context are defined on the monoid of nonzero ideals. Our goal will be the Classification Theorem, which describes a correspondence between abelian extensions of a number field and finite groups of Dirichlet characters of this number field. Associated to an abelian extension of number fields we have two abelian groups: the Galois group and a group of Dirichlet characters. Moreover, we have a homomorphism of one group to the dual of the other, but the problem is to show that it is an isomorphism. In section 13.4 we make a first step: it will be shown by analytical means that the order of the group of Dirichlet characters is less than or equal to the order of the Galois group. In section 13.5 the map between these groups is described. The next chapter is devoted to the proof that it is actually an isomorphism. This is known as Artin’s Reciprocity Theorem. In chapter 15 the classification is completed with a proof of the existence theorem: each finite group of Dirichlet characters corresponds to an abelian extension.

13.1 Ray class groups

In chapter 14 we will see that there is regularity in the splitting of primes in an abelian extension of a number field K . This is what Artin's reciprocity is about. The description of this regularity uses ray class groups $\mathcal{C}_m(K)$, defined in Definition 13.3. They depend on a 'modulus' \mathfrak{m} , just as the groups $(\mathbb{Z}/N)^*$ depend on N . It turns out that, in this context, it is convenient to use the more general notion of prime: not only prime ideals but also the infinite primes as described in section 10.4.

13.1 Definitions and notations. Let K be a number field. A *modulus* of K is a formal product of primes of K , the finite ones can have an exponent > 1 . The exponent of an infinite prime is 0 or 1. The collection of moduli of K is denoted by $\mathcal{M}(K)$. Via unique factorization of ideals the products of finite primes correspond to nonzero ideals of \mathcal{O}_K . Products of infinite primes correspond to collections of infinite primes of K . So: a modulus \mathfrak{m} of K is determined by an ideal $\mathfrak{m}_0 \neq (0)$ of \mathcal{O}_K and a collection \mathfrak{m}_∞ of infinite primes. Notation: $\mathfrak{m} = \mathfrak{m}_0 \mathfrak{m}_\infty$.

The collection $\mathcal{M}(K)$ of moduli of K is an abelian monoid in an obvious way: the product of moduli \mathfrak{m} and \mathfrak{n} is $\mathfrak{m}_0 \mathfrak{n}_0 \mathfrak{m}_\infty \mathfrak{n}_\infty$, where $\mathfrak{m}_0 \mathfrak{n}_0$ is the product of ideals and $\mathfrak{m}_\infty \mathfrak{n}_\infty$ the union of the collections of infinite primes. The neutral element 1 of this monoid is the unit ideal \mathcal{O}_K . The notion of divisor comes with this monoid structure. Moreover the relation 'is a divisor of' is an ordering of the set of moduli. This ordering is such that we have the notions of greatest common divisor (gcd) and least common multiple (lcm).

The notation $\mathcal{M}(K)$ will be used for the monoid, the ordered set as well as for the category determined by the ordered set.

13.2 Notation. Let K be a number field and $\mathfrak{m} \in \mathcal{M}(K)$. Then

$$\mathbb{I}^{\mathfrak{m}}(K) := \{ \mathfrak{a} \in \mathbb{I}(K) \mid v_{\mathfrak{p}}(\mathfrak{a}) = 0 \text{ for all } \mathfrak{p} \mid \mathfrak{m}_0 \}.$$

The group $\mathbb{I}^{\mathfrak{m}}(K)$ depends only on the finite part \mathfrak{m}_0 of the modulus \mathfrak{m} . In the notation of section 6.4: $\mathbb{I}^{\mathfrak{m}}(K) = \mathbb{I}_Q(K)$, where $Q = \{ \mathfrak{p} \in \text{Max}(\mathcal{O}_K) \mid \mathfrak{p} \nmid \mathfrak{m}_0 \}$. It is a free abelian group on the set of finite primes not dividing \mathfrak{m}_0 :

$$\mathbb{I}^{\mathfrak{m}}(K) \xrightarrow{\sim} \bigoplus_{\substack{\mathfrak{p} \in \mathcal{P}_0(K) \\ \mathfrak{p} \nmid \mathfrak{m}_0}} \mathbb{Z},$$

where the maps $\mathbb{I}^{\mathfrak{m}}(K) \rightarrow \mathbb{Z}$ are the restrictions of the $v_{\mathfrak{p}}: \mathbb{I}(K) \rightarrow \mathbb{Z}$.

13.3 Definitions and notations. Let K be a number field and $\mathfrak{m} \in \mathcal{M}(K)$. Then

$$\begin{aligned} K_{\mathfrak{m}} &:= \{ \alpha \in K \mid v_{\mathfrak{p}}(\alpha) \geq 0 \text{ for all } \mathfrak{p} \mid \mathfrak{m}_0 \}, \\ K_{\mathfrak{m}}^1 &:= \{ \alpha \in K_{\mathfrak{m}}^* \mid v_{\mathfrak{p}}(\alpha - 1) \geq v_{\mathfrak{p}}(\mathfrak{m}_0) \text{ for all } \mathfrak{p} \mid \mathfrak{m}_0 \}, \end{aligned}$$

and $\sigma_{\mathfrak{p}}(\alpha) > 0$ for all real $\mathfrak{p} \mid \mathfrak{m}_{\infty}$ }

$$\begin{aligned} \mathbb{S}_{\mathfrak{m}}(K) &:= \{ \alpha \mathcal{O}_K \in \mathbb{I}(K) \mid \alpha \in K_{\mathfrak{m}}^1 \}, \\ \mathcal{C}_{\mathfrak{m}}(K) &:= \mathbb{I}^{\mathfrak{m}}(K) / \mathbb{S}_{\mathfrak{m}}(K). \end{aligned}$$

The ring $K_{\mathfrak{m}}$ is the localization K_P of \mathcal{O}_K , where $P = \{ \mathfrak{p} \in \text{Max}(\mathcal{O}_K) \mid \mathfrak{p} \mid \mathfrak{m}_0 \}$. It is a semi-local Dedekind domain; its group of units is

$$K_{\mathfrak{m}}^* = \{ \alpha \in K^* \mid v_{\mathfrak{p}}(\alpha) = 0 \text{ for all } \mathfrak{p} \mid \mathfrak{m}_0 \}$$

and $K_{\mathfrak{m}}^1$ is a subgroup of this group. Elements of $K_{\mathfrak{m}}^1$ are said to be 1 modulo \mathfrak{m} . The group $\mathbb{S}_{\mathfrak{m}}(K)$ is called the *ray* modulo \mathfrak{m} of K . The group $\mathcal{C}_{\mathfrak{m}}(K)$ is called the *ray class group* modulo \mathfrak{m} of the number field K .

For $\mathfrak{m} = \mathfrak{p}$, a finite prime, the ring $K_{\mathfrak{p}}$ is a discrete valuation ring. The notation $K_{\mathfrak{p}}$ usually is reserved for the \mathfrak{p} -adic completion of K , but in this context it is the valuation ring of the discrete valuation $v_{\mathfrak{p}}: K^* \rightarrow \mathbb{Z}$. For distinction we will sometimes use the notation $K_{\{\mathfrak{p}\}}$ for this ring. For \mathfrak{p} real infinite we have

$$K_{\mathfrak{p}}^1 = \{ \alpha \in K_{\mathfrak{p}}^* \mid \sigma_{\mathfrak{p}}(\alpha) > 0 \}$$

and for \mathfrak{p} complex infinite

$$K_{\mathfrak{p}}^1 = K_{\mathfrak{p}}^*.$$

The group $\mathbb{S}_{\mathfrak{m}}(K)$ is the group of principal fractional ideals of \mathcal{O}_K generated by elements 1 modulo \mathfrak{m} .

For the unit element (1) of the monoid $\mathcal{M}(K)$ we have $K_{(1)} = K$, $K_{(1)}^1 = K^*$, $\mathbb{S}_{(1)}(K) = \mathbb{P}(K)$ and $\mathcal{C}_{(1)}(K) = \mathcal{C}(K)$.

First we have a look at the structure of the groups $K_{\mathfrak{m}}^*/K_{\mathfrak{m}}^1$.

13.4 Lemma. *Let K be a number field and \mathfrak{m} a nonzero ideal of \mathcal{O}_K (= a product of finite primes of K). Then the inclusion $\mathcal{O}_K \rightarrow K_{\mathfrak{m}}$ induces an isomorphism*

$$(\mathcal{O}_K/\mathfrak{m})^* \xrightarrow{\sim} K_{\mathfrak{m}}^*/K_{\mathfrak{m}}^1.$$

PROOF. By Corollary 6.27(i) the inclusion $\mathcal{O}_K \rightarrow K_{\mathfrak{m}}$ induces a ring isomorphism $\mathcal{O}_K/\mathfrak{m} \xrightarrow{\sim} K_{\mathfrak{m}}/\mathfrak{m}K_{\mathfrak{m}}$ and hence also a group isomorphism $(\mathcal{O}_K/\mathfrak{m})^* \xrightarrow{\sim} (K_{\mathfrak{m}}/\mathfrak{m}K_{\mathfrak{m}})^*$. Since $K_{\mathfrak{m}}$ is semi-local, the ring homomorphism $K_{\mathfrak{m}} \rightarrow K_{\mathfrak{m}}/\mathfrak{m}K_{\mathfrak{m}}$ induces by the Chinese Remainder Theorem a surjective group homomorphism $K_{\mathfrak{m}}^* \rightarrow (K_{\mathfrak{m}}/\mathfrak{m}K_{\mathfrak{m}})^*$ and we have

$$K_{\mathfrak{m}}^1 = \text{Ker}(K_{\mathfrak{m}}^* \rightarrow (K_{\mathfrak{m}}/(\mathfrak{m}K_{\mathfrak{m}}))^*) = 1 + \mathfrak{m}K_{\mathfrak{m}}. \quad \square$$

13.5 Lemma. *Let K be a number field and $\mathfrak{m} \in \mathcal{M}(K)$. Then we have a short exact sequence*

$$1 \longrightarrow K_{\mathfrak{m}}^1 \xrightarrow{\subseteq} K_{\mathfrak{m}_0}^1 \longrightarrow \prod_{\substack{\mathfrak{p} \mid \mathfrak{m}_{\infty} \\ \mathfrak{p} \text{ real}}} \mu_2 \longrightarrow 1,$$

where the maps $K_{\mathfrak{m}_0}^1 \rightarrow \mu_2$ are given by $\alpha \mapsto \text{sgn}(\sigma_{\mathfrak{p}}(\alpha))$. (Here \prod stands for the direct product of groups.)

PROOF. The exactness at $K_{\mathfrak{m}_0}^1$ follows directly from the definition of $K_{\mathfrak{m}}^1$. It remains to show that the map $K_{\mathfrak{m}_0}^1 \rightarrow \prod \mu_2$ is surjective, i.e. that $K_{\mathfrak{m}_0}^1$ contains elements with prescribed signs under the real embeddings in \mathfrak{m}_∞ . Note that the ideal \mathfrak{m}_0 maps to a lattice in the real vector space $\mathbb{R}^r \times \mathbb{C}^s$ and that therefore the subset $1 + \mathfrak{m}_0$ of $K_{\mathfrak{m}_0}^*$ contains elements with prescribed signs. \square

13.6 Proposition. *Let K be a number field and $\mathfrak{m} \in \mathcal{M}(K)$. Then we have an isomorphism*

$$K_{\mathfrak{m}}^*/K_{\mathfrak{m}}^1 \xrightarrow{\sim} (\mathcal{O}_K/\mathfrak{m}_0)^* \times \prod_{\substack{\mathfrak{p}|\mathfrak{m}_\infty \\ \mathfrak{p} \text{ real}}} \mu_2 \quad (13.1)$$

induced by the inclusion $K_{\mathfrak{m}} \rightarrow K_{\mathfrak{m}_0}$ and the maps $K_{\mathfrak{m}}^* \rightarrow \mu_2$, $\alpha \mapsto \text{sgn}(\sigma_{\mathfrak{p}}(\alpha))$ for real $\mathfrak{p} | \mathfrak{m}_\infty$.

PROOF. The factor groups of $K_{\mathfrak{m}}^1 \subseteq K_{\mathfrak{m}_0}^1 \subseteq K_{\mathfrak{m}}^*$ form the short exact sequence

$$1 \longrightarrow \prod_{\substack{\mathfrak{p}|\mathfrak{m}_\infty \\ \mathfrak{p} \text{ real}}} \mu_2 \longrightarrow K_{\mathfrak{m}}^*/K_{\mathfrak{m}}^1 \longrightarrow (\mathcal{O}_K/\mathfrak{m}_0)^* \longrightarrow 1, \quad (13.2)$$

which is split in a natural way by the retract induced by the maps $K_{\mathfrak{m}}^* \rightarrow \mu_2$, $\alpha \mapsto \text{sgn}(\sigma_{\mathfrak{p}}(\alpha))$. \square

13.7 Corollary. *Let K be a number field and $\mathfrak{m}, \mathfrak{n} \in \mathcal{M}(K)$ such that $\mathfrak{m} | \mathfrak{n}$. Then the inclusion $K_{\mathfrak{n}}^* \rightarrow K_{\mathfrak{m}}^*$ induces a surjective homomorphism $K_{\mathfrak{n}}^*/K_{\mathfrak{n}}^1 \rightarrow K_{\mathfrak{m}}^*/K_{\mathfrak{m}}^1$.*

PROOF. In the commutative diagram with exact rows

$$\begin{array}{ccccccc} 1 & \longrightarrow & \prod_{\substack{\mathfrak{p}|\mathfrak{n}_\infty \\ \mathfrak{p} \text{ real}}} \mu_2 & \longrightarrow & K_{\mathfrak{n}}^*/K_{\mathfrak{n}}^1 & \longrightarrow & (\mathcal{O}_K/\mathfrak{n}_0)^* \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \downarrow \\ 1 & \longrightarrow & \prod_{\substack{\mathfrak{p}|\mathfrak{m}_\infty \\ \mathfrak{p} \text{ real}}} \mu_2 & \longrightarrow & K_{\mathfrak{m}}^*/K_{\mathfrak{m}}^1 & \longrightarrow & (\mathcal{O}_K/\mathfrak{m}_0)^* \longrightarrow 1 \end{array}$$

the vertical maps on the left and on the right are surjective; the last one as a consequence of the Chinese Remainder Theorem. \square

13.8 Definitions. For K a number field a contravariant functor

$$F: \mathcal{M}(K) \rightarrow \mathcal{A}b$$

is called an *arithmetic projective system* of K . This means that for each pair $\mathfrak{m}, \mathfrak{n} \in \mathcal{M}(K)$ with $\mathfrak{m} \mid \mathfrak{n}$ we have a group homomorphism $f_{\mathfrak{m}}^{\mathfrak{n}}: F(\mathfrak{n}) \rightarrow F(\mathfrak{m})$ such that

$$\begin{aligned} f_{\mathfrak{m}}^{\mathfrak{m}} &= 1_{F(\mathfrak{m})} && \text{for all } \mathfrak{m} \in \mathcal{M}(K), \\ f_{\mathfrak{m}_1}^{\mathfrak{m}_2} f_{\mathfrak{m}_2}^{\mathfrak{m}_3} &= f_{\mathfrak{m}_1}^{\mathfrak{m}_3} && \text{for all } \mathfrak{m}_1, \mathfrak{m}_2, \mathfrak{m}_3 \in \mathcal{M}(K) \text{ with } \mathfrak{m}_1 \mid \mathfrak{m}_2 \text{ and } \mathfrak{m}_2 \mid \mathfrak{m}_3. \end{aligned}$$

An arithmetic projective system F of K is called *multiplicative* if for all $\mathfrak{m}, \mathfrak{n} \in \mathcal{M}(K)$ with $\gcd(\mathfrak{m}, \mathfrak{n}) = 1$ the homomorphism

$$F(\mathfrak{m}\mathfrak{n}) \longrightarrow F(\mathfrak{m}) \oplus F(\mathfrak{n}), \quad x \mapsto (f_{\mathfrak{m}}^{\mathfrak{m}\mathfrak{n}}(x), f_{\mathfrak{n}}^{\mathfrak{m}\mathfrak{n}}(x))$$

is an isomorphism. An arithmetic projective system F of K is called *quasi-multiplicative* if it preserves bicartesian squares, i.e. for all $\mathfrak{m}, \mathfrak{n} \in \mathcal{M}(K)$ the diagram

$$\begin{array}{ccc} F(\text{lcm}(\mathfrak{m}, \mathfrak{n})) & \xrightarrow{f_{\mathfrak{n}}^{\text{lcm}(\mathfrak{m}, \mathfrak{n})}} & F(\mathfrak{n}) \\ \downarrow f_{\mathfrak{m}}^{\text{lcm}(\mathfrak{m}, \mathfrak{n})} & & \downarrow f_{\gcd(\mathfrak{m}, \mathfrak{n})}^{\mathfrak{n}} \\ F(\mathfrak{m}) & \xrightarrow{f_{\gcd(\mathfrak{m}, \mathfrak{n})}^{\mathfrak{m}}} & F(\gcd(\mathfrak{m}, \mathfrak{n})) \end{array} \quad (13.3)$$

is bicartesian.

13.9 Lemma. *An arithmetic projective system F of a number field K is multiplicative if and only if it is quasi-multiplicative and $F(1) = 0$.*

PROOF. For $\mathfrak{m} = \mathfrak{p}^r$ and $\mathfrak{n} = \mathfrak{p}^s$, say with $r \geq s$, we have $\gcd(\mathfrak{m}, \mathfrak{n}) = \mathfrak{p}^s$ and $\text{lcm}(\mathfrak{m}, \mathfrak{n}) = \mathfrak{p}^r$. So in this case the diagram (13.3) becomes

$$\begin{array}{ccc} F(\mathfrak{p}^r) & \xrightarrow{f_{\mathfrak{p}^s}^{\mathfrak{p}^r}} & F(\mathfrak{p}^s) \\ \downarrow 1 & & \downarrow 1 \\ F(\mathfrak{p}^r) & \xrightarrow{f_{\mathfrak{p}^s}^{\mathfrak{p}^r}} & F(\mathfrak{p}^s) \end{array}$$

which trivially is bicartesian. For multiplicative F diagram (13.3) is a finite direct sum of diagrams of this type. Hence such a system is quasi-multiplicative. For $\mathfrak{m} = \mathfrak{n} = 1$ the bicartesian diagram yields a short exact sequence

$$0 \rightarrow F(1) \xrightarrow{\sim} F(1) \oplus F(1) \rightarrow F(1) \rightarrow 0,$$

which shows that $F(1) = 0$.

Conversely, let F be quasi-multiplicative and such that $F(1) = 0$. Then for $\mathfrak{m}, \mathfrak{n} \in \mathcal{M}(K)$ with $\gcd(\mathfrak{m}, \mathfrak{n}) = 1$ the following diagram is bicartesian

$$\begin{array}{ccc} F(\mathfrak{mn}) & \xrightarrow{f_n^{\mathfrak{mn}}} & F(\mathfrak{n}) \\ f_m^{\mathfrak{mn}} \downarrow & & \downarrow f_1^{\mathfrak{n}} \\ F(\mathfrak{m}) & \xrightarrow{f_1^{\mathfrak{m}}} & F(1) \end{array}$$

Since $F(1) = 0$ this means that the corresponding homomorphism $F(\mathfrak{mn}) \rightarrow F(\mathfrak{m}) \oplus F(\mathfrak{n})$ is an isomorphism. Hence F is multiplicative. \square

13.10 Proposition. *The arithmetic projective system $\mathfrak{m} \mapsto K_{\mathfrak{m}}^*/K_{\mathfrak{m}}^1$ of a number field K is multiplicative.*

PROOF. For the modulus 1 we have $K_1^* = K^* = K_1^1$ and so K_1^*/K_1^1 is trivial. By Lemma 13.9 it suffices to show that the system is quasi-multiplicative. Let $\mathfrak{m}_1, \mathfrak{m}_2 \in \mathcal{M}(K)$ and put $\mathfrak{m} = \gcd(\mathfrak{m}_1, \mathfrak{m}_2)$ and $\mathfrak{n} = \text{lcm}(\mathfrak{m}_1, \mathfrak{m}_2)$. Via the isomorphism (13.1) the square

$$\begin{array}{ccc} K_{\mathfrak{n}}^*/K_{\mathfrak{n}}^1 & \longrightarrow & K_{\mathfrak{m}_2}^*/K_{\mathfrak{m}_2}^1 \\ \downarrow & & \downarrow \\ K_{\mathfrak{m}_1}^*/K_{\mathfrak{m}_1}^1 & \longrightarrow & K_{\mathfrak{m}}^*/K_{\mathfrak{m}}^1 \end{array}$$

is the direct product of two squares, one of them being

$$\begin{array}{ccc} (\mathcal{O}_K/\mathfrak{n}_0)^* & \longrightarrow & (\mathcal{O}_K/\mathfrak{m}_{2,0})^* \\ \downarrow & & \downarrow \\ (\mathcal{O}_K/\mathfrak{m}_{1,0})^* & \longrightarrow & (\mathcal{O}_K/\mathfrak{m}_0)^*. \end{array}$$

The groups in this square are the unit groups of the rings in

$$\begin{array}{ccc} \mathcal{O}_K/\mathfrak{n}_0 & \longrightarrow & \mathcal{O}_K/\mathfrak{m}_{2,0} \\ \downarrow & & \downarrow \\ \mathcal{O}_K/\mathfrak{m}_{1,0} & \longrightarrow & \mathcal{O}_K/\mathfrak{m}_0 \end{array}$$

and this square is bicartesian since $\mathfrak{n}_0 = \text{lcm}(\mathfrak{m}_{1,0}, \mathfrak{m}_{2,0}) = \mathfrak{m}_{1,0} \cap \mathfrak{m}_{2,0}$ and $\mathfrak{m}_0 = \text{gcd}(\mathfrak{m}_{1,0}, \mathfrak{m}_{2,0}) = \mathfrak{m}_{1,0} + \mathfrak{m}_{2,0}$. It follows that the square of groups of units is cartesian as well and since the homomorphisms in this square are surjective, it is bicartesian. The other of the two squares in the product is easily seen to be bicartesian as well. \square

By Proposition 13.6 the group $K_{\mathfrak{m}}^*/K_{\mathfrak{m}}^1$ is finite. Its order is $\#(\mathcal{O}_K/\mathfrak{m}_0) \cdot 2^t$, where t is the number of real infinite primes in \mathfrak{m}_∞ . Let's define $\varphi(\mathfrak{m}) = \#(K_{\mathfrak{m}}^*/K_{\mathfrak{m}}^1)$. Then φ is multiplicative in the following sense:

$$\varphi(\mathfrak{m}\mathfrak{n}) = \varphi(\mathfrak{m})\varphi(\mathfrak{n}) \quad \text{if } \text{gcd}(\mathfrak{m}, \mathfrak{n}) = 1.$$

The function φ generalizes the Euler totient function.

13.11 Example. Let $m \in \mathbb{N}^*$ with $m \geq 3$ and let ∞ be the unique real infinite prime of \mathbb{Q} . We compute $\mathbb{Q}_{\mathfrak{m}}^*/\mathbb{Q}_{\mathfrak{m}}^1$, where $\mathfrak{m} = (m)\infty$. Note that $\mathbb{Q}_{\infty}^* = \mathbb{Q}^*$ and $\mathbb{Q}_{\infty}^1 = \mathbb{Q}^+$. We have

$$\mathbb{Q}_{\mathfrak{m}}^*/\mathbb{Q}_{\mathfrak{m}}^1 \xrightarrow{\sim} \mathbb{Q}_{(m)}^*/\mathbb{Q}_{(m)}^1 \times \mathbb{Q}^*/\mathbb{Q}^+ \xrightarrow{\sim} (\mathbb{Z}/m)^* \times \mu_2. \tag{13.4}$$

The class of an $x \in \mathbb{Z} \setminus m\mathbb{Z}$ in $\mathbb{Q}_{\mathfrak{m}}^*/\mathbb{Q}_{\mathfrak{m}}^1$ maps under this isomorphism to $(\bar{x}, \text{sgn}(x))$.

13.12 Example. Let K be a number field. For K the modulus ∞ denotes the product of all infinite primes of K . We have $K_{\infty} = K$ and $K_{\infty}^1 = K^+$ in the notation of exercise 10 of chapter 6. So $K_{\infty}^*/K_{\infty}^1 = K^*/K^+ \xrightarrow{\sim} \mu_2^r$, where r is the number of real infinite primes of K . The ray $\mathbb{S}_{\infty}(K)$ is the group of principal fractional ideals generated by totally positive elements and the ray class group $\mathbb{I}(K)/\mathbb{S}_{\infty}(K)$ is the narrow ideal class group $\mathcal{C}^+(K)$.

Let \mathfrak{m} be a modulus of a number field K . By Proposition 2.28 the restriction $\mathbb{I}^{\mathfrak{m}}(K) \rightarrow \mathcal{C}(K)$ of the canonical map $\mathbb{I}(K) \rightarrow \mathcal{C}(K)$ is surjective. If $\mathfrak{a} \in \mathbb{I}^{\mathfrak{m}}(K)$ is in the kernel of this map, then $\mathfrak{a} = \alpha\mathcal{O}_K$ for an $\alpha \in K^*$. Clearly $\alpha \in K_{\mathfrak{m}}^*$, so the sequence

$$K_{\mathfrak{m}}^* \longrightarrow \mathbb{I}^{\mathfrak{m}}(K) \longrightarrow \mathcal{C}(K) \longrightarrow 1$$

is exact. It follows that the ker-coker exact sequence of the triangle

$$\begin{array}{ccc}
 K_m^1 & \longrightarrow & \mathbb{I}^m(K) \\
 & \searrow & \nearrow \\
 & & K_m^*
 \end{array}$$

is the exact sequence

$$1 \longrightarrow \mathcal{O}_K^* \cap K_m^1 \longrightarrow \mathcal{O}_K^* \longrightarrow K_m^*/K_m^1 \longrightarrow \mathcal{C}_m(K) \longrightarrow \mathcal{C}(K) \longrightarrow 1. \quad (13.5)$$

Since the groups K_m^*/K_m^1 and $\mathcal{C}(K)$ are finite, the ray class group $\mathcal{C}_m(K)$ is finite as well. More precisely, the exact sequence (13.5) implies:

13.13 Theorem. *Let m be a modulus of the number field K . Then we have a short exact sequence*

$$1 \longrightarrow K_m^*/K_m^1 \mathcal{O}_K^* \longrightarrow \mathcal{C}_m(K) \longrightarrow \mathcal{C}(K) \longrightarrow 1. \quad \square$$

13.14 Example. For the modulus $(m)_\infty$ of Example 13.11 the isomorphism (13.4) induces an isomorphism

$$\mathbb{Q}_m^*/\mathbb{Q}_m^1 \mu_2 \xrightarrow{\sim} (\mathbb{Z}/m)^*$$

which maps the class of an $x \in \mathbb{Z} \setminus m\mathbb{Z}$ to $\overline{|x|}$. By Theorem 13.13 we have an isomorphism $(\mathbb{Z}/m)^* \xrightarrow{\sim} \mathcal{C}_m(\mathbb{Q})$, which for $a \in \mathbb{Z} \setminus m\mathbb{Z}$ sends \overline{a} to the class of (a) in $\mathcal{C}_m(\mathbb{Q})$. For the modulus (m) we have an isomorphism

$$\mathbb{Q}_{(m)}^*/\mathbb{Q}_{(m)}^1 \mu_2 \xrightarrow{\sim} (\mathbb{Z}/m)^*/\langle \overline{-1} \rangle$$

and the isomorphism $(\mathbb{Z}/m)^*/\langle \overline{-1} \rangle \xrightarrow{\sim} \mathcal{C}_{(m)}(\mathbb{Q})$ sends the class represented by an $a \in \mathbb{Z} \setminus m\mathbb{Z}$ to the class of (a) .

In chapter 9 a correspondence has been established between abelian number fields and finite groups of Dirichlet characters. These characters are essentially characters of groups $(\mathbb{Z}/N)^*$. In our approach to class field theory the groups $\mathcal{C}_m(K)$ will play the role of the groups $(\mathbb{Z}/N)^*$ in the absolute case. We derive some properties for ray class groups which are similar to properties of the groups $(\mathbb{Z}/N)^*$.

13.15 Proposition. *Let m and n be moduli of a number field K such that $m \mid n$. Then the inclusion $\mathbb{I}^n(K) \rightarrow \mathbb{I}^m(K)$ induces a surjective homomorphism $\mathcal{C}_n(K) \rightarrow \mathcal{C}_m(K)$.*

PROOF. We have a commutative diagram

$$\begin{array}{ccccccc}
 1 & \longrightarrow & K_n^*/K_n^1 \mathcal{O}_K^* & \longrightarrow & \mathcal{C}_n(K) & \longrightarrow & \mathcal{C}(K) \longrightarrow 1 \\
 & & \downarrow & & \downarrow & & \parallel \\
 1 & \longrightarrow & K_m^*/K_m^1 \mathcal{O}_K^* & \longrightarrow & \mathcal{C}_m(K) & \longrightarrow & \mathcal{C}(K) \longrightarrow 1
 \end{array}$$

in which by Theorem 13.13 the rows are short exact sequences. By Corollary 13.7 the map $K_n^* \rightarrow K_m^*/K_m^1\mathcal{O}_K^*$ is surjective. So also $\mathcal{C}_n(K) \rightarrow \mathcal{C}_m(K)$ is surjective. \square

We will have a closer look at the arithmetic projective system $\mathfrak{m} \mapsto \mathcal{C}_m(K)$ of the number field K . It's convenient to convert bicartesian squares into short exact sequences as described at the end of section 9.2.

13.16 Lemma. *Let*

$$\begin{array}{ccccccccc}
 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \\
 & & \downarrow & \searrow & \downarrow & \searrow & \downarrow & \searrow & \\
 & & 0 & \longrightarrow & A_2 & \longrightarrow & B_2 & \longrightarrow & C_2 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
 0 & \longrightarrow & A_1 & \longrightarrow & B_1 & \longrightarrow & C_1 & \longrightarrow & 0 \\
 & & \downarrow & \searrow & \downarrow & \searrow & \downarrow & \searrow & \\
 & & 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0
 \end{array}$$

be a short exact sequence of commutative squares of abelian groups. If two of the three commutative squares are bicartesian, then so is the third.

PROOF. The short exact sequence of commutative squares translates into a short exact sequence of complexes (the columns in the diagram):

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 0 & \longrightarrow & A_1 \oplus A_2 & \longrightarrow & B_1 \oplus B_2 & \longrightarrow & C_1 \oplus C_2 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
 \end{array}$$

If two of these complexes are exact, then so is the third. The proposition follows from this. \square

There is an obvious notion of morphism of arithmetic projective systems:

13.17 Definition. Let F_1 and F_2 be arithmetic projective systems of a number field K . A *morphism of arithmetic projective systems* $g: F_1 \rightarrow F_2$ is a system $(g_m)_{\mathfrak{m} \in \mathcal{M}(K)}$ of group homomorphisms $g_m: F_1(\mathfrak{m}) \rightarrow F_2(\mathfrak{m})$ such that for all $\mathfrak{m}, \mathfrak{n} \in \mathcal{M}(K)$ with $\mathfrak{m} \mid \mathfrak{n}$ the diagram

$$\begin{array}{ccc}
 F_1(\mathfrak{n}) & \xrightarrow{g_{\mathfrak{n}}} & F_2(\mathfrak{n}) \\
 f_{\mathfrak{m}}^{\mathfrak{n}} \downarrow & & \downarrow f_{\mathfrak{m}}^{\mathfrak{n}} \\
 F_1(\mathfrak{m}) & \xrightarrow{g_{\mathfrak{m}}} & F_2(\mathfrak{m})
 \end{array}$$

commutes. (Or for short: g is a morphism of functors.)

Since bicartesian squares correspond to short exact sequences as in the proof of Lemma 13.16 we have for arithmetic projective systems:

13.18 Corollary. *Let $0 \rightarrow F' \rightarrow F \rightarrow F'' \rightarrow 0$ a short exact sequence of arithmetic projective systems of a number field K . If two of them are quasi-multiplicative, respectively multiplicative, then so is the third.*

PROOF. For quasi-multiplicativity this is immediate and for multiplicativity it follows from Lemma 13.9. \square

13.19 Lemma. *The arithmetic projective system $\mathfrak{m} \mapsto K_{\mathfrak{m}}^1$ of a number field K is quasi-multiplicative.*

PROOF. For moduli \mathfrak{m} of K we have short exact sequences

$$1 \longrightarrow K_{\mathfrak{m}}^* \longrightarrow K^* \longrightarrow \bigoplus_{\mathfrak{p}|\mathfrak{m}_0} \mathbb{Z} \longrightarrow 0$$

and

$$1 \longrightarrow K_{\mathfrak{m}}^1 \longrightarrow K_{\mathfrak{m}}^* \longrightarrow K_{\mathfrak{m}}^*/K_{\mathfrak{m}}^1 \longrightarrow 1.$$

The arithmetic projective systems

$$\mathfrak{m} \mapsto K^*, \quad \mathfrak{m} \mapsto \bigoplus_{\mathfrak{p}|\mathfrak{m}_0} \mathbb{Z} \quad \text{and} \quad \mathfrak{m} \mapsto K_{\mathfrak{m}}^*/K_{\mathfrak{m}}^1$$

are quasi-multiplicative, the last one by Proposition 13.10. So by Corollary 13.18 the system $\mathfrak{m} \mapsto K_{\mathfrak{m}}^1$ is quasi-multiplicative as well. \square

13.20 Proposition. *Let \mathfrak{m}_1 and \mathfrak{m}_2 be moduli of a number field K . Then for $\mathfrak{m} = \text{gcd}(\mathfrak{m}_1, \mathfrak{m}_2)$ and $\mathfrak{n} = \text{lcm}(\mathfrak{m}_1, \mathfrak{m}_2)$ the square*

$$\begin{array}{ccc}
 \mathcal{C}_{\mathfrak{n}}(K) & \longrightarrow & \mathcal{C}_{\mathfrak{m}_2}(K) \\
 \downarrow & & \downarrow \\
 \mathcal{C}_{\mathfrak{m}_1}(K) & \longrightarrow & \mathcal{C}_{\mathfrak{m}}(K)
 \end{array}$$

of canonical projections is cocartesian.

PROOF. By Lemma 13.19 we have a commutative diagram with exact rows

$$\begin{array}{ccccccc}
 1 & \longrightarrow & K_n^1 & \longrightarrow & K_{m_1}^1 \times K_{m_2}^1 & \longrightarrow & K_m^1 \longrightarrow 1 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 1 & \longrightarrow & \mathbb{I}^n(K) & \longrightarrow & \mathbb{I}^{m_1}(K) \times \mathbb{I}^{m_2}(K) & \longrightarrow & \mathbb{I}^m(K) \longrightarrow 1
 \end{array}$$

and by taking cokernels of the vertical maps we obtain an exact sequence

$$\mathcal{C}_n(K) \longrightarrow \mathcal{C}_{m_1}(K) \times \mathcal{C}_{m_2}(K) \longrightarrow \mathcal{C}_m(K) \longrightarrow 1. \quad \square$$

13.2 Dirichlet characters of a number field

Let K be a number field. Dirichlet characters of K are essentially characters of ray class groups of K . They will generalize the Dirichlet characters defined in section 9.3 for the field \mathbb{Q} . There is, however, a subtle difference, see Example 13.28.

13.21 Definitions and notation. Let K be a number field and \mathfrak{m} a modulus of K . A *Dirichlet character modulo \mathfrak{m}* of K is a map $\chi: \mathbb{I}^+(K) \rightarrow \mathbb{C}$ satisfying

- (DC1) for all $\mathfrak{a} \in \mathbb{I}^+(K)$: $\chi(\mathfrak{a}) \neq 0 \iff \gcd(\mathfrak{a}, \mathfrak{m}_0) = 1$,
- (DC2) $\chi(\mathfrak{a}\mathfrak{b}) = \chi(\mathfrak{a})\chi(\mathfrak{b})$ for all $\mathfrak{a}, \mathfrak{b} \in \mathbb{I}^+(K)$,
- (DC3) $\chi(\alpha\mathcal{O}_K) = \chi(\beta\mathcal{O}_K)$ for all $\alpha, \beta \in \mathcal{O}_K \setminus \{0\}$ with $\alpha \equiv \beta \pmod{\mathfrak{m}_0}$ and $\text{sgn}(\sigma_{\mathfrak{p}}(\alpha)) = \text{sgn}(\sigma_{\mathfrak{p}}(\beta))$ for all real primes $\mathfrak{p} \mid \mathfrak{m}_{\infty}$.

If χ is a Dirichlet character modulo \mathfrak{m} of K , then

$$\mathcal{C}_m(K) \rightarrow \mathbb{C}^*, \quad \frac{\mathfrak{a}}{\mathfrak{b}} \mapsto \chi(\mathfrak{a})\chi(\mathfrak{b})^{-1} \quad (\text{for } \mathfrak{a} \text{ and } \mathfrak{b} \text{ are ideals relatively prime to } \mathfrak{m}_0)$$

is a character of the ray class group modulo \mathfrak{m} . Conversely, a character $\chi: \mathcal{C}_m(K) \rightarrow \mathbb{C}^*$ determines a Dirichlet character modulo \mathfrak{m} of K :

$$\mathbb{I}^+(K) \rightarrow \mathbb{C}, \quad \mathfrak{a} \mapsto \begin{cases} \chi(\mathfrak{a}) & \text{if } \gcd(\mathfrak{a}, \mathfrak{m}_0) = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Thus Dirichlet characters modulo \mathfrak{m} of K correspond to characters of the ray class group $\mathcal{C}_m(K)$. Since ray class groups are finite, Dirichlet characters take only 0 and roots of unity as values. In particular a Dirichlet character is an ideal character

in the sense of Definition 8.29. The set of Dirichlet characters modulo \mathfrak{m} of K is denoted by $\mathcal{H}_{\mathfrak{m}}(K)$. It is a group under $(\chi_1\chi_2)(\mathfrak{a}) = \chi_1(\mathfrak{a})\chi_2(\mathfrak{a})$; the conjugate character $\bar{\chi}: \mathfrak{a} \mapsto \overline{\chi(\mathfrak{a})}$ of a Dirichlet character χ is the inverse of χ . The group $\mathcal{H}_{\mathfrak{m}}(K)$ is naturally isomorphic to $\mathcal{C}_{\mathfrak{m}}(K)^{\vee}$, the dual of the ray class group.

These Dirichlet characters were introduced by Hecke. That is why I have chosen for the \mathcal{H} -notation. Nowadays the name Hecke character is reserved for characters of idèle class groups, see section 20.2 for the notion of idèle class group. The Dirichlet characters then correspond to Hecke characters of finite order.

A Dirichlet character χ modulo (1) is a multiplicative map $\chi: \mathbb{I}^+(K) \rightarrow \mathbb{C}$ with roots of unity as values and $\chi(\mathfrak{a}) = 1$ for all principal ideals \mathfrak{a} . It induces a character χ of $\mathbb{I}(K)$ with $\chi(\mathfrak{a}) = 1$ for all fractional principal ideals \mathfrak{a} .

As was the case for Dirichlet characters as defined in chapter 9, we can multiply Dirichlet characters of a number field even if their moduli differ:

13.22 Definition. Let \mathfrak{m}_1 and \mathfrak{m}_2 be moduli of a number field K , $\chi_1 \in \mathcal{H}_{\mathfrak{m}_1}(K)$ and $\chi_2 \in \mathcal{H}_{\mathfrak{m}_2}(K)$. We define $\chi_1\chi_2: \mathbb{I}^+(K) \rightarrow \mathbb{C}$ by

$$(\chi_1\chi_2)(\mathfrak{a}) = \chi_1(\mathfrak{a})\chi_2(\mathfrak{a})$$

for all $\mathfrak{a} \in \mathbb{I}^+(K)$. Then $\chi_1\chi_2 \in \mathcal{H}_{\text{lcm}(\mathfrak{m}_1, \mathfrak{m}_2)}(K)$.

Also for these Dirichlet characters we have the notions of induced and primitive character, which we now will make precise. Let \mathfrak{m} and \mathfrak{n} be moduli of a number field K such that $\mathfrak{m} \mid \mathfrak{n}$. Then by Proposition 13.15 we have a canonical surjective group homomorphism $\mathcal{C}_{\mathfrak{n}}(K) \rightarrow \mathcal{C}_{\mathfrak{m}}(K)$. This homomorphism induces an injective homomorphism $\mathcal{C}_{\mathfrak{m}}(K)^{\vee} \rightarrow \mathcal{C}_{\mathfrak{n}}(K)^{\vee}$ and thereby an injective group homomorphism $i_{\mathfrak{n}}^{\mathfrak{m}}: \mathcal{H}_{\mathfrak{m}}(K) \rightarrow \mathcal{H}_{\mathfrak{n}}(K)$. For $\chi \in \mathcal{H}_{\mathfrak{m}}(K)$ the Dirichlet character $i_{\mathfrak{n}}^{\mathfrak{m}}(\chi)$ is given by

$$(i_{\mathfrak{n}}^{\mathfrak{m}}(\chi))(\mathfrak{a}) = \begin{cases} \chi(\mathfrak{a}) & \text{if } \gcd(\mathfrak{a}, \mathfrak{n}_0) = 1, \\ 0 & \text{otherwise.} \end{cases}$$

13.23 Definition. Let \mathfrak{m} and \mathfrak{n} be moduli of a number field K such that $\mathfrak{m} \mid \mathfrak{n}$ and let $\chi \in \mathcal{H}_{\mathfrak{m}}(K)$. Then the Dirichlet character $i_{\mathfrak{n}}^{\mathfrak{m}}(\chi) \in \mathcal{H}_{\mathfrak{n}}(K)$ is said to be *induced* by χ . A Dirichlet character modulo \mathfrak{n} of K is said to be a *primitive* Dirichlet character modulo \mathfrak{n} of K if it is not induced by a Dirichlet character modulo a proper divisor of \mathfrak{n} .

From Proposition 13.20 follows:

13.24 Proposition. Let \mathfrak{m}_1 and \mathfrak{m}_2 be moduli of a number field K . Then for $\mathfrak{m} = \gcd(\mathfrak{m}_1, \mathfrak{m}_2)$ and $\mathfrak{n} = \text{lcm}(\mathfrak{m}_1, \mathfrak{m}_2)$ the square

$$\begin{array}{ccc}
 \mathcal{H}_{\mathfrak{m}}(K) & \longrightarrow & \mathcal{H}_{\mathfrak{m}_2}(K) \\
 \downarrow & & \downarrow \\
 \mathcal{H}_{\mathfrak{m}_1}(K) & \longrightarrow & \mathcal{H}_{\mathfrak{n}}(K)
 \end{array}$$

of canonical injections is cartesian. □

From this it follows that every Dirichlet character of K is induced by a unique primitive Dirichlet character of K .

13.25 Definition. Let χ be a Dirichlet character of the number field K . The modulus of the unique primitive Dirichlet character by which χ is induced is called the *conductor* of χ . Notation: \mathfrak{f}_χ .

13.26 Change of notation and terminology. From now on by a Dirichlet character we always mean a Dirichlet character modulo its conductor: Dirichlet characters are assumed to be primitive. They form a group $\mathcal{H}(K)$. The notation $\mathcal{H}_{\mathfrak{m}}(K)$ will now be used for the subgroup of $\mathcal{H}(K)$ of all Dirichlet characters χ of K with $\mathfrak{f}_\chi \mid \mathfrak{m}$. That means that in $\mathcal{H}_{\mathfrak{m}}(K)$ as originally defined all characters are replaced by primitive characters and that the multiplication is changed accordingly. Under this convention it follows from Proposition 13.24 that

$$\mathcal{H}_{\gcd(\mathfrak{m}_1, \mathfrak{m}_2)}(K) = \mathcal{H}_{\mathfrak{m}_1}(K) \cap \mathcal{H}_{\mathfrak{m}_2}(K).$$

Henceforth, Dirichlet characters in the sense of Definition 13.21 will be referred to as *Dirichlet pre-characters*.

13.27 Definition. Let K be a number field and X a finite subgroup of $\mathcal{H}(K)$. The least modulus \mathfrak{m} of K for which $X \subseteq \mathcal{H}_{\mathfrak{m}}(K)$ is called the *conductor* of X . Notation: \mathfrak{f}_X .

Obviously, the conductor of a finite group of Dirichlet characters is the least common multiple of the conductors of the Dirichlet characters in this group.

13.28 Example. There is a one-to-one correspondence between Dirichlet characters as defined in chapter 9 and Dirichlet characters of \mathbb{Q} as defined in this section. It is induced by the bijection $\mathbb{N}^* \rightarrow \mathbb{I}^+(\mathbb{Q})$, $n \mapsto n\mathbb{Z}$. Thus a Dirichlet character $\chi: \mathbb{Z} \rightarrow \mathbb{C}$ corresponds to the Dirichlet character of \mathbb{Q} defined on finite primes by $p\mathbb{Z} \mapsto \chi(p)$. A Dirichlet character χ of \mathbb{Q} determines a Dirichlet character in the sense of chapter 9 determined by $n \mapsto \chi(n\mathbb{Z})$ for $n \in \mathbb{N}^*$. The conductor of the Dirichlet character of \mathbb{Q} corresponding to a Dirichlet character χ is (N_χ) if χ is even, i.e. if $\chi(-1) = 1$, and it is $(N_\chi)\infty$ if χ is odd. The monoid isomorphism $\mathbb{N}^* \xrightarrow{\sim} \mathbb{I}^+(\mathbb{Q})$ induces a group isomorphism $\mathcal{H}(\mathbb{Q}) \xrightarrow{\sim} \mathcal{D}$ and for $m \in \mathbb{N}^*$ it restricts to $\mathcal{H}_{(m)\infty}(\mathbb{Q}) \xrightarrow{\sim} \mathcal{D}_m$.

Dirichlet characters are determined by their value on finite primes up to a finite number of primes:

13.29 Lemma. *Let χ_1 and χ_2 be Dirichlet characters of a number field K and \mathfrak{m} a modulus of K . Suppose that $\chi_1(\mathfrak{a}) = \chi_2(\mathfrak{a})$ for all $\mathfrak{a} \in \mathbb{I}^{\mathfrak{m}+}(K)$. Then $\chi_1 = \chi_2$.*

PROOF. Choose a modulus \mathfrak{n} which is a multiple of \mathfrak{f}_{χ_1} , \mathfrak{f}_{χ_2} and \mathfrak{m} . Then the Dirichlet characters χ_1 and χ_2 induce the same Dirichlet pre-character modulo \mathfrak{n} and are therefore equal. \square

The main theorem of class field theory is the Classification Theorem. It describes finite abelian extensions of a number field K in terms of Dirichlet characters. Such extensions will correspond to finite subgroups of $\mathcal{H}(K)$. We will conclude this section by describing the group of Dirichlet characters that is going to correspond to a given abelian extension. The description uses the notion of norm for fractional ideals as described in section 7.6.

13.30 Notational convention. Let $L : K$ be a number field extension. A modulus \mathfrak{m} of K determines a modulus of L : the modulus with finite part $j_L^K(\mathfrak{m}_0) = \mathfrak{m}_0 \mathcal{O}_L$ and as infinite part all infinite primes of L above infinite primes in \mathfrak{m}_∞ . This modulus of L will also be denoted by \mathfrak{m} .

13.31 Proposition. *Let $L : K$ be a number field extension and \mathfrak{m} a modulus of K . Then $j_L^K(\mathbb{I}^{\mathfrak{m}}(K)) \subseteq \mathbb{I}^{\mathfrak{m}}(L)$, $N_K^L(\mathbb{I}^{\mathfrak{m}}(L)) \subseteq \mathbb{I}^{\mathfrak{m}}(K)$, $N_K^L(L_{\mathfrak{m}}^1) \subseteq K_{\mathfrak{m}}^1$ and $N_K^L(\mathbb{S}_{\mathfrak{m}}(L)) \subseteq \mathbb{S}_{\mathfrak{m}}(K)$.*

PROOF. The first two inclusions follow directly from the definitions. The last inclusion is, by Proposition 7.67, a direct consequence of the third, so it remains to prove that $N_K^L(L_{\mathfrak{m}}^1) \subseteq K_{\mathfrak{m}}^1$.

Let $M : K$ be the normal closure of $L : K$ and $\sigma_1, \dots, \sigma_k$ the embeddings of L in M which leave the elements of K fixed. Choose prolongations—also named $\sigma_1, \dots, \sigma_k$ —of these embeddings to automorphisms of M . Then for each $\alpha \in L$ we have $N_K^L(\alpha) = \sigma_1(\alpha) \cdots \sigma_k(\alpha)$.

Since $K_{\mathfrak{m}_1}^1 \cap K_{\mathfrak{m}_2}^1 = K_{\mathfrak{m}_1 \mathfrak{m}_2}^1$ if $\gcd(\mathfrak{m}_1, \mathfrak{m}_2) = 1$, it suffices to prove that $N_K^L(L_{\mathfrak{p}r}^1) \subseteq K_{\mathfrak{p}r}^1$ for primes \mathfrak{p} of K . We will do so separately for \mathfrak{p} finite and \mathfrak{p} infinite.

Let $\alpha \in L_{\mathfrak{p}r}^1$, where \mathfrak{p} is a finite prime of K and $r \in \mathbb{N}^*$. Then $v_{\mathfrak{q}}(\alpha - 1) \geq e_K(\mathfrak{q})r$ for all primes \mathfrak{q} of L above \mathfrak{p} . Hence for all primes \mathfrak{r} of M above \mathfrak{p} we have

$$v_{\mathfrak{r}}(\alpha - 1) \geq e_L(\mathfrak{r})e_K(\mathfrak{q})r = e_{\mathfrak{p}}^{(M)}r,$$

where \mathfrak{q} is the prime of L under \mathfrak{r} . For each of the automorphisms σ_j and each of the primes \mathfrak{r} of M above \mathfrak{p} we have

$$v_{\mathfrak{r}}(\sigma_j(\alpha) - 1) = v_{\mathfrak{r}}(\sigma_j(\alpha - 1)) = v_{\sigma_j^{-1}(\mathfrak{r})}(\alpha - 1) \geq e_{\mathfrak{p}}^{(M)}r.$$

Put $e = e_{\mathfrak{p}}^{(M)}$ and let \mathfrak{r} be a prime of M above \mathfrak{p} . Then the above inequality means that $\sigma_j(\alpha) \in M_{\mathfrak{r}^{er}}^1$ and so

$$N_K^L(\alpha) = \sigma_1(\alpha) \cdots \sigma_k(\alpha) \in M_{\mathfrak{r}^{er}}^1,$$

that is $v_{\mathfrak{r}}(N_K^L(\alpha) - 1) \geq er$. Since $v_{\mathfrak{r}}(N_K^L(\alpha) - 1) = e \cdot v_{\mathfrak{p}}(N_K^L(\alpha) - 1)$, it follows that $v_{\mathfrak{p}}(N_K^L(\alpha) - 1) \geq r$, meaning that $N_K^L(\alpha) \in K_{\mathfrak{p}^r}^1$.

Let $\alpha \in L_{\mathfrak{p}}^1$, where \mathfrak{p} is the real infinite prime corresponding to an embedding $\sigma: K \rightarrow \mathbb{R}$. Choose a prolongation $\tau: M \rightarrow \mathbb{C}$ of σ to M . Then the k embeddings $\tau\sigma_1, \dots, \tau\sigma_k: M \rightarrow \mathbb{C}$ have different restrictions to L : if $\tau\sigma_i(\beta) = \tau\sigma_j(\beta)$ for all $\beta \in L$, then by injectivity of τ we have $\sigma_i(\beta) = \sigma_j(\beta)$ for all $\beta \in L$. Hence

$$\sigma(N_K^L(\alpha)) = \tau(N_K^L(\alpha)) = \tau\sigma_1(\alpha) \cdots \tau\sigma_k(\alpha)$$

and this is a positive real number: $\tau\sigma_i(\alpha) > 0$ for all real prolongations $\tau\sigma_i$ of σ and the factors $\tau\sigma_j(\alpha)$ for all complex prolongations $\tau\sigma_j$ come in pairs, which are complex conjugates. \square

The notion of transfer for ideal class groups is now easily generalized to ray class groups.

13.32 Definitions and notations. Let $L: K$ be a number field extension and \mathfrak{m} a modulus of K . By Proposition 13.31 the norm map $N_K^L: \mathbb{I}(L) \rightarrow \mathbb{I}(K)$ induces a homomorphism $\mathcal{C}_{\mathfrak{m}}(L) \rightarrow \mathcal{C}_{\mathfrak{m}}(K)$, the *transfer*, denoted by tr_K^L . The cokernel of this map is denoted by $\mathcal{C}_{\mathfrak{m}}(L: K)$:

$$\mathcal{C}_{\mathfrak{m}}(L: K) = \mathbb{I}^{\mathfrak{m}}(K) / N_K^L(\mathbb{I}^{\mathfrak{m}}(L)) \mathbb{S}_{\mathfrak{m}}(K).$$

As for ideal class groups we have:

13.33 Corollary. *Let $L: K$ be a Galois extension of number fields and \mathfrak{m} a modulus of K . Then the ray class groups modulo \mathfrak{m} form a Galois module with transfers associated to $L: K$. The transfer map being the map given in Definition 13.32.* \square

For an extension $L: K$ of number fields and a modulus \mathfrak{m} of K the transfer $\text{tr}_K^L: \mathcal{C}_{\mathfrak{m}}(L) \rightarrow \mathcal{C}_{\mathfrak{m}}(K)$ induces a map from $\mathcal{H}_{\mathfrak{m}}(K)$ to $\mathcal{H}_{\mathfrak{m}}(L)$. Since for any \mathfrak{m} this last map is induced by $N_K^L: \mathbb{I}(L) \rightarrow \mathbb{I}(K)$, we have a map $\mathcal{H}(K) \rightarrow \mathcal{H}(L)$:

13.34 Definitions and notations. Let $L: K$ be a number field extension. Then the norm map $N_K^L: \mathbb{I}(L) \rightarrow \mathbb{I}(K)$ induces a map $\nu_L^K: \mathcal{H}(K) \rightarrow \mathcal{H}(L)$, the *conorm map*. The kernel of ν_L^K is denoted by $\mathcal{H}(L: K)$; its elements are called *Dirichlet characters of $L: K$* . The subgroup of $\mathcal{H}(L: K)$ consisting of Dirichlet characters of $L: K$ with conductor a divisor of a modulus \mathfrak{m} of K is denoted by $\mathcal{H}_{\mathfrak{m}}(L: K)$, so

$$\mathcal{H}_{\mathfrak{m}}(L: K) = \mathcal{H}(L: K) \cap \mathcal{H}_{\mathfrak{m}}(K).$$

It is the kernel of the map $\mathcal{H}_{\mathfrak{m}}(K) \rightarrow \mathcal{H}_{\mathfrak{m}}(L)$ and so it is isomorphic to the dual of $\mathcal{C}_{\mathfrak{m}}(L: K)$, the cokernel of $\mathcal{C}_{\mathfrak{m}}(L) \rightarrow \mathcal{C}_{\mathfrak{m}}(K)$.

By Lemma 13.29 the Dirichlet character $\nu_L^K(\chi)$ of L is determined by $\nu_L^K(\chi)(\mathfrak{q}) = \chi(N_K^L(\mathfrak{q}))$ for all but finitely many primes \mathfrak{q} of L . The group $\mathcal{H}(L : K)$ consists of all Dirichlet characters $\chi \in \mathcal{H}(K)$ with the property that $\chi(N_K^L(\mathfrak{a})) = 1$ for all $\mathfrak{a} \in \mathbb{I}^+(L)$, where \mathfrak{f} is the conductor of χ .

The groups $\mathcal{H}(L : K)$ for abelian $L : K$ are important for class field theory. In section 13.5 their role is explained. A direct consequence of the definition is the following.

13.35 Lemma. *Let $L_1 : K$ and $L_2 : L_1$ be number field extensions. Then $\mathcal{H}(L_1 : K) \subseteq \mathcal{H}(L_2 : K)$.*

PROOF. The conorm map $\nu_{L_2}^K : \mathcal{H}(K) \rightarrow \mathcal{H}(L_2)$ is the composition of the conorm maps $\nu_{L_1}^K$ and $\nu_{L_2}^{L_1}$. So for the kernels of the conorm maps we have $\mathcal{H}(L_1 : K) \subseteq \mathcal{H}(L_2 : K)$. \square

13.3 Counting ideals in ray classes

Let K be a number field of degree d . We have seen that the Dedekind zeta function $\zeta_K(s)$ is meromorphic on the halfplane $\Re(s) > 1 - \frac{1}{d}$ with only a simple pole in $s = 1$ (Theorem 8.20). The residue in $s = 1$ was computed by counting ideals in ideal classes. Instead of ideal classes we now count, more generally, ideals in ray classes.

13.36 Definition. Let K be a number field and \mathfrak{m} a modulus of K . The *partial zeta function* of a ray class C modulo \mathfrak{m} is defined by the Dirichlet series

$$\zeta(s, C) = \sum_{n=1}^{\infty} \frac{j_C(n)}{n^s} = \sum_{\mathfrak{a} \in C \cap \mathbb{I}^+(K)} \frac{1}{N(\mathfrak{a})^s},$$

where $j_C(n) = \#\{\mathfrak{a} \in C \cap \mathbb{I}^+(K) \mid N(\mathfrak{a}) = n\}$.

For the convergence of the Dirichlet series we consider

$$J_C(N) = \#\{\mathfrak{a} \in C \cap \mathbb{I}^+(K) \mid N(\mathfrak{a}) \leq N\} = \sum_{n=1}^N j_C(n).$$

We proceed as in section 8.2. Fix an ideal $\mathfrak{b} \in C^{-1}$. Then we have a correspondence

$$\left\{ \begin{array}{l} \text{ideals } \mathfrak{a} \text{ in } C \\ \text{with } N(\mathfrak{a}) \leq N \end{array} \right\} \begin{array}{l} \longrightarrow \\ \longleftarrow \end{array} \left\{ \begin{array}{l} \text{principal ideals } (\alpha) \subseteq \mathfrak{b} \\ \text{with } |N_{\mathbb{Q}}^K(\alpha)| \leq N \cdot N(\mathfrak{b}), \alpha \equiv 1 \pmod{\mathfrak{m}_0} \\ \text{and } \sigma_{\mathfrak{p}}(\alpha) > 0 \text{ for all real } \mathfrak{p} \mid \mathfrak{m}_{\infty} \end{array} \right\}$$

$$\begin{array}{ccc} \mathfrak{a} & \longmapsto & \mathfrak{a}\mathfrak{b} \\ \alpha\mathfrak{b}^{-1} & \longleftarrow & (\alpha) \end{array}$$

Choose an $\alpha_0 \in \mathcal{O}_K$ such that

$$\alpha_0 \equiv \begin{cases} 1 \pmod{\mathfrak{m}_0} \\ 0 \pmod{\mathfrak{b}}. \end{cases}$$

The last set can then be described as follows:

the set of all principal ideals (α) with $|\mathbb{N}_{\mathbb{Q}}^K(\alpha)| \leq N \cdot \mathbb{N}(\mathfrak{b})$,
 $\alpha \equiv \alpha_0 \pmod{\mathfrak{m}_0\mathfrak{b}}$ and $\sigma_{\mathfrak{p}}(\alpha) > 0$ for all real $\mathfrak{p} \mid \mathfrak{m}_{\infty}$.

So instead of counting ideals we can count principal ideals:

$$J_C(N) = \#\{(\alpha) \in \mathbb{I}^+(K) \mid \alpha \equiv \alpha_0 \pmod{\mathfrak{m}_0\mathfrak{b}}, |\mathbb{N}(\alpha)| \leq N \cdot \mathbb{N}(\mathfrak{b}) \\ \text{and } \sigma_{\mathfrak{p}}(\alpha) > 0 \text{ for all real } \mathfrak{p} \mid \mathfrak{m}_{\infty}\}.$$

Choose a fundamental system $\varepsilon_1, \dots, \varepsilon_{r+s-1}$ for the group of units $\mathcal{O}_K^* \cap K_{\mathfrak{m}}^1$. Note that by the exactness of sequence 13.5 and the finiteness of $K_{\mathfrak{m}}^*/K_{\mathfrak{m}}^1$ its rank is equal to the rank of \mathcal{O}_K^* . Use this system of units instead of the fundamental system used in section 8.2. It follows that we have to count the elements of $(\iota(\alpha_0) + \Lambda_{\mathfrak{b}}) \cap D_{N \cdot \mathbb{N}(\mathfrak{m}_0\mathfrak{b})}$ which are positive under the embeddings $\sigma_{\mathfrak{p}}$ for real $\mathfrak{p} \mid \mathfrak{m}_{\infty}$. Put $w_{\mathfrak{m}} = \#(\mu(K) \cap K_{\mathfrak{m}}^1)$. Then the computation in section 8.2 leads to

$$w_{\mathfrak{m}} \cdot J_C(N) = \kappa_C N + O(N^{1-\frac{1}{d}}),$$

where, t being the number of real $\mathfrak{p} \mid \mathfrak{m}_{\infty}$,

$$w_{\mathfrak{m}} \cdot \kappa_C = \frac{\text{vol}(D_1)\mathbb{N}(\mathfrak{b})}{2^t \delta(\Lambda_{\mathfrak{m}_0\mathfrak{b}})}.$$

For the sake of obtaining simpler formulas the following notations will be used.

13.37 Definitions and notations. Let K be a number field and let \mathfrak{m} be a modulus of K . Then, $\text{Reg}(\mathfrak{m})$, the *regulator* of \mathfrak{m} is defined as follows

$$\text{Reg}(\mathfrak{m}) = \text{Reg}(\mathcal{O}_K^* \cap K_{\mathfrak{m}}^1).$$

Furthermore, we write

$$\mathbb{N}(\mathfrak{m}) = \#(K_{\mathfrak{m}}^*/K_{\mathfrak{m}}^1) = 2^t \mathbb{N}(\mathfrak{m}_0)$$

and call it the *norm* of \mathfrak{m} .

Thus we have

$$\text{Reg}(\mathfrak{m}) = \frac{(\mathcal{O}_K^* : (\mathcal{O}_K^* \cap K_{\mathfrak{m}}^1))}{w(K)/w_{\mathfrak{m}}} \text{Reg}(K) \tag{13.6}$$

and the formula for $w_{\mathfrak{m}} \cdot \kappa_C$ becomes

$$w_{\mathfrak{m}} \cdot \kappa_C = \frac{2^{r+s} \text{vol}(D')\mathbb{N}(\mathfrak{b})}{2^t \mathbb{N}(\mathfrak{m}_0\mathfrak{b}) \sqrt{|\text{disc}(K)|}} = \frac{2^{r+s} \pi^s \text{Reg}(\mathfrak{m})}{2^t \mathbb{N}(\mathfrak{m}_0) \sqrt{|\text{disc}(K)|}} = \frac{2^r (2\pi)^s \text{Reg}(\mathfrak{m})}{\mathbb{N}(\mathfrak{m}) \sqrt{|\text{disc}(K)|}}.$$

Let's summarize this in a theorem:

13.38 Theorem. *Let K be a number field of degree d , \mathfrak{m} a modulus of K and C a ray class modulo \mathfrak{m} of K . Then the number $J_C(N)$ of ideals \mathfrak{a} of \mathcal{O}_K with $N(\mathfrak{a}) \leq N$ satisfies*

$$J_C(N) = \kappa_C N + O(N^{1-\frac{1}{d}}),$$

where

$$\kappa_C = \frac{2^{r(K)}(2\pi)^{s(K)} \operatorname{Reg}(\mathfrak{m})}{\#(\mu(K) \cap K_{\mathfrak{m}}^1) N(\mathfrak{m}) \sqrt{|\operatorname{disc}(K)|}}. \quad \square$$

For $\zeta(s, C)$ this implies the following.

13.39 Theorem. *Let K , d , \mathfrak{m} and C be as in Theorem 13.38. Then $\zeta(s, C)$ has a continuation to a meromorphic function on the half-plane $\sigma > 1 - \frac{1}{d}$ with only a simple pole at $s = 1$ with residue κ_C .* \square

Using equation (13.6) we get

$$\kappa_C = \frac{2^{r(K)}(2\pi)^{s(K)} \operatorname{Reg}(K)}{w(K) \sqrt{|\operatorname{disc}(K)|}} \cdot \frac{(\mathcal{O}_K^* : (\mathcal{O}_K^* \cap K_{\mathfrak{m}}^1))}{N(\mathfrak{m})}.$$

This formula already follows from the fact alone that κ_C does not depend on C . This can be seen as follows.

$$\sum_{C \in \mathcal{C}_{\mathfrak{m}}(K)} \zeta(s, C) = \sum_{\mathfrak{a} \in \mathbb{I}^{\mathfrak{m}+}} \frac{1}{N(\mathfrak{a})^s} = \prod_{\mathfrak{p} | \mathfrak{m}_0} \frac{1}{1 - \frac{1}{N(\mathfrak{p})^s}} = \zeta_K(s) \cdot \prod_{\mathfrak{p} | \mathfrak{m}_0} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right).$$

Put $h_{\mathfrak{m}}(K) = \#(\mathcal{C}_{\mathfrak{m}}(K))$. Then for the residue in $s = 1$ we have:

$$\begin{aligned} h_{\mathfrak{m}}(K) \cdot \kappa_C &= h(K) \cdot \frac{2^{r(K)}(2\pi)^{s(K)} \operatorname{Reg}(K)}{w(K) \sqrt{|\operatorname{disc}(K)|}} \cdot \prod_{\mathfrak{p} | \mathfrak{m}_0} \left(1 - \frac{1}{N(\mathfrak{p})}\right) \\ &= h(K) \cdot \frac{2^{r(K)}(2\pi)^{s(K)} \operatorname{Reg}(K)}{w(K) \sqrt{|\operatorname{disc}(K)|}} \cdot \frac{\#((\mathcal{O}_K/\mathfrak{m}_0)^*)}{N(\mathfrak{m}_0)} \end{aligned}$$

and by the exactness of sequence (13.5)

$$\frac{h(K)}{h_{\mathfrak{m}}(K)} = \frac{(\mathcal{O}_K^* : (\mathcal{O}_K^* \cap K_{\mathfrak{m}}^1))}{\#(K_{\mathfrak{m}}^*/K_{\mathfrak{m}}^1)} = \frac{(\mathcal{O}_K^* : (\mathcal{O}_K^* \cap K_{\mathfrak{m}}^1))}{2^t \cdot \#((\mathcal{O}_K/\mathfrak{m}_0)^*)}.$$

So it follows that indeed

$$\begin{aligned} \kappa_C &= \frac{2^{r(K)}(2\pi)^{s(K)} \operatorname{Reg}(K)}{w(K) \sqrt{|\operatorname{disc}(K)|}} \cdot \frac{(\mathcal{O}_K^* : (\mathcal{O}_K^* \cap K_{\mathfrak{m}}^1))}{2^t N(\mathfrak{m}_0)} \\ &= \frac{2^{r(K)}(2\pi)^{s(K)} \operatorname{Reg}(K)}{w(K) \sqrt{|\operatorname{disc}(K)|}} \cdot \frac{(\mathcal{O}_K^* : (\mathcal{O}_K^* \cap K_{\mathfrak{m}}^1))}{N(\mathfrak{m})}. \end{aligned}$$

13.4 Dirichlet L-series and the First Fundamental Inequality

In this section we use the notion of Dirichlet density to show that for a Galois extension $L : K$ of number fields the group $\mathcal{H}(L : K)$ is finite and that its order is at most $[L : K]$.

13.40 Definition. Let K be a number field and $\chi \in \mathcal{H}(K)$. The series

$$L(s, \chi) = \sum_{\mathfrak{a} \in \mathbb{I}^+(K)} \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s}$$

is called the *L-series* of the Dirichlet character χ .

The *L-series* of the trivial Dirichlet character is just the Dedekind zeta function of K . It has a simple pole at $s = 1$. For the other Dirichlet characters we have the following.

13.41 Proposition. Let χ be a nontrivial Dirichlet character. The series $L(s, \chi)$ converges absolutely on the half-plane $\sigma > 1$ and has a continuation to an analytic function on the half-plane $\sigma > 1 - \frac{1}{d}$, where d is the degree of K .

PROOF. Put $\mathfrak{f} = \mathfrak{f}_\chi$. The *L-series* converges absolutely on the half-plane $\sigma > 1$ as does any Dirichlet series associated to an ideal character (Proposition 8.31). Since χ is a Dirichlet character, the value $\chi(\mathfrak{a})$ is zero if and only if $\gcd(\mathfrak{f}, \mathfrak{a}) = 0$, so

$$L(s, \chi) = \sum_{\mathfrak{a} \in \mathbb{I}^+(K)} \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s} = \sum_{\mathfrak{a} \in \mathbb{I}^+(\mathfrak{f}, K)} \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s}.$$

The value $\chi(\mathfrak{a})$ only depends on the ray class modulo \mathfrak{f} of \mathfrak{a} . So

$$\begin{aligned} L(s, \chi) &= \sum_{C \in \mathcal{C}_f(K)} \sum_{\mathfrak{a} \in C \cap \mathbb{I}^+(K)} \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s} = \sum_{C \in \mathcal{C}_f(K)} \chi(C) \sum_{\mathfrak{a} \in C \cap \mathbb{I}^+(K)} \frac{1}{N(\mathfrak{a})^s} \\ &= \sum_{C \in \mathcal{C}_f(K)} \chi(C) \zeta(s, C). \end{aligned}$$

By Theorem 13.38 all $\zeta(s, C)$ have continuations to meromorphic functions on $\sigma > 1 - \frac{1}{d}$ and have only a simple pole at $s = 1$. The residue κ_f of $\zeta(s, C)$ doesn't depend on C . So $L(s, \chi)$ has a continuation to a meromorphic function on $\sigma > 1 - \frac{1}{d}$ and has at most one simple pole at $s = 1$. But since χ is nontrivial and

$$\sum_{C \in \mathcal{C}_f(K)} \chi(C) \kappa_f = \kappa_f \sum_{C \in \mathcal{C}_f(K)} \chi(C) = 0,$$

the continued function $L(s, \chi)$ is analytic at $s = 1$ as well. □

As was the case for the Dirichlet characters in chapter 9, for nontrivial Dirichlet characters the L -series has a continuation to an analytic function on the whole complex plane. Neukirch gives a detailed exposition in [31] in which the complexity is built up gradually by subsequently considering the Riemann zeta function, the L -series of a Dirichlet character (in the sense of chapter 9), the Dedekind zeta function of a number field and, finally, the L -series of a Dirichlet character of a number field.

13.42 Proposition. *Let K be a number field and X a finite group of Dirichlet characters of K . Then the set*

$$P = \{ \mathfrak{p} \in \text{Max}(\mathcal{O}_K) \mid \chi(\mathfrak{p}) = 1 \text{ for all } \chi \in X \}$$

has a Dirichlet density. Moreover $\delta(P) \leq \frac{1}{h}$, where $h = \#(X)$.

PROOF. Proposition 8.31 implies that $\sum_{\mathfrak{p}} \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s}$ converges absolutely on the half-plane $\sigma > 1$ for each Dirichlet character χ and

$$\log L(s, \chi) \sim \sum_{\mathfrak{p}} \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s} = \sum_{\mathfrak{p} \nmid \mathfrak{f}} \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s},$$

where \mathfrak{f} is the conductor of X . We have

$$\sum_{\chi \in X} \sum_{\mathfrak{p} \nmid \mathfrak{f}} \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s} = \sum_{\mathfrak{p} \nmid \mathfrak{f}} \sum_{\chi \in X} \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s} = \sum_{\mathfrak{p} \in P} \frac{h}{N(\mathfrak{p})^s}.$$

Hence

$$\sum_{\mathfrak{p} \in P} \frac{1}{N(\mathfrak{p})^s} \sim \frac{1}{h} \sum_{\chi \in X} \log L(s, \chi) = -\frac{1}{h} \log(s-1) + \frac{1}{h} \sum_{\substack{\chi \in X \\ \chi \neq 1}} \log L(s, \chi).$$

By Proposition 13.41 the functions $L(s, \chi)$ are for $\chi \neq 1$ analytic at $s = 1$. So if we knew that $L(1, \chi) \neq 0$ for these χ (which is in fact the case, as we will see later), we could conclude that $\delta(P) = \frac{1}{h}$. For now, let n_χ be the multiplicity of the zero at $s = 1$ of the function $L(s, \chi)$ (possibly $n_\chi = 0$, as in fact is the case), that is

$$\frac{L(s, \chi)}{(s-1)^{n_\chi}}$$

does not vanish at $s = 1$. Then

$$\log L(s, \chi) \sim n_\chi \log(s-1)$$

and

$$\sum_{\mathfrak{p} \in P} \frac{1}{N(\mathfrak{p})^s} \sim -\frac{1}{h} \log(s-1) + \frac{\sum_{\chi \neq 1} n_\chi}{h} \log(s-1) = -\frac{1 - \sum_{\chi \neq 1} n_\chi}{h} \log(s-1).$$

So we have

$$\delta(P) = \frac{1 - \sum_{\chi \neq 1} n_\chi}{h} \leq \frac{1}{h}. \quad \square$$

Since the Dirichlet density cannot be negative, for at most one of the characters $\chi \in X$ the function $L(s, \chi)$ can have a zero at $s = 1$ and, moreover, it can only be a simple root. Let χ^* be this exceptional character in X . It must be a real character, since otherwise the character $\overline{\chi^*}$ would be exceptional as well. It will turn out that this situation doesn't occur.

The proof of Proposition 13.42 shows the following.

13.43 Corollary. *In the notation of Proposition 13.42: if $\delta(P) = \frac{1}{h}$, then $L(1, \chi) \neq 0$ for all $\chi \neq 1$ in X .* □

13.44 Theorem (The First Fundamental Inequality). *Let $L : K$ be a Galois extension of number fields. Then the group $\mathcal{H}(L : K)$ is finite and $\#(\mathcal{H}(L : K)) \leq [L : K]$.*

PROOF. Since $\mathcal{H}(L : K)$ is a torsion group it suffices to prove that the order of each finite subgroup of $\mathcal{H}(L : K)$ is at most $[L : K]$. So let X be a finite subgroup of $\mathcal{H}(L : K)$, say $\#(X) = h$. Let P be as in Proposition 13.42. Then $\delta(P) \leq \frac{1}{h}$. By Theorem 8.37 the set

$$Q = \{ \mathfrak{p} \in \text{Max}(\mathcal{O}_K) \mid \mathfrak{p} \text{ splits completely in } L \text{ and } \mathfrak{p} \nmid \mathfrak{f}_X \}$$

has Dirichlet density $\frac{1}{[L:K]}$. If $\mathfrak{p} \in Q$, then for $\mathfrak{q} \in \text{Max}(\mathcal{O}_L)$ above \mathfrak{p} we have $\mathfrak{q} \in \mathbb{I}^{\mathfrak{f}_X}(L)$ and $N_K^L(\mathfrak{q}) = \mathfrak{p}$. From $X \subseteq \mathcal{H}(L : K)$ follows that $\chi(\mathfrak{p}) = \nu_L^K(\chi)(\mathfrak{q}) = 1$. So $Q \subseteq P$ and as a consequence we have for the Dirichlet densities

$$\frac{1}{[L : K]} = \delta(Q) \leq \delta(P) \leq \frac{1}{h}. \quad \square$$

The finiteness of $\mathcal{H}(L : K)$ makes the following definition possible.

13.45 Definition and notation. Let $L : K$ be an abelian number field extension. The *conductor* of the extension $L : K$ is the conductor of the finite group $\mathcal{H}(L : K)$. Notation for this conductor: $\mathfrak{f}_K(L)$.

For a Galois extension $L : K$ of number fields and a modulus \mathfrak{m} of K we have

$$\mathcal{H}_\mathfrak{m}(L : K) = \mathcal{H}(L : K) \iff \mathcal{H}(L : K) \subseteq \mathcal{H}_\mathfrak{m}(K) \iff \mathfrak{f}_K(L) \mid \mathfrak{m}.$$

Therefore, for multiples \mathfrak{m} of $\mathfrak{f}_K(L)$ the groups $\mathcal{C}_\mathfrak{m}(L : K)$ are all isomorphic. More precisely:

13.46 Proposition. *Let $L : K$ be a Galois extension of number fields, $\mathfrak{f} = \mathfrak{f}_K(L)$ and \mathfrak{m} a modulus of K such that $\mathfrak{f} \mid \mathfrak{m}$. Then the inclusion $\mathbb{I}^\mathfrak{m}(K) \subseteq \mathbb{I}^\mathfrak{f}(K)$ induces an isomorphism $\mathcal{C}_\mathfrak{m}(L : K) \xrightarrow{\sim} \mathcal{C}_\mathfrak{f}(L : K)$.* □

13.5 The Artin map

The Artin map of an abelian number field extension is defined on the subgroup of $\mathbb{I}(K)$ generated by the nonramifying prime ideals and takes values in the Galois group of the extension:

13.47 Definition and notation. Let $L : K$ be an abelian extension of number fields. The subgroup of $\mathbb{I}(K)$ generated by all prime ideals of K which do not ramify in L is denoted by $\mathbb{I}^L(K)$. So

$$\mathbb{I}^L(K) = \{ \mathfrak{a} \in \mathbb{I}(K) \mid v_{\mathfrak{p}}(\mathfrak{a}) = 0 \text{ for all in } L \text{ ramifying } \mathfrak{p} \in \text{Max}(\mathcal{O}_K) \}.$$

The *Artin map* of $L : K$ is the map

$$\varphi_K^{(L)} : \mathbb{I}^L(K) \rightarrow \text{Gal}(L : K), \quad \mathfrak{a} \mapsto \prod_{\substack{\mathfrak{p} \in \text{Max}(\mathcal{O}_K) \\ e_{\mathfrak{p}}^{(L)} = 1}} (\varphi_{\mathfrak{p}}^{(L)})^{v_{\mathfrak{p}}(\mathfrak{a})}.$$

The kernel of $\varphi_K^{(L)}$ is called the *Artin kernel* of $L : K$.

Thus the Artin map is given on the basis elements \mathfrak{p} of the free abelian group $\mathbb{I}^L(K)$ by mapping \mathfrak{p} to the Frobenius automorphism of \mathfrak{p} in $\text{Gal}(L : K)$. The Artin map $\varphi_K^{(L)}$ is also called the *Artin symbol*, in which case often a notation like $\left(\frac{L:K}{\mathfrak{a}}\right)$ is used for $\varphi_K^{(L)}(\mathfrak{a})$.

For each modulus \mathfrak{m} of K , which is divisible by all in L ramifying primes, the group $\mathbb{I}^{\mathfrak{m}}(L)$ is a subgroup of $\mathbb{I}^L(K)$, so for such \mathfrak{m} the Artin map has a restriction to this subgroup:

$$\varphi_K^{(L)}|_{\mathfrak{m}} : \mathbb{I}^{\mathfrak{m}}(K) \rightarrow \text{Gal}(L : K), \quad \mathfrak{a} \mapsto \varphi_K^{(L)}(\mathfrak{a}).$$

13.48 Theorem. Let $L : K$ be an abelian extension of number fields and \mathfrak{m} a modulus of K which is a multiple of all in L ramifying finite primes of K . Then the Artin map, restricted to $\mathbb{I}^{\mathfrak{m}}(K)$,

$$\varphi_K^{(L)}|_{\mathfrak{m}} : \mathbb{I}^{\mathfrak{m}}(K) \rightarrow \text{Gal}(L : K)$$

is surjective.

PROOF. According to the Frobenius Density Theorem for abelian extensions (Theorem 8.39) each cyclic subgroup of $\text{Gal}(L : K)$ is generated by the Frobenius automorphism of some nonramifying finite prime $\mathfrak{p} \nmid \mathfrak{m}$ of K . \square

In the next chapter it will be shown that, given an abelian extension $L : K$ of number fields, there exists a modulus \mathfrak{m} of K such that the ray $\mathbb{S}_{\mathfrak{m}}(K)$ is contained in the Artin kernel of $L : K$. This has far-going implications. It is the reason why

ray class groups have been introduced. If for some modulus \mathfrak{m} the group $\mathbb{S}_{\mathfrak{m}}(K)$ is in the Artin kernel, then the Artin map induces a surjective homomorphism $\mathcal{C}_{\mathfrak{m}}(K) \rightarrow \text{Gal}(L : K)$ of finite groups.

13.49 Definition. Let $L : K$ be an abelian number field extension. A modulus \mathfrak{m} of K is called a *modulus for $L : K$* if

(M1) all in L ramifying finite primes of K are divisors of \mathfrak{m} ,

(M2) $\mathbb{S}_{\mathfrak{m}}(K) \subseteq \text{Ker}(\varphi_K^{(L)}|_{\mathfrak{m}})$.

Note that (M1) is necessary for the Artin map to be defined. Later, in chapter 15, we will see that the moduli for $L : K$ are the multiples of the conductor $f_K(L)$. It will be shown that the prime divisors of the conductor are just the ramifying primes, finite and infinite. So far we do not even know whether moduli for abelian number field extensions do exist.

For the determination of the Artin kernel it is important to realize that it contains the norms of fractional ideals:

13.50 Proposition. *Let $L : K$ be an abelian number field extension and \mathfrak{m} a modulus of K which is a multiple of all finite ramifying primes. Then $N_K^L(\mathbb{I}^{\mathfrak{m}}(L)) \subseteq \text{Ker}(\varphi_K^{(L)})$.*

PROOF. It suffices to show that $\varphi_K^{(L)}(N_K^L(\mathfrak{q})) = 1$ for every unramified finite prime \mathfrak{q} of L . For such a \mathfrak{q} we have $N_K^L(\mathfrak{q}) = \mathfrak{p}^{f_{\mathfrak{p}}^{(L)}}$, where $\mathfrak{p} = \mathfrak{q} \cap K$. The order of $\varphi_{\mathfrak{p}}^{(L)}$ equals $f_{\mathfrak{p}}^{(L)}$ and hence $N_K^L(\mathfrak{q})$ is in the kernel of the Artin map. \square

If \mathfrak{m} is a modulus for the abelian extension $L : K$ of number fields, then it are precisely the ray classes represented by norms of fractional ideals which constitute the Artin kernel:

13.51 Theorem. *Let $L : K$ be an abelian number field extension and \mathfrak{m} a modulus for $L : K$. Then*

$$\text{Ker}(\varphi_K^{(L)}|_{\mathfrak{m}}) = N_K^L(\mathbb{I}^{\mathfrak{m}}(L))\mathbb{S}_{\mathfrak{m}}(K).$$

PROOF. By Proposition 13.50 we have

$$N_K^L(\mathbb{I}^{\mathfrak{m}}(L))\mathbb{S}_{\mathfrak{m}}(K) \subseteq \text{Ker}(\varphi_K^{(L)}|_{\mathfrak{m}})$$

and by Theorem 13.44

$$\#(\mathbb{I}^{\mathfrak{m}}(K)/N_K^L(\mathbb{I}^{\mathfrak{m}}(L))\mathbb{S}_{\mathfrak{m}}(K)) = \#(\mathcal{H}(L : K) \cap \mathcal{H}_{\mathfrak{m}}(K)) \leq [L : K].$$

By Theorem 13.48 the index of the Artin kernel in $\mathbb{I}^{\mathfrak{m}}(K)$ is $[L : K]$. So the two subgroups coincide. \square

13.52 Corollary. *Let $L : K$ be an abelian number field extension and \mathfrak{m} a modulus for $L : K$. Then the Artin map $\varphi_K^{(L)}$ induces an isomorphism*

$$\mathbb{I}^{\mathfrak{m}}(K)/\mathbb{N}_K^L(\mathbb{I}^{\mathfrak{m}}(L))\mathbb{S}_{\mathfrak{m}}(K) \xrightarrow{\sim} \text{Gal}(L : K).$$

PROOF. This is a direct consequence of Theorem 13.48 and Theorem 13.51. \square

Artin's Reciprocity Theorem (Theorem 14.16) states that for every abelian number field extension there exists a modulus and moreover, that for such a modulus it suffices to be divisible by all ramifying primes, the finite ones to a sufficiently high power.

The Artin map of a subextension is given by restriction of the automorphism to the subfield:

13.53 Lemma (Consistency property). *Let $L : K$ be an abelian number field extension and L' an intermediate field of $L : K$. Then $\varphi_K^{(L')}(\mathfrak{a}) = \varphi_K^{(L)}(\mathfrak{a})|_{L'}$ for all $\mathfrak{a} \in \mathbb{I}^L(K)$.*

PROOF. A finite prime \mathfrak{p} of K that does not ramify in L , does not ramify in L' either and for the Frobenius automorphisms we have $\varphi_{\mathfrak{p}}^{(L')} = \varphi_{\mathfrak{p}}^{(L)}|_{L'}$. \square

The behavior of the Artin map under a base field extension is as follows.

13.54 Lemma. *Let $K' : K$ be a number field extension, $L : K$ an abelian number field extension, \mathfrak{m} a modulus of K divisible by all finite in L ramifying primes of K and $\mathfrak{a} \in \mathbb{I}^{\mathfrak{m}}(K')$. Then*

$$\varphi_{K'}^{(LK')}(\mathfrak{a})|_L = \varphi_K^{(L)}(\mathbb{N}_K^{K'}(\mathfrak{a})).$$

PROOF. The maps $\mathfrak{a} \mapsto \varphi_{K'}^{(LK')}(\mathfrak{a})|_L$ and $\mathfrak{a} \mapsto \varphi_K^{(L)}(\mathbb{N}_K^{K'}(\mathfrak{a}))$ are both group homomorphisms from $\mathbb{I}^{\mathfrak{m}}(K')$ to $\text{Gal}(L : K)$, so it suffices to show that they coincide on the generating prime ideals of $\mathbb{I}^{\mathfrak{m}}(K')$. Let $\mathfrak{p}' \in \text{Max}(\mathcal{O}_{K'})$ with $\mathfrak{p}' \nmid \mathfrak{m}$ and put $\mathfrak{p} = \mathfrak{p}' \cap K$ and $f = f_K(\mathfrak{p}')$. Then by Proposition 7.80 and the definition of the norm of a fractional ideal (Definition 7.65)

$$\varphi_{K'}^{(LK')}(\mathfrak{p}')|_L = \varphi_{\mathfrak{p}'}^{(LK')}|_L = (\varphi_{\mathfrak{p}}^{(L)})^f = \varphi_K^{(L)}(\mathfrak{p}^f) = \varphi_K^{(L)}(\mathbb{N}_K^{K'}(\mathfrak{p}')). \quad \square$$

For the existence of a modulus for abelian extensions it suffices to consider cyclic extensions:

13.55 Proposition. *If there are moduli for cyclic number field extensions, then there is one for any abelian number field extension.*

PROOF. Let $L : K$ be an abelian number field extension. The dual of $G = \text{Gal}(L : K)$ is generated by its cyclic subgroups, so in G there is a collection of subgroups, say H_1, \dots, H_r , such that G/H_i is cyclic for $i = 1, \dots, r$ and $\bigcap_{i=1}^r H_i = \{1\}$. Then L is the composite of the fields L^{H_i} and the extensions $L^{H_i} : K$ are cyclic. Choose for each i a modulus \mathfrak{m}_i for $L^{H_i} : K$. A prime of K that does not ramify in each of the L^{H_i} , does not ramify in L . So the primes not dividing $\mathfrak{m} = \mathfrak{m}_1 \mathfrak{m}_2 \cdots \mathfrak{m}_r$ do not ramify in L . Restriction of automorphisms in G to the subfields L^{H_i} yields an injective group homomorphism

$$G \longrightarrow G/H_1 \times G/H_2 \times \cdots \times G/H_r.$$

For $\mathfrak{a} \in \mathbb{I}^{\mathfrak{m}}(K)$ we have $\varphi_K^{(L^{H_i})}(\mathfrak{a}) = \varphi_K^{(L)}(\mathfrak{a})|_{L^{H_i}}$ by Lemma 13.53. Because $\mathbb{S}_{\mathfrak{m}}(K) \subseteq \mathbb{S}_{\mathfrak{m}_i}(K)$ for all i , the ray $\mathbb{S}_{\mathfrak{m}}(K)$ is in the Artin kernel of each of the extensions $L : L^{H_i}$ and is therefore in the Artin kernel of $L : K$. \square

In chapter 14 we will prove Artin's Reciprocity Law. According to Proposition 13.55 it suffices to prove it for cyclic extensions. A consequence will be that the Artin map induces an isomorphism from $\text{Gal}(L : K)^\vee$ to $\mathcal{H}(L : K)$. Thus to each abelian extension of K there is associated a finite subgroup of $\mathcal{H}(K)$. It will be shown in section 15.3 that every finite subgroup is of the form $\mathcal{H}(K_X : K)$ for a unique abelian extension $K_X : K$. This is the Existence Theorem.

Thus a classification of abelian extensions of a number field K is obtained. Its proof will be completed in chapter 15. For a given number field K we will have a correspondence between abelian number field extensions $L : K$ and finite subgroups of $\mathcal{H}(K)$:

$$\begin{array}{ccc} \text{abelian} & & \text{finite groups of} \\ \text{extensions of } K & \longleftrightarrow & \text{Dirichlet characters of } K \\ \\ L : K & \longmapsto & \mathcal{H}(L : K) \\ \\ K_X : K & \longleftarrow & X \end{array}$$

The maps $L \mapsto \mathcal{H}(L : K)$ and $X \mapsto K_X : K$ are inverses of each other and they preserve the ordering given by inclusion. The field K_X is called the *class field* for X : the prime divisors of the conductor of $\mathcal{H}(L : K)$ are just the ramifying primes and the Artin map $\varphi_K^{(L)}|_{\mathfrak{f}} : \mathbb{I}^{\mathfrak{f}}(K) \rightarrow \text{Gal}(L : K)$ induces an isomorphism $\text{Gal}(L : K)^\vee \xrightarrow{\sim} \mathcal{H}(L : K)$.

Finite subgroups X of $\mathcal{H}(K)$ are contained in $\mathcal{H}_{\mathfrak{m}}(K)$ for some modulus \mathfrak{m} of K and so determine a factor group of the ray class group $\mathcal{C}_{\mathfrak{m}}(K)$. The splitting of a prime of K in K_X is determined by its class in this factor group. It was Weber who introduced at the end of the nineteenth century the term 'class field'.

The classification is both beautiful and deep. Our strategy for its proof is as follows.

1. In section 14.1 we show that for cyclic number field extensions $L : K$ we have $\#(\mathcal{H}(L : K)) = [L : K]$.
2. Though for cyclic extensions $L : K$ the group $\mathcal{H}(L : K)$ has the right order, it still has to be shown that there is a modulus for $L : K$. This is done in section 14.3. As remarked above Artin's Reciprocity Law follows from this in full generality.
3. In section 15.3 the existence of class fields will be proved.

13.56 Examples. A special case of the Classification Theorem: the group $\mathcal{H}_1(K)$ of a number field K corresponds to the maximal nonramified abelian extension of K . This is the so-called *Hilbert class field* of K . Properties of this extension will be studied in section 15.8. The group $\mathcal{H}_1(K)$ is (isomorphic to) the dual of $\mathcal{C}(K)$ and the Artin map induces an isomorphism $\mathcal{C}(K) \xrightarrow{\sim} \text{Gal}(K_{\mathcal{H}_1(K)} : K)$.

- a) The field $\mathbb{Q}(\sqrt{2}, \sqrt{5})$ is the Hilbert class field of $\mathbb{Q}(\sqrt{10})$. Actually, this is a direct consequence of exercise 7 of chapter 7.
- b) The field $\mathbb{Q}(\alpha, \sqrt{-23})$, where $\alpha^3 = \alpha + 1$ is the Hilbert class field of $\mathbb{Q}(\sqrt{-23})$. The extension is unramified (exercise 9 of chapter 7). Exercise 13 of chapter 3 was about the computation of the ideal class group of $\mathbb{Q}(\sqrt{-23})$. The groups $\text{Gal}(\mathbb{Q}(\alpha, \sqrt{-23}) : \mathbb{Q}(\sqrt{-23}))$ and $\mathcal{C}(\mathbb{Q}(\sqrt{-23}))$ are indeed isomorphic. It is far from obvious that the Artin map induces an isomorphism.

EXERCISES

1. Let $K = \mathbb{Q}(\sqrt{-2}, \sqrt{3})$ and let \mathfrak{m} be the modulus (2). An integral basis of K is $(1, \sqrt{-2}, \sqrt{3}, \alpha)$, where $\alpha = \frac{\sqrt{-2} + \sqrt{-6}}{2}$. In Example 5.23 it is shown that $\mathcal{C}(K)$ is a group of order 2 generated by the class of the prime ideal $\mathfrak{p}_2 = (2, \alpha + 1)$ and in Example 5.37 that $\mathcal{O}_K^* = \langle -1, \alpha \rangle$.
 - (i) Compute $K_{\mathfrak{m}}^*/K_{\mathfrak{m}}^1$.
 - (ii) Compute $\mathcal{C}_{\mathfrak{m}}(K)$.
 - (iii) Determine the conductor of $\mathcal{H}_{\mathfrak{m}}(K)$.
2. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and let \mathfrak{m} be the modulus ∞ . An integral basis of K is $(1, \sqrt{2}, \sqrt{3}, \alpha)$, where $\alpha = \frac{\sqrt{2} + \sqrt{6}}{2}$. In Example 5.24 it is shown that the group $\mathcal{C}(K)$ is trivial and in Example 5.38 that $\mathcal{O}_K^* = \langle -1, 1 + \sqrt{2}, \sqrt{2} + \sqrt{3}, \alpha \rangle$.
 - (i) Compute $K_{\mathfrak{m}}^*/K_{\mathfrak{m}}^1$.
 - (ii) Show that $\mathcal{C}_{\mathfrak{m}}(K)$ is of order 2.
 - (iii) Determine the conductor of $\mathcal{H}_{\mathfrak{m}}(K)$.

3. Let K be a cubic number field with one real embedding. Show that $\mathcal{C}_\infty(K) = \mathcal{C}(K)$. What is the conductor of $\mathcal{H}_\infty(K)$?
4. Let $K = \mathbb{Q}(\sqrt[3]{2})$. Then $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{2}]$, a principal ideal domain (Example 5.18). The unit group \mathcal{O}_K^* is generated by -1 and $\sqrt[3]{2} - 1$ (Example 5.42). The prime number 3 totally ramifies in K , say $(3) = \mathfrak{p}^3$.
 - (i) Compute $\mathcal{C}_\mathfrak{m}(K)$ for $\mathfrak{m} = (3)$ and for $\mathfrak{m} = \mathfrak{p}^\infty$.
 - (ii) Determine the conductor of $\mathcal{H}_{(3)}(K)$.
5. Let p be a prime number $\equiv 1 \pmod{4}$. Determine the number of Dirichlet characters of $\mathbb{Q}(i)$ having conductor (p) .
6. Let p be a prime number and \mathfrak{p} the unique prime of $\mathbb{Q}(\zeta_p)$ above p . Prove that $\mathcal{C}_\mathfrak{p}(\mathbb{Q}(\zeta_p)) \cong \mathcal{C}(\mathbb{Q}(\zeta_p))$.
7. Let $L : K$ be a number field extension. In 13.30 a map $\mathcal{M}(K) \rightarrow \mathcal{M}(L)$ is described. Let's denote this map as j_L^K . Then

$$j_L^K(\mathfrak{m}) = j_L^K(\mathfrak{m}_0)j_L^K(\mathfrak{m}_\infty),$$

where the second j_L^K is the map defined in Definition 13.33 (restricted to $\mathbb{I}^+(K)$): $j_L^K(\mathfrak{m}_0) = \mathfrak{m}_0\mathcal{O}_L$ and $j_L^K(\mathfrak{m}_\infty)$ is the product of all infinite primes above the primes in \mathfrak{m}_∞ . Show that the map j_L^K is injective.

8. Let L be an abelian number field and K a subfield of L . Show that there exists a modulus for $L : K$. Prove that $\mathcal{H}(L : K) \cong \mathcal{D}(L)/\mathcal{D}(K)$.
9. Let K be a number field and χ a nontrivial Dirichlet character of K of odd order. Show that the remark on page 339 implies that $L(1, \chi) \neq 0$.
10. Show that $\mathbb{Q}(i, \sqrt{5})$ is the Hilbert class field of $\mathbb{Q}(\sqrt{-5})$. Verify that the Artin map induces an isomorphism $\mathcal{C}(\mathbb{Q}(\sqrt{-5})) \xrightarrow{\sim} \text{Gal}(\mathbb{Q}(i, \sqrt{5}) : \mathbb{Q}(\sqrt{-5}))$.

14 Artin's Reciprocity Law

Let $L : K$ be an abelian number field extension. In section 14.3 we will prove that there exists, in the sense of Definition 13.49, a modulus \mathfrak{m} for $L : K$, which by Theorem 13.51 means that the Artin map $\varphi_K^{(L)}|_{\mathfrak{m}}$ is defined and induces an isomorphism

$$\mathbb{I}^{\mathfrak{m}}(K)/N_K^L(\mathbb{I}^{\mathfrak{m}}(L))\mathbb{S}_{\mathfrak{m}}(K) \xrightarrow{\sim} \text{Gal}(L : K). \quad (14.1)$$

This is Artin's Reciprocity Law. We have already seen that it suffices to show that such a modulus exists for cyclic extensions (Proposition 13.55). We first prove in section 14.1 that for cyclic extensions the two groups in (14.1) are of equal order. For this we use the Galois cohomology computations in section 12.3. As a byproduct we obtain Hasse's Principle for cyclic number field extensions in section 14.2.

In section 14.4 we show that as a consequence of Artin's Reciprocity Law the map

$$\begin{array}{ccc} \text{abelian} & & \text{finite groups of} \\ \text{extensions of } K & \xrightarrow{\quad} & \text{Dirichlet characters of } K \\ L : K & \longmapsto & \mathcal{H}(L : K) \end{array}$$

is injective. In the next chapter we show that it is a bijection.

14.1 The Fundamental Equality

Let $L : K$ be a cyclic Galois extension of number fields of degree n . Put $G = \text{Gal}(L : K) = \langle \sigma \rangle$. We show for a modulus \mathfrak{m} of K which is a multiple of all in L ramifying primes, with the finite ones to a sufficiently high power in \mathfrak{m} , that the group

$$\mathcal{C}_{\mathfrak{m}}(L : K) = \mathbb{I}^{\mathfrak{m}}(K)/N_K^L(\mathbb{I}^{\mathfrak{m}}(L))\mathbb{S}_{\mathfrak{m}}(K).$$

is of order $n = [L : K]$. By the First Fundamental Inequality (Theorem 13.44) we already know that its order is at most n . Note that by Artin's Reciprocity Law, which will be proved in section 14.3, this group is for some modulus \mathfrak{m} isomorphic to the Galois group G and that the isomorphism is induced by the Artin map.

Here we only prove that it has the right order. This is just a step in the proof of Artin's Reciprocity Law.

We start with a modulus \mathfrak{m} of K which is a multiple of all in L ramifying finite primes of K . In the computation we will need extra conditions on \mathfrak{m} .

Let the homomorphism $f: L^* \rightarrow \mathbb{I}^{\mathfrak{m}}(L)$ be the composition of the homomorphism $L^* \rightarrow \mathbb{I}(L)$, $\alpha \mapsto \alpha\mathcal{O}_L$ and the projection $\mathbb{I}(L) \rightarrow \mathbb{I}^{\mathfrak{m}}(L)$. The homomorphism f induces a homomorphism $f_*: H^0(L^*) \rightarrow H^0(\mathbb{I}^{\mathfrak{m}}(L))$. By Theorem 12.17 and Corollary 12.19

$$H^0(L^*) = K^*/N_K^L(L^*) \quad \text{and} \quad H^0(\mathbb{I}^{\mathfrak{m}}(L)) = \mathbb{I}^{\mathfrak{m}}(K)/N_K^L(\mathbb{I}^{\mathfrak{m}}(L)).$$

The group $\mathcal{C}_{\mathfrak{m}}(L : K)$ is a homomorphic image of $\mathbb{I}^{\mathfrak{m}}(K)/N_K^L(\mathbb{I}^{\mathfrak{m}}(L))$, so we have a commutative square

$$\begin{array}{ccc} H^0(L^*) & \longrightarrow & K^*/N_K^L(L^*)K_{\mathfrak{m}}^1 \\ f_* \downarrow & & \downarrow g \\ H^0(\mathbb{I}^{\mathfrak{m}}(L)) & \longrightarrow & \mathcal{C}_{\mathfrak{m}}(L : K) \end{array}$$

in which the vertical maps are induced by f . This square can be completed to the diagram with exact rows and columns on top of the opposite page. The snake lemma and the surjectivity of $K_{\mathfrak{m}}^1 \rightarrow \mathbb{S}_{\mathfrak{m}}(K)$ are used here. From Proposition 13.6 and the first two exact sequences in the proof of Lemma 13.19 follows that the group $K^*/K_{\mathfrak{m}}^1$ is finitely generated. The group $K^*/N_K^L(L^*)$ is a torsion group. So $K^*/N_K^L(L^*)K_{\mathfrak{m}}^1$ is finite: it is a finitely generated torsion group. It follows that $\text{Coker}(f_*)$ is finite and we will see that $\text{Ker}(f_*)$ is finite as well. The diagram then shows that

$$\#(\mathcal{C}_{\mathfrak{m}}(L : K)) = \#(K^*/N_K^L(L^*)K_{\mathfrak{m}}^1) \cdot \frac{\#(\text{Coker}(f_*))}{\#(\text{Ker}(f_*))} \cdot \#(X). \quad (14.2)$$

We will compute the first two factors of the product on the right hand side. The outcome will be that their product is $[L : K]$.

Computation of the order of $K^*/N_K^L(L^*)K_{\mathfrak{m}}^1$

In this computation the modulus \mathfrak{m} of K is an arbitrary one, but at the end it is required that its finite prime divisors occur in \mathfrak{m} with sufficiently high powers.

14.1 Proposition. *The arithmetic projective system $\mathfrak{m} \mapsto K^*/N_K^L(L^*)K_{\mathfrak{m}}^1$ is multiplicative.*

$$\begin{array}{ccccccc}
 & & 1 & & 1 & & 1 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 1 & \longrightarrow & X & \longrightarrow & \text{Ker}(f_*) & \longrightarrow & \text{Ker}(g) \longrightarrow 1 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 1 & \longrightarrow & \frac{K_m^1}{N_K^L(L^*) \cap K_m^1} & \longrightarrow & H^0(L^*) & \longrightarrow & K^*/N_K^L(L^*)K_m^1 \longrightarrow 1 \\
 & & \downarrow & & \downarrow f_* & & \downarrow g \\
 1 & \longrightarrow & \frac{\mathbb{S}_m(K)}{N_K^L(\mathbb{I}^m(L)) \cap \mathbb{S}_m(K)} & \longrightarrow & H^0(\mathbb{I}^m(L)) & \longrightarrow & \mathcal{C}_m^L(L : K) \longrightarrow 1 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & 1 & \longrightarrow & \text{Coker}(f_*) & \xrightarrow{\sim} & \text{Coker}(g) \longrightarrow 1 \\
 & & & & \downarrow & & \downarrow \\
 & & & & 1 & & 1
 \end{array}$$

PROOF. Let \mathfrak{m}_1 and \mathfrak{m}_2 be moduli of K such that $\gcd(\mathfrak{m}_1, \mathfrak{m}_2) = 1$. Then to prove that the map

$$K^*/N_K^L(L^*)K_{\mathfrak{m}_1\mathfrak{m}_2}^1 \longrightarrow K^*/N_K^L(L^*)K_{\mathfrak{m}_1}^1 \times K^*/N_K^L(L^*)K_{\mathfrak{m}_2}^1$$

is an isomorphism. This means that we have to prove

$$N_K^L(L^*)K_{\mathfrak{m}_1}^1 \cap N_K^L(L^*)K_{\mathfrak{m}_2}^1 = N_K^L(L^*)K_{\mathfrak{m}_1\mathfrak{m}_2}^1$$

and

$$N_K^L(L^*)K_{\mathfrak{m}_1}^1 N_K^L(L^*)K_{\mathfrak{m}_2}^1 = K^*.$$

By Lemma 13.19 $K_{\mathfrak{m}_1}^1 K_{\mathfrak{m}_2}^1 = K^*$, from which the last equality follows.

For the proof of the first equality let $\gamma = N_K^L(\alpha_1)b_1 = N_K^L(\alpha_2)b_2$ with $\alpha_1, \alpha_2 \in L^*$, $b_1 \in K_{\mathfrak{m}_1}^1$ and $b_2 \in K_{\mathfrak{m}_2}^1$. From $L_{\mathfrak{m}_1}^1 \cap L_{\mathfrak{m}_2}^1 = L_{\mathfrak{m}_1\mathfrak{m}_2}^1$ and $L_{\mathfrak{m}_1}^1 L_{\mathfrak{m}_2}^1 = L^*$ (Lemma 13.19) follows that $L^*/L_{\mathfrak{m}_1\mathfrak{m}_2}^1 \xrightarrow{\sim} L^*/L_{\mathfrak{m}_1}^1 \times L^*/L_{\mathfrak{m}_2}^1$. So there exists an $\alpha \in L^*$ such that $\alpha \equiv \alpha_1 \pmod{L_{\mathfrak{m}_1}^1}$ and $\alpha \equiv \alpha_2 \pmod{L_{\mathfrak{m}_2}^1}$. Then by Proposition 13.31 $\gamma = N_K^L(\alpha)N_K^L(\alpha^{-1}\alpha_1)b_1 \in N_K^L(\alpha)K_{\mathfrak{m}_1}^1$ and similarly $\gamma \in N_K^L(\alpha)K_{\mathfrak{m}_2}^1$. Hence $\gamma \in N_K^L(\alpha)K_{\mathfrak{m}_1\mathfrak{m}_2}^1$. So

$$N_K^L(L^*)K_{\mathfrak{m}_1}^1 \cap N_K^L(L^*)K_{\mathfrak{m}_2}^1 \subseteq N_K^L(L^*)K_{\mathfrak{m}_1\mathfrak{m}_2}^1.$$

Equality holds because the other inclusion is obvious. \square

So the computation of the order of $K^*/N_K^L(L^*)K_m^1$ comes down to this computation in case the modulus \mathfrak{m} has only one prime divisor. Completion at this prime will be used for this computation. First note that in general global norms are local norms:

14.2 Lemma. *Let $L : K$ be a Galois extension of number fields, \mathfrak{p} a prime of K , \mathfrak{q} a prime of L above \mathfrak{p} and $\alpha \in L$. Then there is a $\beta \in L$ such that $N_{\mathfrak{p}}^{\mathfrak{q}}(\beta) = N_K^L(\alpha)$.*

PROOF. Put $G = \text{Gal}(L : K)$ and $Z = Z_K(\mathfrak{q})$. The restriction of automorphisms in $\text{Gal}(L_{\mathfrak{q}} : K_{\mathfrak{p}})$ to L induces an isomorphism $\text{Gal}(L_{\mathfrak{q}} : K_{\mathfrak{p}}) \xrightarrow{\sim} Z$ (Theorem 10.45). Let R be a system of right representatives of the right cosets of Z in G . Then

$$N_K^L(\alpha) = \prod_{\sigma \in G} \sigma(\alpha) = \prod_{\rho \in R} \prod_{\tau \in Z} \tau \rho(\alpha) = \prod_{\rho \in R} N_{\mathfrak{p}}^{\mathfrak{q}}(\rho(\alpha)) = N_{\mathfrak{p}}^{\mathfrak{q}}\left(\prod_{\rho \in R} \rho(\alpha)\right). \quad \square$$

14.3 Lemma. *Let \mathfrak{p} be a finite prime of K , \mathfrak{q} a prime of L above \mathfrak{p} and $t \in \mathbb{N}^*$. Then the inclusion $K^* \rightarrow K_{\mathfrak{p}}^*$ induces an isomorphism*

$$K^*/N_K^L(L^*)K_{\mathfrak{p}}^1 \xrightarrow{\sim} K_{\mathfrak{p}}^*/N_{\mathfrak{p}}^{\mathfrak{q}}(L_{\mathfrak{q}}^*)(1 + \hat{\mathfrak{p}}^t).$$

PROOF. By Lemma 14.2 we have $N_K^L(L^*) \subseteq N_{\mathfrak{p}}^{\mathfrak{q}}(L_{\mathfrak{q}}^*)$. The induced map is surjective since the map $K^* \rightarrow K_{\mathfrak{p}}^*/(1 + \hat{\mathfrak{p}}^t)$ is surjective. For injectivity we need

$$K^* \cap N_{\mathfrak{p}}^{\mathfrak{q}}(L_{\mathfrak{q}}^*)(1 + \hat{\mathfrak{p}}^t) \subseteq N_K^L(L^*)K_{\mathfrak{p}}^1.$$

Let $\gamma = N_{\mathfrak{p}}^{\mathfrak{q}}(\alpha)\beta$ with $\gamma \in K^*$, $\alpha \in L_{\mathfrak{q}}^*$ and $\beta \in 1 + \hat{\mathfrak{p}}^t$. Since $L_{\mathfrak{q}}^* = L^*(1 + \hat{\mathfrak{q}}^{et})$, where $e = e_{\mathfrak{p}}^{(L)}$, we can assume that $\alpha \in L^*$. Then $\beta \in (1 + \hat{\mathfrak{p}}^t) \cap K^* = K_{\mathfrak{p}}^1$. Put $Z = Z_K(\mathfrak{q})$ and let R be a system of representatives of the right cosets of Z in G . Then $\mathfrak{p}\mathcal{O}_L = \prod_{\rho \in R} \rho(\mathfrak{q})^e$. Take α' such that

$$\alpha' \equiv \begin{cases} \alpha \pmod{L_{\mathfrak{q}}^1}, \\ 1 \pmod{L_{\rho(\mathfrak{q})}^1} \end{cases} \text{ for } \rho \notin Z.$$

Then $\rho^{-1}(\alpha') \equiv 1 \pmod{L_{\mathfrak{q}}^1}$ if $\rho \notin Z$ and so

$$N_K^L(\alpha') = \prod_{\rho \in R} \prod_{\tau \in Z} \tau \rho^{-1}(\alpha') \equiv \prod_{\tau \in Z} \tau(\alpha') = N_{\mathfrak{p}}^{\mathfrak{q}}(\alpha') \equiv N_{\mathfrak{p}}^{\mathfrak{q}}(\alpha) \pmod{L_{\mathfrak{q}}^1}.$$

Thus $N_{\mathfrak{p}}^{\mathfrak{q}}(\alpha) \in N_K^L(L^*)(L_{\mathfrak{q}}^1 \cap K^*) = N_K^L(L^*)K_{\mathfrak{p}}^1$. So $\gamma = N_{\mathfrak{p}}^{\mathfrak{q}}(\alpha)\beta \in N_K^L(L^*)K_{\mathfrak{p}}^1$. \square

14.4 Lemma. *Let \mathfrak{p} be an infinite prime of K and \mathfrak{q} a prime of L above \mathfrak{p} . Then the inclusion $K^* \rightarrow K_{\mathfrak{p}}^*$ induces an isomorphism*

$$K^*/N_K^L(L^*)K_{\mathfrak{p}}^1 \xrightarrow{\sim} K_{\mathfrak{p}}^*/N_{\mathfrak{p}}^{\mathfrak{q}}(L_{\mathfrak{q}}^*).$$

PROOF. The group $K_{\mathfrak{p}}^*/N_{\mathfrak{p}}^{\mathfrak{q}}(L_{\mathfrak{q}}^*)$ is trivial if \mathfrak{p} does not ramify and otherwise it is of order 2. If \mathfrak{p} is complex, then $K_{\mathfrak{p}}^1 = K^*$. So let's assume that \mathfrak{p} is real and corresponds to an embedding $\sigma_{\mathfrak{p}}: K \rightarrow \mathbb{R}$. For $\beta \in L^*$ we have

$$\sigma_{\mathfrak{p}}(N_K^L(\beta)) = \prod_{\tau \in G} \sigma_{\mathfrak{q}\tau}(\beta),$$

where $\sigma_{\mathfrak{q}}$ is a fixed embedding of L in \mathbb{R} or \mathbb{C} above the embedding $\sigma_{\mathfrak{p}}$. If \mathfrak{p} does not ramify, choose $\beta \in L$ such that $\sigma_{\mathfrak{q}\tau}(\beta) < 0$ for exactly one of the embeddings $\sigma_{\mathfrak{q}\tau}: L \rightarrow \mathbb{R}$. Then $N_K^L(\beta) \notin K_{\mathfrak{p}}^1$ and so also the group $K^*/N_K^L(L^*)K_{\mathfrak{p}}^1$ is trivial. If \mathfrak{p} ramifies, then there is a $\tau_0 \in G$ of order 2 such that $\sigma_{\mathfrak{q}\tau_0} = \overline{\sigma_{\mathfrak{q}}}$. In this case $\sigma_{\mathfrak{p}}(N_K^L(\beta))$ is a product of elements $\sigma_{\mathfrak{q}\tau}(\beta) \cdot \sigma_{\mathfrak{q}\tau\tau_0}(\beta) = \sigma_{\mathfrak{q}\tau}(\beta) \cdot \overline{\sigma_{\mathfrak{q}\tau}(\beta)} > 0$ and so $N_K^L(\beta) \in K_{\mathfrak{p}}^1$. \square

14.5 Proposition. *For sufficiently high exponents of the finite primes in the modulus \mathfrak{m} we have*

$$\#(K^*/N_K^L(L^*)K_{\mathfrak{m}}^1) = \prod_{\mathfrak{p}|\mathfrak{m}} e_{\mathfrak{p}}^{(L)} f_{\mathfrak{p}}^{(L)}.$$

PROOF. Let \mathfrak{p} be a finite prime of K and \mathfrak{q} a prime of L above \mathfrak{p} . By Theorem 11.22 $1 + \hat{\mathfrak{p}}^t \subseteq K_{\mathfrak{p}}^{*n}$ for $t > v_{\mathfrak{p}}(n) + \frac{e}{p-1}$, where p is the prime number under \mathfrak{p} and $e = e_{\mathbb{Q}_p}^{(K_{\mathfrak{p}})} = e_{\mathbb{Q}}(\mathfrak{p})$. For such t we have by Lemma 14.3 an isomorphism

$$K^*/N_K^L(L^*)K_{\mathfrak{p}}^{1t} \xrightarrow{\sim} K_{\mathfrak{p}}^*/N_{\mathfrak{p}}^{\mathfrak{q}}(L_{\mathfrak{q}}^*)$$

and by Theorem 12.22 the last group is of order $e_{\mathfrak{p}}^{(L)} f_{\mathfrak{p}}^{(L)}$. So the proposition follows from Proposition 14.1 and Lemma 14.4. \square

It is only in this last proposition we need that \mathfrak{m} is a multiple of a sufficiently high power of each of its finite prime divisors. The exponent t of such a prime \mathfrak{p} has to be such that $1 + \hat{\mathfrak{p}}^t \subseteq N_{\mathfrak{p}}^{\mathfrak{q}}(L_{\mathfrak{q}}^*)$.

Computation of $\frac{\#(\text{Coker}(f_*))}{\#(\text{Ker}(f_*))}$

This computation holds for all moduli \mathfrak{m} . Only at the very end of this computation the modulus \mathfrak{m} is required to be a multiple of all ramifying primes.

Let Q be the set of finite primes of L which do not divide \mathfrak{m} . Then we have the exact sequence of G -modules

$$1 \longrightarrow L_Q^* \longrightarrow L^* \xrightarrow{f} \mathbb{I}^{\mathfrak{m}}(L) \longrightarrow \mathcal{C}\ell(L_Q) \longrightarrow 1.$$

14 Artin's Reciprocity Law

Let Y be the image of $f: L^* \rightarrow \mathbb{I}^m(L)$. The above exact sequence splits into two short exact sequences

$$1 \longrightarrow L_Q^* \longrightarrow L^* \longrightarrow Y \longrightarrow 1$$

and

$$1 \longrightarrow Y \longrightarrow \mathbb{I}^m(L) \longrightarrow \mathcal{C}\ell(L_Q) \longrightarrow 1.$$

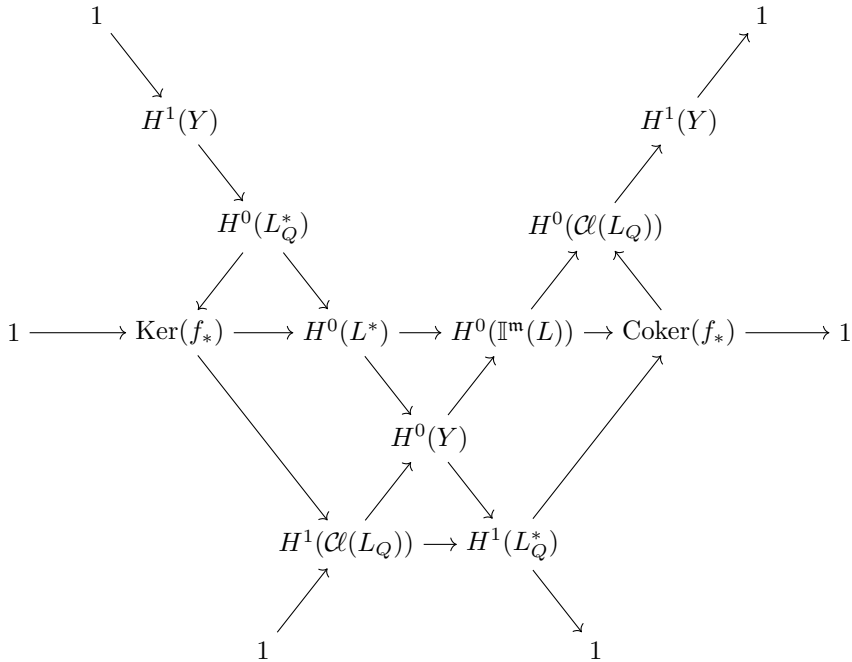
Because $H^1(L^*) = 1$ and $H^1(\mathbb{I}^m(L)) = 1$, the exact hexagons of cohomology groups become exact sequences

$$1 \longrightarrow H^1(Y) \longrightarrow H^0(L_Q^*) \longrightarrow H^0(L^*) \longrightarrow H^0(Y) \longrightarrow H^1(L_Q^*) \longrightarrow 1$$

and

$$1 \longrightarrow H^1(\mathcal{C}\ell(L_Q)) \longrightarrow H^0(Y) \longrightarrow H^0(\mathbb{I}^m(L)) \longrightarrow H^0(\mathcal{C}\ell(L_Q)) \longrightarrow H^1(Y) \longrightarrow 1.$$

These sequences fit in the diagram for the ker-coker exact sequence of $H^0(L^*) \rightarrow H^0(Y) \rightarrow H^0(\mathbb{I}^m(L))$:



Connecting head and tail of the exact sequence from the top left to the top right yields an exact hexagon

$$\begin{array}{ccc}
 & H^1(\mathcal{C}(L_Q)) \rightarrow H^1(L_Q^*) & \\
 & \nearrow & \searrow \\
 \text{Ker}(f_*) & & \text{Coker}(f_*) \\
 & \nwarrow & \swarrow \\
 & H^0(L_Q^*) \leftarrow H^0(\mathcal{C}(L_Q)) &
 \end{array}$$

Since $\mathcal{C}(L_Q)$ is finite, it follows that

$$\frac{\#(\text{Coker}(f_*))}{\#(\text{Ker}(f_*))} = q(L_Q^*). \tag{14.3}$$

As at the end of section 6.3, the ker-coker exact sequence of $L^* \rightarrow \mathbb{I}(L) \rightarrow \mathbb{I}^m(L)$ is:

$$1 \longrightarrow \mathcal{O}_L^* \longrightarrow L_Q^* \longrightarrow \bigoplus_{\mathfrak{q}|\mathfrak{m}_0} \mathbb{Z} \longrightarrow \mathcal{C}(\mathcal{O}_L) \longrightarrow \mathcal{C}(L_Q) \longrightarrow 1.$$

Since $\mathcal{C}(\mathcal{O}_L)$ and $\mathcal{C}(L_Q)$ are finite, we have

$$q(L_Q^*) = q(\mathcal{O}_L^*) \cdot q\left(\bigoplus_{\mathfrak{q}|\mathfrak{m}_0} \mathbb{Z}\right).$$

This leads to a formula for the Herbrand quotient of L_Q^* :

$$q\left(\bigoplus_{\mathfrak{q}|\mathfrak{m}_0} \mathbb{Z}\right) = \prod_{\mathfrak{p}|\mathfrak{m}_0} q\left(\bigoplus_{\mathfrak{q}|\mathfrak{p}\mathcal{O}_L} \mathbb{Z}\right) = \prod_{\mathfrak{p}|\mathfrak{m}_0} \frac{1}{e_{\mathfrak{p}}^{(L)} f_{\mathfrak{p}}^{(L)}}$$

and so by Theorem 12.24

$$q(L_Q^*) = [L : K] \cdot \prod_{\substack{\mathfrak{p}|\mathfrak{m}_0 \\ \text{or } \mathfrak{p} \text{ infinite}}} \frac{1}{e_{\mathfrak{p}}^{(L)} f_{\mathfrak{p}}^{(L)}}.$$

We obtained the following:

14.6 Proposition. *If the modulus \mathfrak{m} is a multiple of all ramifying primes, then*

$$\frac{\#(\text{Coker}(f_*))}{\#(\text{Ker}(f_*))} = [L : K] \cdot \prod_{\mathfrak{p}|\mathfrak{m}} \frac{1}{e_{\mathfrak{p}}^{(L)} f_{\mathfrak{p}}^{(L)}}. \quad \square$$

Conclusion

Let $L : K$ be an abelian number field extension. Choose a modulus \mathfrak{m} of K such that the prime divisors of \mathfrak{m} are the in L ramifying primes and such that the finite ones among these have in \mathfrak{m} a power such that Proposition 14.5 applies. Then by this proposition and Proposition 14.6 the equation (14.2) becomes

$$\#(\mathcal{C}_{\mathfrak{m}}(L : K)) = [L : K] \cdot \#(X).$$

So $\#(\mathcal{C}_{\mathfrak{m}}(L : K)) \geq [L : K]$. Hence we proved:

14.7 Theorem (The Second Fundamental Inequality). *Let $L : K$ be a cyclic Galois extension of number fields and \mathfrak{m} a modulus of K divisible by all in L ramifying primes, the finite ones to a sufficiently high power. Then*

$$\#(\mathcal{C}_{\mathfrak{m}}(L : K)) \geq [L : K]. \quad \square$$

The First Fundamental Inequality (Theorem 13.44) tells us that

$$\#(\mathcal{C}_{\mathfrak{m}}(L : K)) = \#(\mathcal{H}(L : K) \cap \mathcal{H}_{\mathfrak{m}}) \leq \mathcal{H}(L : K) \leq [L : K].$$

So we proved the fundamental equality, which is stated here explicitly because of its importance:

14.8 Theorem (The Fundamental Equality). *Let $L : K$ be a cyclic Galois extension of number fields and \mathfrak{m} a modulus of K divisible by all in L ramifying primes, the finite ones to a sufficiently high power. Then*

$$\#(\mathcal{C}_{\mathfrak{m}}(L : K)) = [L : K]. \quad \square$$

For the \mathfrak{m} in the theorem we have in equation 14.2: $\#(X) = 1$. A consequence is a local-global principle of Hasse as formulated in the next section.

In more modern approaches the first and second inequality are called respectively the second and the first inequality, in accordance with the order the inequalities are proved.

For \mathfrak{m} as in the theorem we have $\mathcal{H}(L : K) \subseteq \mathcal{H}_{\mathfrak{m}}(K)$. In particular $\mathfrak{f}_K(L) \mid \mathfrak{m}$, which implies that the prime divisors of $\mathfrak{f}_K(L)$ ramify in L . In terms of Dirichlet characters we now have:

14.9 Corollary. *Let $L : K$ be a cyclic Galois extension of number fields. Then*

$$\#(\mathcal{H}(L : K)) = [L : K].$$

and the prime divisors of the conductor of $L : K$ ramify in L . □

For a first indication of the strength of this theorem, let $L : K$ be a cyclic unramified number field extension. Then we can take $\mathfrak{m} = (1)$, the trivial modulus, and we obtain

$$\#(\mathbb{I}(K)/N_K^L(\mathbb{I}(L))\mathbb{P}(K)) = [L : K].$$

The group $\mathbb{I}(K)/N_K^L(\mathbb{I}(L))\mathbb{P}(K)$ is a homomorphic image of $\mathbb{I}(K)/\mathbb{P}(K) = \mathcal{C}(K)$. It follows that $[L : K] \mid \#(\mathcal{C}(K))$. So the existence of an abelian unramified extension of K has consequences for the ideal class group of K . Later, when we have the full Classification Theorem, we will see that this works both ways.

14.2 Hasse's Principle

Another consequence of the computation in the previous section is that $X = 1$, which means that the map $K_m^1 \rightarrow \mathbb{S}_m(K)$ induces an isomorphism

$$\frac{K_m^1}{N_K^L(L^*) \cap K_m^1} \xrightarrow{\sim} \frac{\mathbb{S}_m(K)}{N_K^L(\mathbb{I}^m(L)) \cap \mathbb{S}_m(K)}. \tag{14.4}$$

This leads to *Hasse's Principle* for cyclic extensions: an element is a global norm if and only if it is everywhere—i.e. at every prime—a local norm.

14.10 Theorem (Hasse's Principle). *Let $L : K$ be a cyclic extension of number fields and $a \in K^*$. Then*

$$a \in N_K^L(L^*) \iff a \in N_{\mathfrak{p}}^{\mathfrak{q}}(L_{\mathfrak{q}}^*) \text{ for all primes } \mathfrak{p} \text{ of } K,$$

where for each \mathfrak{p} the \mathfrak{q} is a prime of L above \mathfrak{p} .

PROOF. The \Rightarrow -part follows from Lemma 14.2.

Since the map (14.4) is an isomorphism, it follows from the diagram on page 349 that the following square is cartesian:

$$\begin{array}{ccc} H^0(L^*) & \longrightarrow & K^*/N_K^L(L^*)K_m^1 \\ f_* \downarrow & & \downarrow g \\ H^0(\mathbb{I}^m(L)) & \longrightarrow & \mathcal{C}_m(L : K) \end{array}$$

Let $a \in K^*$ be a local norm at a finite prime \mathfrak{p} of K , say $a = N_{\mathfrak{p}}^{\mathfrak{q}}(\beta_{\mathfrak{p}})$, where \mathfrak{q} is a prime of L above \mathfrak{p} and $\beta_{\mathfrak{p}} \in L_{\mathfrak{q}}^*$. Put $f_{\mathfrak{p}} = f_{\mathfrak{p}}^{(L)}$. By definition of the norm for fractional ideals we have

$$v_{\mathfrak{p}}(a) = v_{\mathfrak{p}}(N_{\mathfrak{p}}^{\mathfrak{q}}(\beta_{\mathfrak{p}})) = f_{\mathfrak{p}} \cdot v_{\mathfrak{q}}(\beta_{\mathfrak{p}}).$$

Let P be the collection of finite primes \mathfrak{p} of K with $\mathfrak{p} \nmid \mathfrak{m}_0$. Choose for every prime $\mathfrak{p} \in P$ a prime \mathfrak{q} of L above \mathfrak{p} and let Q be the collection of these primes \mathfrak{q} of L . If $a \in K^*$ is a local norm at all primes in P , then

$$f(a) = \prod_{\mathfrak{p} \in P} \mathfrak{p}^{v_{\mathfrak{p}}(a)} = \prod_{\mathfrak{p} \in P} \mathfrak{p}^{f_{\mathfrak{p}} \cdot v_{\mathfrak{q}}(\beta_{\mathfrak{p}})} = N_K^L \left(\prod_{\mathfrak{q} \in Q} \mathfrak{q}^{v_{\mathfrak{q}}(\beta_{\mathfrak{p}})} \right) \in N_K^L(\mathbb{I}^{\mathfrak{m}}(L)).$$

So the image of $a \cdot N_K^L(L^*)$ under $f_* : H^0(L^*) \rightarrow H^0(\mathbb{I}^{\mathfrak{m}}(L))$ is trivial.

Let a be a local norm at every prime \mathfrak{p} of K . Then in particular a is a local norm at the prime divisors of \mathfrak{m} . Lemma 14.3, Lemma 14.4 and Proposition 14.1 imply that $a \in N_K^L(L^*)K_{\mathfrak{m}}^1$, so also the image of $a \cdot N_K^L(L^*)$ under the horizontal map is trivial. Since the square is cartesian it follows that $a \in N_K^L(L^*)$. \square

Furtwangler proved the principle for cyclic extensions of prime order in 1902. Hasse originally conjectured that this principle holds in general for abelian number field extensions. In 1931 he proved that the principle holds for cyclic extensions in general ([16]). In the same paper he gave a counterexample: $\mathbb{3}$ is not a global norm for the biquadratic extension $\mathbb{Q}(\sqrt{-3}, \sqrt{13}) : \mathbb{Q}$, but is a local norm at every prime of \mathbb{Q} (exercise 3). In 1967 Tate gave, using idèles and cohomology, in [7] another counterexample as an exercise: $\mathbb{Q}(\sqrt{13}, \sqrt{17}) : \mathbb{Q}$. In [21] M. Keune has shown that, using a method similar to Hasse's, for prime numbers p and q with $p, q \equiv 1 \pmod{4}$ and $\left(\frac{p}{q}\right) = 1$ the biquadratic extension $\mathbb{Q}(\sqrt{p}, \sqrt{q}) : \mathbb{Q}$ is a counterexample.

14.3 Artin's Reciprocity Law

In this section we prove the existence of a modulus for any abelian number field extension. The following propositions show that the existence of a modulus for some abelian number field extensions implies the existence of a modulus for various other extensions.

14.11 Proposition. *Let \mathfrak{m} be a modulus for the abelian number field extension $L : K$ and let $K' : K$ be any number field extension. Then \mathfrak{m} is a modulus for $K'L : K'$ as well.*

PROOF. The ray $\mathbb{S}_{\mathfrak{m}}(K)$ is contained in the Artin kernel of $L : K$. By Proposition 13.31 $N_K^{K'}(\mathbb{S}_{\mathfrak{m}}(K')) \subseteq \mathbb{S}_{\mathfrak{m}}(K)$, so for $\mathfrak{a} \in \mathbb{S}_{\mathfrak{m}}(K')$ we have, using Lemma 13.54,

$$\varphi_{K'}^{(K'L)}(\mathfrak{a}) = \varphi_K^{(L)}(N_K^{K'}(\mathfrak{a})) = 1.$$

So the ray $\mathbb{S}_{\mathfrak{m}}(K')$ is in the Artin kernel of $K'L : K'$. \square

14.12 Proposition. *Let \mathfrak{m} be a modulus for the abelian number field extension $L : K$ and let K' be an intermediate field of this extension. Then \mathfrak{m} is a modulus for both $L : K'$ and $K' : K$.*

PROOF. That \mathfrak{m} is a modulus for $L : K'$ follows from Proposition 14.11. Since $\text{Ker}(\varphi_K^{(L)}) \subseteq \text{Ker}(\varphi_K^{(K')})$ the modulus \mathfrak{m} is a modulus for $K' : K$ as well. \square

For cyclotomic extensions there is a modulus:

14.13 Proposition. *Let K be a number field and L an intermediate field of a cyclotomic extension $K(\zeta_m) : K$. Then the modulus $(m)_\infty$ (extended from \mathbb{Q}) is a modulus for $L : K$.*

PROOF. The modulus $(m)_\infty$ is a modulus for $\mathbb{Q}(\zeta_m) : \mathbb{Q}$. The proposition follows from Proposition 14.11 and Proposition 14.12. \square

For the proof of Artin's Reciprocity Law we need a lemma which is a corollary of the following lemma.

14.14 Lemma. *Let $a, n \in \mathbb{N}^*$ and $a \geq 2$. Then infinitely many odd prime numbers l have powers l^m such that $n \mid o(\bar{a})$, where $\bar{a} \in (\mathbb{Z}/l^m)^*$.*

PROOF. First we show that there is a power l^m of a prime number l such that $\bar{a} \in (\mathbb{Z}/l^m)^*$ is of order n .

The n -th cyclotomic polynomial is defined as

$$\Phi_n(X) = \prod_{\substack{0 \leq k < n \\ \gcd(k,n)=1}} (X - \zeta_n^k) \in \mathbb{Z}[X].$$

Because $a \geq 2$ we have $|a - \zeta_n^k| \geq 1$ and there is equality only if $k = 0$ and $a = 2$. For $n \geq 2$ it follows that $|\Phi_n(a)| > 1$. Let l be a prime divisor of $\Phi_n(a)$. Then $\bar{a} \in \mathbb{F}_l^*$ is of order $nl^{-v_l(n)}$. Since $\Phi_n(X) \mid X^n - 1$ in $\mathbb{Z}[X]$, it follows that $l \mid a^n - 1$. Put $m = v_l(a^n - 1)$. Then $o(\bar{a}) \mid n$, where $\bar{a} \in (\mathbb{Z}/l^m)^*$. Because $\text{Ker}((\mathbb{Z}/l^m)^* \rightarrow \mathbb{F}_l^*)$ is an l -group, $o(\bar{a}) = nl^{-k}$ for a k with $0 \leq k \leq v_l(n)$. Suppose $k > 0$. Then $l^m \mid a^{n/l} - 1$ and in particular $a^{n/l} \equiv 1 \pmod{l}$. From

$$a^n - 1 = (a^{n/l} - 1)(a^{n(l-1)/l} + a^{n(l-2)/l} + \dots + a^{n/l} + 1)$$

and $a^{n(l-1)/l} + a^{n(l-2)/l} + \dots + a^{n/l} + 1 \equiv 0 \pmod{l}$ follows that $v_l(a^{n/l} - 1) < m$, contradicting $l^m \mid a^{n/l} - 1$. So $k = 0$, that is $o(\bar{a}) = n$, where $\bar{a} \in (\mathbb{Z}/l^m)^*$.

Apply this construction with n replaced by pm , where p is a prime. Since the prime divisors of $\#((\mathbb{Z}/l^m)^*)$ for all powers of a single prime l are divisors of $l(l-1)$, infinitely many l are obtained when p varies over all primes. Hence $n \mid o(\bar{a})$ for a modulo powers of infinitely many (odd) prime numbers. \square

14.15 Lemma. *Let $L : K$ be a number field extension and \mathfrak{p} a finite prime of K . Then there are powers q of infinitely many odd primes such that*

$$\mathfrak{p} \nmid q\mathcal{O}_K, \quad [L : K] \mid o(\varphi_{\mathfrak{p}}^{(K(\zeta_q))}) \quad \text{and} \quad K(\zeta_q) \cap L = K.$$

PROOF. The number field L has only finitely many subfields. Let K_1, \dots, K_r be the subfields of L which are contained in a cyclotomic field, say $K_i \subseteq \mathbb{Q}(\zeta_{m_i})$. Put $m = m_1 m_2 \cdots m_r$. By Lemma 14.14 there are powers q of infinitely many odd primes such that $\gcd(q, m) = 1$ and the order of $\varphi_{\mathfrak{p}}^{(K(\zeta_q))}$ ($=$ order of $N(\mathfrak{p})$ in $(\mathbb{Z}/q)^*$) is a multiple of $[L : K]$. It remains to prove that $K(\zeta_q) \cap L = K$. The subfields of L contained in a cyclotomic field are all contained in $\mathbb{Q}(\zeta_m)$. So $L \cap \mathbb{Q}(\zeta_q) \subseteq \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_q) = \mathbb{Q}$ and also $K \cap \mathbb{Q}(\zeta_q) = \mathbb{Q}$. By Galois theory

$$\text{Gal}(\mathbb{Q}(\zeta_q) : \mathbb{Q}) \cong \text{Gal}(L(\zeta_q) : L) \cong \text{Gal}(K(\zeta_q) : (L \cap K(\zeta_q)))$$

and

$$\text{Gal}(K(\zeta_q) : K) \cong \text{Gal}(\mathbb{Q}(\zeta_q) : \mathbb{Q}).$$

Hence $L \cap K(\zeta_q) = K$. □

14.16 Theorem (Artin's Reciprocity Law). *Let $L : K$ be an abelian extension of number fields. Then there is a modulus \mathfrak{m} of K having the ramifying primes as its prime divisors, such that the Artin map $\varphi_K^{(L)} : \mathbb{I}^L(K) \rightarrow \text{Gal}(L : K)$ induces an isomorphism*

$$\mathbb{I}^{\mathfrak{m}}(K) / N_K^L(\mathbb{I}^{\mathfrak{m}}(L)) \mathbb{S}_{\mathfrak{m}}(K) \xrightarrow{\sim} \text{Gal}(L : K).$$

PROOF. By Proposition 13.55 we may assume that $L : K$ is cyclic. Let \mathfrak{m} be such that the Fundamental Equality holds for $L : K$:

$$\#(\mathcal{C}_{\mathfrak{m}}(L : K)) = (\mathbb{I}^{\mathfrak{m}}(K) : N_K^L(\mathbb{I}^{\mathfrak{m}}(L)) \mathbb{S}_{\mathfrak{m}}(K)) = [L : K].$$

Choose a generator σ of $\text{Gal}(L : K)$. We will construct an $\mathfrak{a} \in \mathbb{I}^{\mathfrak{m}}(K)$ such that $\varphi_K^{(L)}(\mathfrak{a}) = \sigma$ and for all finite primes $\mathfrak{p} \nmid \mathfrak{m}$ the following property holds:

$$(P) \quad \text{if } \varphi_{\mathfrak{p}}^{(L)} = \sigma^t, \text{ then } \frac{\mathfrak{p}}{\mathfrak{a}^t} \in N_K^L(\mathbb{I}^{\mathfrak{m}}(L)) \mathbb{S}_{\mathfrak{m}}(K).$$

The proof will consist of three parts: the construction of \mathfrak{a} , the proof of property (P) and finally the theorem will be proved using property (P).

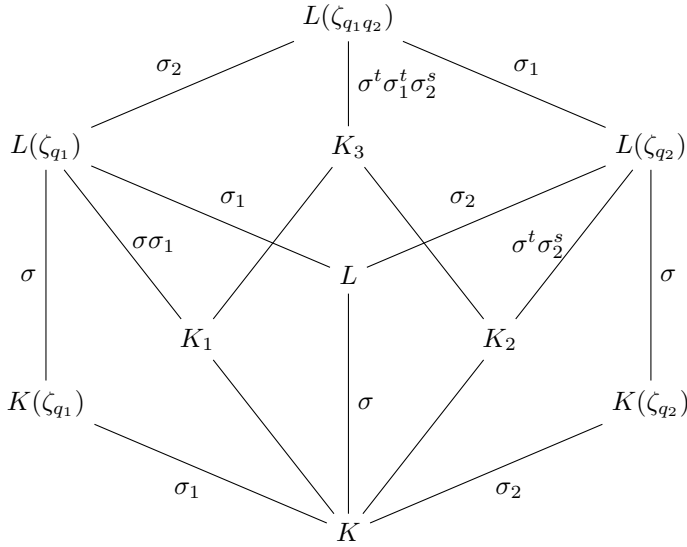
Construction of \mathfrak{a}

By Lemma 14.15 there is an odd prime power q_1 such that

$$\gcd(q_1 \mathcal{O}_K, \mathfrak{m}) = 1, \quad [L : K] \mid [K(\zeta_{q_1}) : K] \quad \text{and} \quad K(\zeta_{q_1}) \cap L = K.$$

(Just take some finite prime \mathfrak{p} of K , choose q_1 such that $\gcd(q_1 \mathcal{O}_K, \mathfrak{m}) = 1$ and note that $\mathfrak{o}(\varphi_{\mathfrak{p}}^{(K(\zeta_{q_1}))}) \mid [K(\zeta_{q_1}) : K]$.) Let $\text{Gal}(L(\zeta_{q_1}) : L)$ be generated by σ_1 . Choose prolongations of σ and σ_1 to $L(\zeta_{q_1})$ such that the restrictions to respectively $K(\zeta_{q_1})$ and L are the identity. Put $K_1 = L(\zeta_{q_1})^{\sigma \sigma_1}$. Choose $\mathfrak{a}_1 \in \mathbb{I}^{q_1 \mathfrak{m}}(K_1)$ such that $\varphi_{K_1}^{(L(\zeta_{q_1}))}(\mathfrak{a}_1) = \sigma \sigma_1$ and take $\mathfrak{a} = N_{K_1}^{K_1}(\mathfrak{a}_1) \in \mathbb{I}^{q_1 \mathfrak{m}}(K)$. Then

$$\varphi_K^{(L(\zeta_{q_1}))}(\mathfrak{a}) = \sigma \sigma_1 \quad \text{and} \quad \varphi_K^{(L)}(\mathfrak{a}) = \varphi_K^{(L(\zeta_{q_1}))}(\mathfrak{a})|_L = \sigma.$$



From

$$\begin{aligned} \text{Gal}(L(\zeta_{q_1}) : K_1(\zeta_{q_1})) &= \text{Gal}(L(\zeta_{q_1}) : K(\zeta_{q_1})) \cap \text{Gal}(L(\zeta_{q_1}) : K_1) \\ &= \langle \sigma \rangle \cap \langle \sigma \sigma_1 \rangle = \{1\} \end{aligned}$$

follows that \$K_1(\zeta_{q_1}) = L(\zeta_{q_1})\$. So the extension \$L(\zeta_{q_1}) : K_1\$ is cyclotomic and therefore \$(q_1)_\infty\$ is a modulus for this extension.

Proof of property (P)

Now let \$\mathfrak{p}\$ be a finite prime of \$K\$ not dividing \$\mathfrak{m}\$. Then \$\varphi_{\mathfrak{p}}^{(L)} = \sigma^t\$ for an integer \$t\$. Again by Lemma 14.15 there exists an odd prime power \$q_2\$ such that

$$\mathfrak{p} \nmid q_2 \mathcal{O}_K, \quad \gcd(q_2 \mathcal{O}_K, \mathfrak{m}) = 1, \quad K(\zeta_{q_2}) \cap L(\zeta_{q_1}) = K \quad \text{and} \quad [L : K] \mid \text{o}(\varphi_{\mathfrak{p}}^{(K(\zeta_{q_2}))}).$$

Fix a generator \$\sigma_2\$ of \$\text{Gal}(L(\zeta_{q_2}) : L)\$ and choose the prolongation of \$\sigma_2\$ to \$L(\zeta_{q_2})\$ which restricts to the identity on \$L\$. Then \$\varphi_{\mathfrak{p}}^{(K(\zeta_{q_2}))} = \sigma_2^s\$ for some integer \$s\$. Because \$\varphi_{\mathfrak{p}}^{(L)} = \sigma^t\$, we have \$\varphi_{\mathfrak{p}}^{(L(\zeta_{q_2}))} = \sigma^t \sigma_2^s\$ and so \$Z_{\mathfrak{p}}^{(L(\zeta_{q_2}))} = \langle \sigma^t \sigma_2^s \rangle\$. Put \$K_2 = L(\zeta_{q_2})^{\sigma^t \sigma_2^s}\$. Again, from

$$\begin{aligned} \text{Gal}(L(\zeta_{q_2}) : K_2(\zeta_{q_2})) &= \text{Gal}(L(\zeta_{q_2}) : K(\zeta_{q_2})) \cap \text{Gal}(L(\zeta_{q_2}) : K_2) \\ &= \langle \sigma \rangle \cap \langle \sigma^t \sigma_1^s \rangle = \{1\} \end{aligned}$$

follows that \$K_2(\zeta_{q_2}) = L(\zeta_{q_2})\$. So \$(q_2)_\infty\$ is a modulus for the extension \$L(\zeta_{q_2}) : K_2\$.

Finally, put $K_3 = L(\zeta_{q_1 q_2})^{\sigma^t \sigma_1^t \sigma_2^s}$. Then $K_3 \supseteq K_1, K_2$. Choose $\mathfrak{b}_3 \in \mathbb{I}^{q_1 q_2 \mathfrak{m}}(K_3)$ such that

$$\varphi_{K_3}^{(L(\zeta_{q_1 q_2}))}(\mathfrak{b}_3) = \sigma^t \sigma_1^t \sigma_2^s.$$

Then for $\mathfrak{b}_1 = N_{K_1}^{K_3}(\mathfrak{b}_3)$ and $\mathfrak{b}_2 = N_{K_2}^{K_3}(\mathfrak{b}_3)$ we have

$$\begin{aligned} \varphi_{K_1}^{(L(\zeta_{q_1}))}(\mathfrak{b}_1) &= \varphi_{K_1}^{(L(\zeta_{q_1 q_2}))}(\mathfrak{b}_1)|_{L(\zeta_{q_1})} = \varphi_{K_3}^{(L(\zeta_{q_1 q_2}))}(\mathfrak{b}_3)|_{L(\zeta_{q_1})} \\ &= \sigma^t \sigma_1^t \sigma_2^s|_{L(\zeta_{q_1})} = \sigma^t \sigma_1^t = \varphi_{K_1}^{(L(\zeta_{q_1}))}(\mathfrak{a}_1^t) \end{aligned}$$

and

$$\begin{aligned} \varphi_{K_2}^{(L(\zeta_{q_2}))}(\mathfrak{b}_2) &= \varphi_{K_2}^{(L(\zeta_{q_1 q_2}))}(\mathfrak{b}_2)|_{L(\zeta_{q_2})} = \varphi_{K_3}^{(L(\zeta_{q_1 q_2}))}(\mathfrak{b}_3)|_{L(\zeta_{q_2})} \\ &= \sigma^t \sigma_1^t \sigma_2^s|_{L(\zeta_{q_2})} = \sigma^t \sigma_2^s = \varphi_{\mathfrak{p}}^{(L(\zeta_{q_2}))} = \varphi_{\mathfrak{p}_2}^{(L(\zeta_{q_2}))}, \end{aligned}$$

where \mathfrak{p}_2 is a prime of K_2 above \mathfrak{p} . Note that \mathfrak{p} splits completely in K_2 . Hence

$$\frac{\mathfrak{b}_1}{\mathfrak{a}_1^t} \in \text{Ker}(\varphi_{K_1}^{(L(\zeta_{q_1}))} : \mathbb{I}^{q_1 \mathfrak{m}}(K_1) \rightarrow \text{Gal}(L(\zeta_{q_1}) : K_1))$$

and so, since $(q_1)\infty$ is a modulus for $L(\zeta_{q_1}) : K_1$

$$\frac{\mathfrak{b}_1}{\mathfrak{a}_1^t} \in N_{K_1}^{L(\zeta_{q_1})}(\mathbb{I}^{q_1 \mathfrak{m}}(L(\zeta_{q_1}))\mathbb{S}_{q_1 \mathfrak{m}}(K_1)) \subseteq N_{K_1}^{L(\zeta_{q_1})}(\mathbb{I}^{\mathfrak{m}}(L(\zeta_{q_1}))\mathbb{S}_{\mathfrak{m}}(K_1)).$$

Similarly

$$\frac{\mathfrak{b}_2}{\mathfrak{p}_2} \in N_{K_2}^{L(\zeta_{q_2})}(\mathbb{I}^{\mathfrak{m}}(L(\zeta_{q_2}))\mathbb{S}_{\mathfrak{m}}(K_2)).$$

Apply $N_K^{K_1}$ and $N_K^{K_2}$:

$$\frac{\mathfrak{b}}{\mathfrak{a}^t}, \frac{\mathfrak{b}}{\mathfrak{p}} \in N_K^L(\mathbb{I}^{\mathfrak{m}}(L))\mathbb{S}_{\mathfrak{m}}(K)$$

and hence also

$$\frac{\mathfrak{p}}{\mathfrak{a}^t} \in N_K^L(\mathbb{I}^{\mathfrak{m}}(L))\mathbb{S}_{\mathfrak{m}}(K).$$

The theorem follows from Property (P)

Let $\mathfrak{c} \in \mathbb{I}^{\mathfrak{m}}(K)$ such that \mathfrak{c} is in the Artin kernel: $\varphi_K^{(L)}(\mathfrak{c}) = 1$. For each finite prime $\mathfrak{p} \nmid \mathfrak{m}$ of K write $\varphi_{\mathfrak{p}}^{(L)} = \sigma^{t_{\mathfrak{p}}}$. Thus for each \mathfrak{p} we have $\frac{\mathfrak{p}}{\mathfrak{a}^{t_{\mathfrak{p}}}} \in N_K^L(\mathbb{I}^{\mathfrak{m}}(L))\mathbb{S}_{\mathfrak{m}}(K)$. Then

$$\varphi_K^{(L)}(\mathfrak{c}) = \prod_{\mathfrak{p}} (\varphi_{\mathfrak{p}}^{(L)})^{v_{\mathfrak{p}}(\mathfrak{c})} = \prod_{\mathfrak{p}} \sigma^{t_{\mathfrak{p}} v_{\mathfrak{p}}(\mathfrak{c})} = \sigma^u,$$

where $u = \sum t_p v_p(\mathfrak{c})$. Because \mathfrak{c} is in the Artin kernel and $\mathfrak{o}(\sigma) = [L : K]$, this implies that $[L : K] \mid u$. Now

$$\frac{\mathfrak{c}}{\mathfrak{a}^u} = \prod_p \left(\frac{\mathfrak{p}}{\mathfrak{a}^{t_p}} \right)^{v_p(\mathfrak{c})} \in N_K^L(\mathbb{I}^{\mathfrak{m}}(L))\mathbb{S}_{\mathfrak{m}}(K)$$

and because $[L : K] \mid u$ we have $\mathfrak{a}^u \in N_K^L(\mathbb{I}^{\mathfrak{m}}(L))$. Hence $\mathfrak{c} \in N_K^L(\mathbb{I}^{\mathfrak{m}}(L))\mathbb{S}_{\mathfrak{m}}(K)$. Therefore, the Artin kernel is contained in $N_K^L(\mathbb{I}^{\mathfrak{m}}(L))\mathbb{S}_{\mathfrak{m}}(K)$. Finally, since both have index $[L : K]$ in $\mathbb{I}^{\mathfrak{m}}(K)$, they coincide. \square

In particular, the trivial modulus (1) of a number field K is a modulus for any unramified abelian extension $L : K$ and the Artin map induces an isomorphism

$$\mathbb{I}(K)/N_K^L(\mathbb{I}(L))\mathbb{P}(K) \xrightarrow{\sim} G.$$

In other words, it induces a surjective homomorphism $\mathcal{C}(K) \rightarrow G$ and the kernel of this homomorphism is $\text{tr}_K^L(\mathcal{C}(L))$.

14.17 Application. In Application 9.42 it was shown that for each finite abelian group G there exists an extension $L : K$ of abelian number fields such that $\text{Gal}(L : K) \cong G$ and no prime ideal of K ramifies in L . With a small adaptation of the proof one can realize that the infinite primes do not ramify either:

Choose for $i = 1, \dots, r$ the prime numbers p_i in the proof such that $p_i \equiv 1 \pmod{2n_i}$. Then the Dirichlet characters χ_i are even. Choose χ_{r+1} to be an odd character. Then $\chi = \chi_1 \cdots \chi_{r+1}$ is odd and as a result the field K is complex.

So for any abelian G there exists an unramified extension with $\text{Gal}(L : K) \cong G$. By Artin's Reciprocity Theorem we have a surjective homomorphism $\mathcal{C}(K) \rightarrow G$. So for any abelian G there exists a number field K such that G is a homomorphic image of its ideal class group, or, what amounts to the same, the ideal class group contains a subgroup isomorphic to G . It is unknown whether any abelian G is realizable as an ideal class group of some number field.

14.4 The dual Artin isomorphism and class fields

An abelian extension of a number field determines a finite group of Dirichlet characters of the base field. We will show that each finite group of Dirichlet characters is the group of Dirichlet characters of at most one abelian extension.

Let $L : K$ be an abelian number field extension. By Artin's Reciprocity Law the Artin map $\varphi_K^{(L)} : \mathbb{I}^L(K) \rightarrow \text{Gal}(L : K)$ induces an isomorphism $\mathcal{C}_{\mathfrak{m}}(L : K) \xrightarrow{\sim} \text{Gal}(L : K)$ for some modulus \mathfrak{m} of K having the ramifying primes as its prime divisors. Dual to this isomorphism is an isomorphism $\text{Gal}(L : K)^\vee \xrightarrow{\sim} \mathcal{H}(L : K)$.

14.18 Definition and notation. Let $L : K$ be an abelian number field extension. Then the *dual Artin isomorphism* of $L : K$ is the isomorphism

$$\check{\varphi}_K^{(L)} : \text{Gal}(L : K)^\vee \xrightarrow{\sim} \mathcal{H}(L : K)$$

defined by $\check{\varphi}_K^{(L)}(\xi)(\mathfrak{a}) = \xi(\varphi_K^{(L)}(\mathfrak{a}))$ for all $\xi \in \text{Gal}(L : K)^\vee$ and all $\mathfrak{a} \in \mathbb{I}^L(K) \cap \mathbb{I}^+(K)$.

By Lemma 13.29 the values of a Dirichlet character on all prime ideals but a finite number of them determine the Dirichlet character. So $\check{\varphi}_K^{(L)}$ is determined by $\check{\varphi}_K^{(L)}(\xi)(\mathfrak{p}) = \xi(\varphi_{\mathfrak{p}}^{(L)})$ for all $\xi \in \text{Gal}(L : K)^\vee$ and all nonramifying $\mathfrak{p} \in \text{Max}(\mathcal{O}_K)$.

14.19 Proposition. Let $L_1 : K$ and $L_2 : K$ be abelian number field extensions such that $L_1 \subseteq L_2$. Let $p : \text{Gal}(L_2 : K) \rightarrow \text{Gal}(L_1 : K)$ be induced by restriction of automorphisms to L_1 . Then the following square commutes

$$\begin{array}{ccc} \text{Gal}(L_2 : K)^\vee & \xrightarrow[\sim]{\check{\varphi}_K^{(L_2)}} & \mathcal{H}(L_2 : K) \\ p^\vee \uparrow & & \uparrow \subseteq \\ \text{Gal}(L_1 : K)^\vee & \xrightarrow[\sim]{\check{\varphi}_K^{(L_1)}} & \mathcal{H}(L_1 : K) \end{array}$$

PROOF. Let $\xi \in \text{Gal}(L_1 : K)^\vee$ and $\mathfrak{p} \in \text{Max}(\mathcal{O}_K)$ not ramifying in L_2 . Then

$$\check{\varphi}_K^{(L_2)} p^\vee(\xi)(\mathfrak{p}) = \check{\varphi}_K^{(L_2)}(\xi p)(\mathfrak{p}) = \xi p(\varphi_{\mathfrak{p}}^{(L_2)}) = \xi(\varphi_{\mathfrak{p}}^{(L_1)}) = \check{\varphi}_K^{(L_1)}(\xi)(\mathfrak{p}).$$

Hence $\check{\varphi}_K^{(L_2)} p^\vee = \check{\varphi}_K^{(L_1)}$. Note that $\mathcal{H}(L_1 : K) \subseteq \mathcal{H}(L_2 : K)$ by Lemma 13.35. \square

14.20 Corollary. Let $L_1 : K$ and $L_2 : K$ be abelian number field extensions. Then

$$\mathcal{H}(L_1 \cap L_2 : K) = \mathcal{H}(L_1 : K) \cap \mathcal{H}(L_2 : K)$$

and

$$\mathcal{H}(L_1 L_2 : K) = \mathcal{H}(L_1 : K) \mathcal{H}(L_2 : K).$$

PROOF. By Galois theory the square

$$\begin{array}{ccc} \text{Gal}(L_1 L_2 : K) & \xrightarrow{p} & \text{Gal}(L_2 : K) \\ p \downarrow & & \downarrow p \\ \text{Gal}(L_1 : K) & \xrightarrow{p} & \text{Gal}((L_1 \cap L_2) : K) \end{array}$$

of surjective homomorphisms is bicartesian. By Proposition 14.19 the following square of inclusions is bicartesian as well.

$$\begin{array}{ccc}
 \mathcal{H}(L_1 \cap L_2 : K) & \xrightarrow{\subseteq} & \mathcal{H}(L_2 : K) \\
 \subseteq \downarrow & & \downarrow \subseteq \\
 \mathcal{H}(L_1 : K) & \xrightarrow{\subseteq} & \mathcal{H}(L_1 L_2 : K)
 \end{array} \quad \square$$

14.21 Definition. Let K be a number field and X a finite group of Dirichlet characters of K . If $L : K$ is an abelian number field extension such that $\mathcal{H}(L : K) = X$, then L is called a *class field* for X .

Class fields are unique. This is a consequence of:

14.22 Proposition. Let $L_1 : K$ and $L_2 : K$ be abelian number field extensions.

$$L_1 \subseteq L_2 \iff \mathcal{H}(L_1 : K) \subseteq \mathcal{H}(L_2 : K).$$

PROOF.

\Rightarrow : This is Lemma 13.35.

\Leftarrow : If $\mathcal{H}(L_1 : K) \subseteq \mathcal{H}(L_2 : K)$, then by Corollary 14.20 $\mathcal{H}(L_1 L_2 : K) = \mathcal{H}(L_2 : K)$. This implies $[L_1 L_2 : K] = [L_2 : K]$ and since $L_2 \subseteq L_1 L_2$, we have $L_2 = L_1 L_2$, that is $L_1 \subseteq L_2$. \square

For an abelian extension of number fields we now have a correspondence between intermediate fields and groups of Dirichlet characters of the extension.

14.23 Corollary. Let $L : K$ be an abelian number field extension. Then the map $L' \mapsto \mathcal{H}(L' : K)$ is an inclusion preserving bijection from the set of intermediate fields of $L : K$ to the set of subgroups of $\mathcal{H}(L : K)$.

PROOF. The dual Artin map $\check{\varphi}_K^{(L)}$ is an isomorphism and induces an inclusion preserving bijection from the set of subgroups of $\text{Gal}(L : K)^\vee$ to the set of subgroups of $\mathcal{H}(L : K)$. \square

In section 9.1 an elaborate but relatively elementary proof was given of the theorem of Kronecker and Weber. The proof involved a detailed study of various ramification groups. The following proof illustrates the strength of class field theory.

14.24 Theorem (Kronecker-Weber). *Let K be an abelian number field. Then K is a subfield of a cyclotomic field.*

PROOF. The conductor $f_{\mathbb{Q}}(K)$ is either of the form (m) or $(m)_{\infty}$ for some $m \in \mathbb{N}^*$. So for such m we have $\mathcal{H}(K : \mathbb{Q}) \subseteq \mathcal{H}_{(m)_{\infty}}(\mathbb{Q}) = \mathcal{H}(\mathbb{Q}(\zeta_m) : \mathbb{Q})$. Hence $K \subseteq \mathbb{Q}(\zeta_m)$. \square

The Translation Theorem describes the behavior of the group of Dirichlet characters of an abelian extension under a change of the base field. It is based on Lemma 13.54. In the notation of this lemma, we have a commutative square

$$\begin{array}{ccc} \mathbb{I}^m(K') & \xrightarrow{\varphi_{K'}^{(LK')}} & \text{Gal}(LK' : K') \\ \downarrow N_K^{K'} & & \downarrow i \\ \mathbb{I}^m(K) & \xrightarrow{\varphi_K^{(L)}} & \text{Gal}(L : K) \end{array}$$

where i is the restriction of automorphisms to L . Divide by the Artin kernels:

$$\begin{array}{ccc} \mathcal{C}_m(LK' : K') & \xrightarrow[\sim]{\varphi_{K'}^{(LK')}} & \text{Gal}(LK' : K') \\ \downarrow N_K^{K'} & & \downarrow i \\ \mathcal{C}_m(L : K) & \xrightarrow[\sim]{\varphi_K^{(L)}} & \text{Gal}(L : K) \end{array}$$

Dually,

$$\begin{array}{ccc} \text{Gal}(L : K)^{\vee} & \xrightarrow[\sim]{\check{\varphi}_K^{(L)}} & \mathcal{H}(L : K) \\ \downarrow i^{\vee} & & \downarrow \nu_{K'}^K \\ \text{Gal}(K'L : K')^{\vee} & \xrightarrow[\sim]{\check{\varphi}_{K'}^{(K'L)}} & \mathcal{H}(K'L : K') \end{array}$$

and this proves the following theorem.

14.25 Translation Theorem. Let $K' : K$ be a number field extension and $L : K$ an abelian number field extension. Then

$$\mathcal{H}(K'L : K') = \nu_{K'}^K(\mathcal{H}(L : K)).$$

In particular, if K' is an intermediate field of $L : K$, then

$$\mathcal{H}(L : K') = \nu_{K'}^K(\mathcal{H}(L : K)). \quad \square$$

EXERCISES

- Show that the proof of formula (14.3) simplifies if we assume that \mathfrak{m} is such that $L_{\mathfrak{Q}}$ is a principal ideal domain.
- Let m be a squarefree integer $\neq 1$.
 - Show that there exists an $\alpha \in \mathbb{Q}(\sqrt{m})$ such that $\mathbb{Q}(\sqrt{m}, \sqrt{\alpha}) : \mathbb{Q}$ is not a Galois extension.
 - Show that there exists an abelian extension $L : \mathbb{Q}(\sqrt{m})$ which is not contained in a cyclotomic extension of $\mathbb{Q}(\sqrt{m})$.
- ([16]) Let $L = \mathbb{Q}(\sqrt{-3}, \sqrt{13})$ and $K = \mathbb{Q}(\sqrt{-39})$. Let $\text{Gal}(L : \mathbb{Q}) = \langle \sigma, \tau \rangle$ with σ and τ such that $\sigma(\sqrt{-3}) = \sqrt{-3}$ and $\tau(\sqrt{-39}) = \sqrt{-39}$.
 - Show that 3 is a local norm of $L : \mathbb{Q}$ at every prime of \mathbb{Q} .
 - Show that $L : K$ is unramified.
 - Let $\mathfrak{p}_2 = (2, \frac{1+\sqrt{-39}}{2})$. Prove that \mathcal{O}_K is cyclic of order 4 and that this group is generated by the class of \mathfrak{p}_2 .
 - Let $\alpha = \frac{3-\sqrt{-39}}{4}$. Prove that 3 is a norm of $L : \mathbb{Q}$ if and only if there exists a $\beta \in K^*$ such that $\frac{\alpha\beta}{\sigma(\beta)}$ is a norm of $L : K$.
 - Let $\beta \in K^*$ and \mathfrak{p}_3 the unique prime of K above 3. Show that

$$\frac{\alpha\beta}{\sigma(\beta)} \mathcal{O}_K = \frac{\mathfrak{p}_3 \cdot \beta \mathfrak{p}_2}{\sigma(\beta \mathfrak{p}_2)}.$$

- Show that for $\mathfrak{p} \in \text{Max}(\mathcal{O}_K)$ the ideal class of $\frac{\mathfrak{p}}{\sigma(\mathfrak{p})}$ is of order ≤ 2 . It is of order 2 if and only if the class of \mathfrak{p} is of order 4.
- Prove that there is a $\mathfrak{p} \in \text{Max}(\mathcal{O}_K)$ such that the class of \mathfrak{p} is of order 4 and

$$v_{\mathfrak{p}}\left(\frac{\alpha\beta}{\sigma(\beta)}\right) \text{ is odd.}$$

- Conclude that 3 is not a norm of $L : \mathbb{Q}$.

- Let p be an odd prime number and q an odd prime divisor of $p-1$. Let $K = \mathbb{Q}(\sqrt[q]{p})$ and L the subfield of $\mathbb{Q}(\zeta_p)$ of degree q over \mathbb{Q} .
 - Show that p totally ramifies both in K and L .

14 Artin's Reciprocity Law

- (ii) Let \mathfrak{p} be a prime ideal of KL above p and let \mathfrak{p}' and \mathfrak{p}'' be the primes under \mathfrak{p} of respectively K and L . Show that both $K_{\mathfrak{p}'} : \mathbb{Q}_p$ and $L_{\mathfrak{p}''} : \mathbb{Q}_p$ are Galois extensions.
 - (iii) Show that there is an $\alpha \in L_{\mathfrak{p}''}^*$ such that $\overline{L_{\mathfrak{p}''}} = \mathbb{Q}_p(\alpha)$ and $\alpha^q \in \mathbb{Q}_p$.
 - (iv) Show that p does not totally ramify in KL .
 - (v) Prove that $KL : K$ is an unramified Galois extension. Conclude that $\mathcal{C}(K)$ contains an element of order q .
5. ([23], Theorem 1) Let $L : K$ be an unramified cyclic extension of number fields. Set $G = \text{Gal}(L : K)$.
- (i) Prove that the homomorphism $L^* \rightarrow \mathbb{P}(L)$, $\alpha \mapsto \alpha \mathcal{O}_L$ of G -modules induces an injective homomorphism $H^0(L^*) \rightarrow H^0(\mathbb{P}(L))$. (Hint: Hasse's Principle)
 - (ii) Prove that $H^0(\mathcal{O}_L^*) \cong H^1(\mathbb{P}(L))$.
 - (iii) Show that the inclusion $\mathbb{P}(L) \rightarrow \mathbb{I}(L)$ induces a short exact sequence

$$1 \longrightarrow \mathbb{I}(L)^G / \mathbb{P}(L)^G \longrightarrow \mathcal{C}(L)^G \longrightarrow H^1(\mathbb{P}(L)) \longrightarrow 1.$$

- (iv) Show that

$$(\mathbb{I}(L)^G : \mathbb{P}(L)^G) = \frac{\#(\mathcal{C}(K))}{(\mathbb{P}(L)^G : \mathbb{P}(K))}$$

and

$$\#(\mathcal{C}(L)^G) = \frac{\#(\mathcal{C}(K))}{(\mathbb{P}(L)^G : \mathbb{P}(K))} \cdot \#(H^0(\mathcal{O}_L^*)).$$

- (v) Show that the inclusion $\mathcal{O}_L^* \rightarrow L^*$ induces a short exact sequence

$$1 \longrightarrow \mathbb{P}(K) \longrightarrow \mathbb{P}(L)^G \rightarrow H^1(\mathcal{O}_L^*) \longrightarrow 1.$$

- (vi) Prove that

$$\#(\mathcal{C}(L)^G) = \frac{\#(\mathcal{C}(K))}{[L : K]}.$$

- (vii) Let $L : K$ be an unramified cyclic extension of number fields. Show that the order of the kernel of $j_L^K : \mathcal{C}(K) \rightarrow \mathcal{C}(L)$ is at least $[L : K]$.

For $[L : K]$ a prime number the final result in the last exercise is known as Hilbert's Theorem 94. It is Satz 94 in [18], also known as Hilbert's Zahlbericht. Translation: [19].

15 The Classification Theorem

The Classification Theorem relates finite groups of Dirichlet characters of a number field to abelian extensions of this number field. What is so far still missing is the existence of an abelian extension corresponding to a given group of Dirichlet characters. This existence problem will be reduced in section 15.1 to the case in which the base field contains sufficiently many roots of unity. Then the extension looked for is a Kummer extension. Kummer extensions are treated in general in section 15.2. The full Classification Theorem is proved in section 15.3. A direct consequence is Chebotarev's Density Theorem for Galois extensions of number fields (section 15.4). Dirichlet characters describe the splitting behavior of primes in an abelian extension of number fields. In the sections 15.5 and 15.6 this description is completed with the Complete Splitting Theorem and a description of the conductor.

In section 15.6 an isomorphism $\vartheta_{\mathfrak{p}}^{(L)}: K_{\mathfrak{p}}/N_{\mathfrak{p}}^q(L_{\mathfrak{q}}^*) \xrightarrow{\sim} \text{Gal}(L_{\mathfrak{q}}: K_{\mathfrak{p}})$, the *local Artin map* for the completion of an abelian number field extension $L: K$, is constructed. The so-called *Hilbert symbols* are based on this map. These symbols are treated in the next chapter. In this chapter the local Artin map is used for a description of the conductor of abelian number field extensions.

In section 15.8 we have a look at the special case of unramified abelian extensions of a number field. The maximal one among these is known as the Hilbert class field. An important property of Hilbert class fields is the Principal Ideal Theorem: ideals in the base field become principal in the Hilbert class field. Using a generalization of Artin maps to Galois extensions of number fields in general, not just the abelian ones, as described in section 15.7, the Principal Ideal Theorem is reduced to pure group theory. The proof is in the last section.

15.1 Reduction steps

In this section reduction steps toward the Existence Theorem (Theorem 15.27) are made. We have to show that for any finite group X of Dirichlet characters of a number field K there exists a class field. Here is an outline of the proof:

1. First we note that if for a group $X' \geq X$ a class field exists, then so there exists one for X . This is Proposition 15.1.

2. Next it is shown that, if there is a class field for the group $\nu_{K'}^K(X)$ of Dirichlet characters of K' , where $K' : K$ is abelian, then there is one for X as well. This is Theorem 15.7. The result of step 1 is used here.
3. We will show that, if K contains μ_n , then there is a modulus \mathfrak{m} of K such that the group ${}_n\mathcal{H}_{\mathfrak{m}}(K)$ has a class field.¹ This is Theorem 15.26. The required extension is an n -Kummer extension. As explained in section 15.2 such extensions of K are classified by subgroups of K^* containing the subgroup K^{*n} of n -th powers as a subgroup of finite index.
4. By the result of step 2 we may assume that the field contains μ_n , where n is an exponent for the group X . Finally, by the steps 1 and 3, it suffices to choose the modulus \mathfrak{m} such that also $X \leq {}_n\mathcal{H}_{\mathfrak{m}}(K)$.

The first reduction step:

15.1 Proposition. *Let K be a number field and let X_1 and X_2 be finite groups of Dirichlet characters of K such that $X_1 \subseteq X_2$. If there is a class field for X_2 , then there is a class field for X_1 as well.*

PROOF. This is just a reformulation of Corollary 14.23. □

The Classification Theorem describes a correspondence between abelian extensions of a number field K and finite subgroups of $\mathcal{H}(K)$. This proposition is the part of the theorem that describes the correspondence between subextensions of a given abelian extension $L : K$ and subgroups of $\mathcal{H}(L : K)$.

15.2 Lemma. *Let $L : K$ be a number field extension and $\sigma : L \rightarrow \mathbb{C}$ an embedding. Then the following squares commute.*

$$\begin{array}{ccc}
 \mathbb{I}(L) & \xrightarrow{N_K^L} & \mathbb{I}(K) & & \mathcal{H}(\sigma(K)) & \xrightarrow{\nu_{\sigma(L)}^{\sigma(K)}} & \mathcal{H}(\sigma(L)) \\
 \sim \downarrow \sigma_* & & \sim \downarrow \sigma_* & & \sim \downarrow \sigma^* & & \sim \downarrow \sigma^* \\
 \mathbb{I}(\sigma(L)) & \xrightarrow{N_{\sigma(K)}^{\sigma(L)}} & \mathbb{I}(\sigma(K)) & & \mathcal{H}(K) & \xrightarrow{\nu_L^K} & \mathcal{H}(L)
 \end{array}$$

PROOF. For the commutativity of the first square it suffices to show that the maps $N_{\sigma(K)}^{\sigma(L)}\sigma_*$ and $\sigma_*N_K^L$ agree on finite primes of L . Let $\mathfrak{q} \in \text{Max}(\mathcal{O}_L)$ and $\mathfrak{p} = \mathfrak{q} \cap K$. Put $f = f_{\mathfrak{p}}^{(L)}$. Then $\sigma(\mathfrak{q}) \in \text{Max}(\mathcal{O}_{\sigma(L)})$ and $\sigma(\mathfrak{q}) \cap \sigma(K) = \sigma(\mathfrak{p})$. Therefore,

$$(N_{\sigma(K)}^{\sigma(L)}\sigma_*)(\mathfrak{q}) = N_{\sigma(K)}^{\sigma(L)}\sigma(\mathfrak{q}) = \sigma(\mathfrak{p})^f = \sigma(\mathfrak{p}^f) = \sigma(N_K^L(\mathfrak{q})) = (\sigma_*N_K^L)(\mathfrak{q}).$$

¹Notation: For $n \in \mathbb{N}^*$ and A a (multiplicative) group ${}_nA$ is the subgroup of $a \in A$ with $a^n = 1$.

The commutativity of the second square follows from the commutativity of the first. Let $\xi \in \mathcal{H}(\sigma(K))$. Then $(\nu_L^K \sigma^*)(\xi) = \nu_L^K(\xi \sigma_*)$ and $\sigma^* \nu_{\sigma(L)}^{\sigma(K)}(\xi) = \nu_{\sigma(L)}^{\sigma(K)}(\xi) \sigma_*$. If \mathfrak{m} is the conductor of ξ , then the Dirichlet characters $\nu_L^K(\xi \sigma_*)$ and $\nu_{\sigma(L)}^{\sigma(K)}(\xi) \sigma_*$ coincide on $\mathbb{I}^{\sigma^{-1}(\mathfrak{m})}(K)$ and so, by Lemma 13.29, they are equal. \square

15.3 Corollary. *Let $L : K$ be a number field extension. Then an embedding $\sigma : L \xrightarrow{\sim} \sigma(L) \subset \mathbb{C}$ induces an isomorphism*

$$\sigma^* : \mathcal{H}(\sigma(L) : \sigma(K)) \xrightarrow{\sim} \mathcal{H}(L : K), \quad \xi \mapsto \xi \sigma_*. \quad \square$$

15.4 Notation. Let $L : K$ be a Galois extension of number fields, $\sigma : L \rightarrow \mathbb{C}$ an embedding and $\tau \in \text{Gal}(L : K)$. Then we have a group isomorphism

$$f_\sigma : \text{Gal}(L : K) \xrightarrow{\sim} \text{Gal}(\sigma(L) : \sigma(K)), \quad \tau \mapsto \sigma \tau \sigma^{-1}.$$

15.5 Lemma. *Let $L : K$ be an abelian number field extension, $\sigma : L \rightarrow \mathbb{C}$ an embedding and \mathfrak{m} a modulus for $L : K$. Then the following squares of isomorphisms commute.*

$$\begin{array}{ccc} \mathcal{C}_{\mathfrak{m}}(L : K) & \xrightarrow[\sim]{\varphi_K^{(L)}} & \text{Gal}(L : K) \\ \sim \downarrow \sigma_* & & \sim \downarrow f_\sigma \\ \mathcal{C}_{\sigma(\mathfrak{m})}(\sigma(L) : \sigma(K)) & \xrightarrow[\sim]{\varphi_{\sigma(K)}^{(\sigma(L))}} & \text{Gal}(\sigma(L) : \sigma(K)) \\ \\ \text{Gal}(\sigma(L) : \sigma(K))^\vee & \xrightarrow[\sim]{\check{\varphi}_{\sigma(K)}^{(\sigma(L))}} & \mathcal{H}(\sigma(L) : \sigma(K)) \\ \sim \downarrow f_\sigma^\vee & & \sim \downarrow \sigma^* \\ \text{Gal}(L : K)^\vee & \xrightarrow[\sim]{\check{\varphi}_K^{(L)}} & \mathcal{H}(L : K) \end{array}$$

PROOF. Let $\mathfrak{a} \in \mathbb{I}^{\mathfrak{m}}(L)$. Then

$$f_\sigma \varphi_K^{(L)}(\mathfrak{a}) = \sigma \varphi_K^{(L)}(\mathfrak{a}) \sigma^{-1} = \varphi_{\sigma(K)}^{(\sigma(L))}(\sigma(\mathfrak{a})).$$

The commutativity of the second square follows from the commutativity of the first. \square

15.6 Proposition. *Let $K : K_0$ be a Galois extension of number fields and $L : K$ an abelian number field extension. Then $L : K_0$ is a Galois extension if and only if $\tau^*(\mathcal{H}(L : K)) = \mathcal{H}(L : K)$ for all $\tau \in \text{Gal}(K : K_0)$.*

If $L : K_0$ is a Galois extension, then the action of $\text{Gal}(K : K_0)$ on $\mathcal{H}(L : K)$ is compatible with the action of this group on $\text{Gal}(L : K)$, i.e. for $\tau \in \text{Gal}(K : K_0)$ the following diagrams commute (\mathfrak{m} is a modulus for $L : K$):

$$\begin{array}{ccc}
 \mathcal{C}_m(L : K) & \xrightarrow[\sim]{\varphi_K^{(L)}} & \text{Gal}(L : K) & & \text{Gal}(L : K)^\vee & \xrightarrow[\sim]{\check{\varphi}_K^{(L)}} & \mathcal{H}(L : K) \\
 \sim \downarrow \tau_* & & \sim \downarrow f_\tau & & \sim \downarrow f_\tau^\vee & & \sim \downarrow \tau^* \\
 \mathcal{C}_m(L : K) & \xrightarrow[\sim]{\varphi_K^{(L)}} & \text{Gal}(L : K) & & \text{Gal}(L : K)^\vee & \xrightarrow[\sim]{\check{\varphi}_K^{(L)}} & \mathcal{H}(L : K)
 \end{array}$$

where the τ in f_τ is a prolongation of τ to L .

PROOF. Let an embedding $\sigma : L \rightarrow \mathbb{C}$ satisfy $\sigma(a) = a$ for all $a \in K_0$. Then $\sigma(K) = K$ because $K : K_0$ is a Galois extension and so by Corollary 15.3 $\sigma^*(\mathcal{H}(\sigma(L) : K)) = \mathcal{H}(L : K)$. Hence the following are equivalent:

- $L : K_0$ is a Galois extension;
- $\sigma(L) = L$ for all $\sigma : L \rightarrow \mathbb{C}$ with $\sigma(a) = a$ for all $a \in K_0$;
- $\mathcal{H}(\sigma(L) : K) = \mathcal{H}(L : K)$ for all $\sigma : L \rightarrow \mathbb{C}$ with $\sigma(a) = a$ for all $a \in K_0$;
- $(\sigma^*)^{-1}(\mathcal{H}(L : K)) = \mathcal{H}(L : K)$ for all $\sigma : L \rightarrow \mathbb{C}$ with $\sigma(a) = a$ for all $a \in K_0$;
- $\sigma^*(\mathcal{H}(L : K)) = \mathcal{H}(L : K)$ for all $\sigma : L \rightarrow \mathbb{C}$ with $\sigma(a) = a$ for all $a \in K_0$;
- $\tau^*(\mathcal{H}(L : K)) = \mathcal{H}(L : K)$ for all $\tau \in \text{Gal}(K : K_0)$.

The last equivalence follows from the fact that every $\sigma : L \rightarrow \mathbb{C}$ fixing elements of K_0 is a prolongation of some $\tau \in \text{Gal}(K : K_0)$. The commutativity of the diagrams follows from Lemma 15.5. \square

15.7 Theorem. *Let $K' : K$ be an abelian number field extension and X a finite group of Dirichlet characters of K such that there is a class field for $\nu_{K'}^X(X) \subseteq \mathcal{H}(K')$. Then there is a class field for X .*

PROOF. First we prove the theorem under the extra condition that the extension $K' : K$ is cyclic. So let $K' : K$ be cyclic and L' the class field for $\nu_{K'}^X(X)$. Let τ be a generator of $\text{Gal}(K' : K)$. Then $N_K^{K'} \tau_* = N_K^{K'}$ and so $\tau^* \nu_{K'}^X(X) = \nu_{K'}^X(X)$. By Proposition 15.6 the extension $L' : K$ is a Galois extension. The identity $N_K^{K'} \tau_* = N_K^{K'}$ also implies that the action of τ on $\nu_{K'}^X(X) = \mathcal{H}(L' : K')$ is trivial and so by the same proposition the action of τ on $\text{Gal}(L' : K')$ is trivial. Since $\text{Gal}(K' : K)$ is cyclic this implies that $L' : K$ is abelian: the group $\text{Gal}(L' : K)$ is

generated by the abelian subgroup $\text{Gal}(L' : K')$ and a prolongation of τ to L' . From $\nu_{K'}^K(X) = \mathcal{H}(L' : K') = \text{Ker}(\nu_{L'}^{K'})$ follows that $X \subseteq \text{Ker}(\nu_{L'}^{K'} \nu_{K'}^K) = \text{Ker}(\nu_{L'}^K) = \mathcal{H}(L' : K)$. Hence by Proposition 15.1 there is a class field for the group X .

For the general case take a chain of cyclic extensions

$$K = K_0 \subseteq K_1 \subseteq \dots \subseteq K_{j-1} \subseteq K_j \subseteq \dots \subseteq K_r = K'.$$

There is a sequence of finite groups of Dirichlet characters:

$$X, \nu_{K_1}^K(X), \dots, \nu_{K_{j-1}}^K(X), \nu_{K_j}^K(X), \dots, \nu_{K_r}^K(X) = \nu_{K'}^K(X).$$

Since $\nu_{K_j}^K(X) = \nu_{K_j}^{K_{j-1}} \nu_{K_{j-1}}^K(X)$, we have by the cyclic case, that if there is a class field for $\nu_{K_j}^K(X)$, then there is one for $\nu_{K_{j-1}}^K(X)$. This proves that there is a class field for X . \square

This theorem makes it possible to assume in the proof of the Existence Theorem that the base field contains a primitive n -th root of unity, where n is an exponent of this finite group of Dirichlet characters: adjunction of a root of unity is an abelian extension. Then the class field extension has to be a Kummer extension. This was the second step in the proof. In the next section we consider first Kummer extensions in general.

15.2 Kummer extensions

In the previous section the proof of the Existence Theorem was reduced to the case in which the base field has enough roots of unity. The meaning of ‘enough’ in this context is made precise in the following definition.

15.8 Definition. Let $n \in \mathbb{N}^*$. An abelian extension $L : K$ is called an *n-Kummer extension* if $\text{Gal}(L : K)$ has exponent n and K contains a primitive n -th root of unity.

For Kummer extensions the intermediate fields correspond to certain subgroups of the multiplicative group of the base field. This explains their relevance for class field theory. The theory of Kummer extensions is purely algebraic, it is a part of Galois theory.

15.9 Proposition. Let K be a field containing a primitive n -th root of unity and $L : K$ a cyclic Galois extension of degree n . Then there is an $\alpha \in L$ such that $L = K(\alpha)$ and $\alpha^n \in K$.

PROOF. Let $\zeta \in K$ be a primitive n -th root of unity and σ a generator of $\text{Gal}(L : K)$. Then $N_K^L(\zeta) = \zeta^n = 1$. So by Hilbert’s Theorem 90 (Theorem 12.17) there is an $\alpha \in L^*$ such that $\frac{\alpha}{\sigma(\alpha)} = \zeta$. Then $\sigma(\alpha^k) = \alpha^k \iff n \mid k$. So $\alpha^n \in K$ and $L = K(\alpha)$. \square

15.10 Proposition. *Let $L : K$ be an n -Kummer extension. Then there are $\alpha_1, \dots, \alpha_r \in L$ such that $\alpha_j^n \in K$ for $j = 1, \dots, r$ and $L = K(\alpha_1, \dots, \alpha_r)$.*

PROOF. The group $\text{Gal}(L : K)^\vee$ is generated by a finite number of elements of order a divisor of n . So by Galois theory there are intermediate fields L_1, \dots, L_r of $L : K$ such that each $\text{Gal}(L_j : K)$ is cyclic of order a divisor of n and $L = L_1 \cdots L_r$. Now the proposition follows from Proposition 15.9. \square

15.11 Proposition. *Let $L : K$ be an n -Kummer extension and $L = K(\alpha_1, \dots, \alpha_r)$ with $\alpha_1^n, \dots, \alpha_r^n \in K^*$. Then $L^{*n} \cap K^* = K^{*n} \langle \alpha_1^n, \dots, \alpha_r^n \rangle$.*

PROOF. Put $L_j = K(\alpha_1, \dots, \alpha_j)$ for $j = 1, \dots, r$. The extensions $L_j : K$ are n -Kummer extensions. Clearly, $K^{*n} \langle \alpha_1^n, \dots, \alpha_j^n \rangle \subseteq L_j^{*n} \cap K^*$. We show that

$$L_j^{*n} \cap K^* = K^{*n} \langle \alpha_1^n, \dots, \alpha_j^n \rangle \quad \text{for } j = 1, \dots, r. \quad (15.1)$$

Let $\beta \in L_1^*$ such that $\beta^n \in K^*$. The group $\text{Gal}(L_1 : K)$ is generated by an automorphism σ with $\sigma(\alpha_1) = \zeta\alpha_1$, where ζ is a, not necessarily primitive, n -th root of unity. Then $\sigma(\beta) = \zeta^k\beta$ for some integer k . From $\sigma(\beta\alpha_1^{-k}) = \beta\alpha_1^{-k}$ follows that $\beta \in K^* \langle \alpha_1 \rangle$ and so $\beta^n \in K^{*n} \langle \alpha_1^n \rangle$.

Assume that $L_{j-1}^{*n} \cap K^* = K^{*n} \langle \alpha_1^n, \dots, \alpha_{j-1}^n \rangle$ for some $j \leq r$. Let $\beta \in L_j^*$ such that $\beta^n \in K^*$. The extension $L_j : L_{j-1}$ is a cyclic n -Kummer extension, so as above $L_j^{*n} \cap L_{j-1}^* = L_{j-1}^{*n} \langle \alpha_j^n \rangle$. So $\beta^n = \gamma^n \alpha_j^{nk}$, where $\gamma \in L_{j-1}^*$ and $k \in \mathbb{Z}$. Because $\beta^n \alpha_j^{-nk} \in L_{j-1}^{*n} \cap K^* = K^{*n} \langle \alpha_1^n, \dots, \alpha_{j-1}^n \rangle$, we have $\beta^n \in K^{*n} \langle \alpha_1^n, \dots, \alpha_j^n \rangle$. So identity (15.1) holds for all j and in particular for $j = r$. \square

A classification theorem for Kummer extensions:

15.12 Theorem. *Let K be a field containing a primitive n -th root of unity. Then there is a one-to-one correspondence between n -Kummer extensions of K and subgroups A of K^* containing K^{*n} such that A/K^{*n} is finite:*

$$\begin{array}{ccc} \begin{array}{l} n\text{-Kummer} \\ \text{extensions of } K \end{array} & \longleftrightarrow & \begin{array}{l} \text{subgroups of } K^* \text{ containing } K^{*n} \\ \text{as a subgroup of finite index} \end{array} \\ L : K & \longmapsto & L^{*n} \cap K^* \\ K(\sqrt[n]{A}) & \longleftarrow & A \end{array}$$

(The extensions of K are assumed to be inside a fixed algebraic closure of K .)

PROOF. We will prove:

- a) If $L : K$ is an n -Kummer extension, then for $A = L^{*n} \cap K^*$ we have $L = K(\sqrt[n]{A})$ and A/K^{*n} is finite.

b) If A is a subgroup of K^* containing K^{*n} and such that A/K^{*n} is finite, then $K(\sqrt[n]{A}) : K$ is an n -Kummer extension and $A = L^{*n} \cap K^*$, where $L = K(\sqrt[n]{A})$.

For a proof of a) let $L : K$ be an n -Kummer extension. Then by Proposition 15.10 there are $\alpha_1, \dots, \alpha_r \in L^*$ such that $L = K(\alpha_1, \dots, \alpha_r)$ and $\alpha_j^n \in K$ for $j = 1, \dots, r$. By Proposition 15.11 $L = K(\alpha_1, \dots, \alpha_r) = K(\sqrt[n]{A})$. The group $L^{*n} \cap K^*/K^{*n}$ is generated by the classes of $\alpha_1^n, \dots, \alpha_r^n$ and these are of finite order. So the group A/K^{*n} is finite. We have $\alpha_1, \dots, \alpha_n \in \sqrt[n]{A} \subseteq L^*$ and $L = K(\alpha_1, \dots, \alpha_r)$, so $L = K(\sqrt[n]{A})$.

Now let A be a group with $K^{*n} \subseteq A \subseteq K^*$ and A/K^{*n} finite. Then $A = K^{*n}\langle a_1, \dots, a_r \rangle$ with $a_1, \dots, a_r \in A$ and $K(\sqrt[n]{A}) = K(\alpha_1, \dots, \alpha_n) : K$, where $\alpha_j^n = a_j$ for $j = 1, \dots, r$. Put $L = K(\alpha_1, \dots, \alpha_n)$. Then $L : K$ is an n -Kummer extension and, as we have seen, $L^{*n} \cap K^* = K^{*n}\langle \alpha_1^n, \dots, \alpha_r^n \rangle = A$. \square

Theorem 15.14 describes the connection between the Galois group of a Kummer extension and the corresponding subgroup of the multiplicative group of the base field. The main tool is the following.

15.13 Lemma. *Let $L : K$ be an n -Kummer extension and $\beta \in L^*$ such that $\beta^n \in K^*$. Then the map*

$$\text{Gal}(L : K) \rightarrow \mu_n, \quad \sigma \mapsto \frac{\sigma(\beta)}{\beta}$$

is a group homomorphism.

PROOF. Let $\sigma, \tau \in \text{Gal}(L : K)$. Put $\frac{\tau(\beta)}{\beta} = \zeta \in \mu_n$. Then

$$\frac{\sigma\tau(\beta)}{\beta} = \frac{\sigma(\zeta\beta)}{\beta} = \frac{\zeta\sigma(\beta)}{\beta} = \frac{\sigma(\beta)}{\beta} \cdot \frac{\tau(\beta)}{\beta}. \quad \square$$

15.14 Theorem. *Let $L : K$ be an n -Kummer extension. Then the map*

$$L^{*n} \cap K^* \rightarrow \text{Gal}(L : K)^\vee, \quad a \mapsto \left(\sigma \mapsto \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}} \right)$$

*induces an isomorphism $(L^{*n} \cap K^*)/K^{*n} \xrightarrow{\sim} \text{Gal}(L : K)^\vee$.*

PROOF. By Lemma 15.13 we have a bilinear map

$$\text{Gal}(L : K) \times (L^{*n} \cap K^*)/K^{*n} \rightarrow \mu_n, \quad (\sigma, aK^{*n}) \mapsto \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}.$$

The theorem follows from the nondegeneracy of this pairing.

If $\sigma(\sqrt[n]{a}) = \sqrt[n]{a}$ for all $\sigma \in \text{Gal}(L : K)$, then $\sqrt[n]{a} \in K^*$ and so $a \in K^{*n}$.

If $\sigma(\sqrt[n]{a}) = \zeta \sqrt[n]{a}$ for all $a \in L^{*n} \cap K^*$, then it follows from Proposition 15.11 that $\sigma = 1$. \square

15.3 The Existence Theorem

As indicated at the end of section 15.1 we can assume that the class field extension we are looking for is a Kummer extension. We need some results on the splitting behavior of primes in a Kummer extension of number fields. The first such property is given by the following lemma.

15.15 Lemma. *Let F be a local field containing a primitive n -th root of unity and $\alpha \in F^*$ such that $v(\alpha) = v(n) = 0$. Then the n -Kummer extension $F(\sqrt[n]{\alpha}) : F$ of local fields is unramified.*

PROOF. The minimal polynomial of $\gamma = \sqrt[n]{\alpha}$ is $X^d - \beta$ for some $d \mid n$ and $\beta = \gamma^d$. Put $E = F(\gamma)$. By Definition 7.22

$$\text{disc}(1, \gamma, \dots, \gamma^{d-1}) \in \mathfrak{d}_F(E).$$

Since $d \mid n$ and $\beta^n = \alpha^d$, we also have $v(\beta) = v(d) = 0$. Then from

$$\text{disc}(1, \gamma, \dots, \gamma^{d-1}) = \pm N_F^E(d\gamma^{d-1}) = \pm d^d \beta^{d-1}$$

follows that $v_F(\text{disc}(1, \gamma, \dots, \gamma^{d-1})) = 0$. So $\mathfrak{d}_F(E) = \mathcal{O}_F$. Therefore, $E : F$ is unramified (Theorem 7.28). \square

15.16 Corollary. *Let K be a number field containing μ_n , $a \in K^*$ and \mathfrak{p} a finite prime of K satisfying $v_{\mathfrak{p}}(a) = v_{\mathfrak{p}}(n) = 0$. Then \mathfrak{p} does not ramify in the n -Kummer extension $K(\sqrt[n]{a}) : K$.*

PROOF. Take the \mathfrak{q} -adic completion of $K(\sqrt[n]{a})$, where \mathfrak{q} is a prime above \mathfrak{p} , and apply Lemma 15.15. \square

The n -Kummer extensions of a field K correspond to finite subgroups of K^*/K^{*n} . For local fields this group is finite:

15.17 Proposition. *Let F be a local field. Assume that F contains a primitive n -th root of unity. Then*

$$\#(F^*/F^{*n}) = n^2 N(\mathfrak{p}_F)^{v_F(n)}.$$

PROOF. We will use group cohomology in a rather trivial setting. Let G be a cyclic group of order n and consider F^* as a G -module with trivial G -action. Then $H^0(F^*) = F^*/F^{*n}$ and $H^1(F^*) = \mu_n$. So $\#(F^*/F^{*n}) = n \cdot q(F^*)^{-1}$. We have the short exact sequence of G -modules

$$1 \longrightarrow \mathcal{O}_F^* \longrightarrow F^* \xrightarrow{v_F} \mathbb{Z} \longrightarrow 0.$$

So $q(F^*) = q(\mathcal{O}_F^*)q(\mathbb{Z}) = q(\mathcal{O}_F^*)n^{-1}$ and it remains to compute $q(\mathcal{O}_F^*)$. For sufficiently large r we have

$$q(\mathcal{O}_F^*) = q(1 + \mathfrak{p}^r) = q(\mathfrak{p}^r) = q(\mathcal{O}_F) = \frac{\#(H^1(\mathcal{O}_F))}{\#(H^0(\mathcal{O}_F))} = \frac{1}{\#(\mathcal{O}_F/n\mathcal{O}_F)}$$

$$= \frac{1}{\#(\mathcal{O}_F/\mathfrak{p}_F^{v_F(n)})} = N(\mathfrak{p}_F)^{-v_F(n)}.$$

Hence $\#(F^*/F^{*n}) = n \cdot q(F^*)^{-1} = n^2 q(\mathcal{O}_F)^{-1} = n^2 N(\mathfrak{p}_F)^{v_F(n)}$. \square

We will use the following lemma, which is similar to Proposition 14.1 and so is its proof.

15.18 Lemma. *Let $n \in \mathbb{N}^*$. The arithmetic projective system $\mathfrak{m} \mapsto K^*/K^{*n}K_{\mathfrak{m}}^1$ of a number field K is multiplicative.*

PROOF. Let \mathfrak{m}_1 and \mathfrak{m}_2 be moduli of K with $\gcd(\mathfrak{m}_1, \mathfrak{m}_2) = 1$. The identity $K_{\mathfrak{m}_1}^1 K_{\mathfrak{m}_2}^1 = K^*$ implies that $K^{*n} K_{\mathfrak{m}_1}^1 K^{*n} K_{\mathfrak{m}_2}^1 = K^*$, so it remains to prove that

$$K^{*n} K_{\mathfrak{m}_1}^1 \cap K^{*n} K_{\mathfrak{m}_2}^1 = K^{*n} K_{\mathfrak{m}_1 \mathfrak{m}_2}^1.$$

Let $c = a_1^n b_1 = a_2^n b_2$ with $a_1, a_2 \in K^*$, $b_1 \in K_{\mathfrak{m}_1}^1$ and $b_2 \in K_{\mathfrak{m}_2}^1$. There is an $a \in K^*$ such that $a^{-1} a_1 \in K_{\mathfrak{m}_1}^1$ and $a^{-1} a_2 \in K_{\mathfrak{m}_2}^1$. Then $c = a^n (a^{-1} a_1)^n b_1 = a^n (a^{-1} a_2)^n b_2$ and so $(a^{-1} a_1)^n b_1 = (a^{-1} a_2)^n b_2 \in K_{\mathfrak{m}_1}^1 \cap K_{\mathfrak{m}_2}^1 = K_{\mathfrak{m}_1 \mathfrak{m}_2}^1$. Hence $c \in K^{*n} K_{\mathfrak{m}_1 \mathfrak{m}_2}^1$. \square

15.19 Proposition. *Let K be a number field containing μ_n and \mathfrak{m} a modulus of K divisible by the prime divisors of $n\mathcal{O}_K$ and all infinite primes of K , the finite prime divisors with a sufficiently large exponent. Let S be the set of prime divisors of \mathfrak{m} . Then*

$$\#(K^*/K^{*n}K_{\mathfrak{m}}^1) = n^{2s},$$

where $s = \#(S)$.

PROOF. By Lemma 15.18 $\#(K^*/K^{*n}K_{\mathfrak{m}}^1)$ is the product of all $\#(K^*/K^{*n}K_{\mathfrak{p}^r}^1)$ over $\mathfrak{p} \in S$. For \mathfrak{p} real infinite necessarily $n = 2$ and since $K^{*2} \subseteq K_{\mathfrak{p}}^1$, we have $\#(K^*/K^{*2}K_{\mathfrak{p}}^1) = \#(K^*/K_{\mathfrak{p}}^1) = 2$. For \mathfrak{p} complex infinite $\#(K^*/K^{*n}K_{\mathfrak{p}}^1) = 1$.

For finite $\mathfrak{p} \in S$ we have $K^*/K^{*n}K_{\mathfrak{p}^r}^1 \xrightarrow{\sim} K_{\mathfrak{p}}^*/K_{\mathfrak{p}}^{*n}$ for r sufficiently large. So by Proposition 15.17 $\#(K^*/K^{*n}K_{\mathfrak{p}^r}^1) = n^2 N(\mathfrak{p})^{v_{\mathfrak{p}}(n)}$.

Let s_0 be the number of finite primes in S and s_{∞} the number of infinite primes. Then for $n \neq 2$ by Lemma 15.18:

$$\begin{aligned} \#(K^*/K^{*n}K_{\mathfrak{m}}^1) &= \prod_{\mathfrak{p}|\mathfrak{m}_0} n^2 N(\mathfrak{p})^{v_{\mathfrak{p}}(n)} = n^{2s_0} N\left(\prod_{\mathfrak{p}|\mathfrak{m}_0} \mathfrak{p}^{v_{\mathfrak{p}}(n)}\right) = n^{2s_0} N(n\mathcal{O}_K) \\ &= n^{2s_0} n^{[K:\mathbb{Q}]} = n^{2s_0} n^{2s_{\infty}} = n^{2s}. \end{aligned}$$

For $n = 2$ let r_{∞} be the number of real infinite primes. Then

$$\begin{aligned} \#(K^*/K^{*2}K_{\mathfrak{m}}^1) &= 2^{2s_0} N(2\mathcal{O}_K) 2^{r_{\infty}} = 2^{2s_0} \cdot 2^{r_{\infty} + 2(s_{\infty} - r_{\infty})} \cdot 2^{r_{\infty}} \\ &= 2^{2s_0 + 2s_{\infty}} = 2^{2s}. \end{aligned} \quad \square$$

15.20 Definition. A collection S of primes of a number field K is called *saturated* if it contains $\mathcal{P}_\infty(K)$. The collection $\mathcal{P}_\infty(K)$ is the smallest saturated collection of primes and is often denoted by S_∞ .

15.21 Definition and notations. Let K be a number field, S a finite saturated collection of primes of K . Then $\mathbb{I}^S(K)$ denotes the subgroup of $\mathbb{I}(K)$ of all \mathfrak{a} with $v_{\mathfrak{p}}(\mathfrak{a}) = 0$ for all finite primes $\mathfrak{p} \in S$. An element $\alpha \in K^*$ is called an S -unit of K if $v_{\mathfrak{p}}(\alpha) = 0$ for all finite primes $\mathfrak{p} \notin S$. The group of S -units of K is denoted by K^S .

Note that K^S is the same the group as K_P^* described in Notations 6.30, where P is the complement of S in $\mathcal{P}(K)$. So K^S is the unit group of the Dedekind domain K_P . The exact sequence (6.1) on page 140 becomes

$$1 \longrightarrow \mathcal{O}_K^* \longrightarrow K^S \longrightarrow \bigoplus_{\substack{\mathfrak{p} \in S \\ \mathfrak{p} \text{ finite}}} \mathbb{Z} \longrightarrow \mathcal{C}(K) \longrightarrow \mathcal{C}^S(K) \longrightarrow 1,$$

where $\mathcal{C}^S(K)$ is the ideal class group of K_P .

15.22 Definition. The group $\mathcal{C}^S(K)$ described above is called the S -ideal class group of K .

By the above exact sequence $\mathcal{C}^S(K)$ is isomorphic to the factor group of $\mathcal{C}(K)$ obtained by killing the classes of the finite primes in S .

Theorem 6.31 can be reformulated as follows:

15.23 Theorem. *Let S be a finite saturated collection of primes of K and $\#(S) = s$. Then $K^S/\mu(K)$ is a free abelian group of rank $s - 1$. \square*

Here we will need the following consequence.

15.24 Corollary. *Let the number field K contain a primitive n -th root of unity and let S be a finite saturated collection of primes of K . Then $K^S/(K^S)^n \cong (\mathbb{Z}/n)^{\#(S)}$. \square*

15.25 Proposition. *Let the number field K contain μ_n and let S be a finite saturated collection of primes of K containing all prime divisors of $n\mathcal{O}_K$. Then the extension $K(\sqrt[n]{K^S}) : K$ is an n -Kummer extension with $\text{Gal}(K(\sqrt[n]{K^S}) : K) \cong (\mathbb{Z}/n)^{\#(S)}$ and the ramifying primes are all in S .*

PROOF. By Theorem 15.23 the group K^S is finitely generated, so $K(\sqrt[n]{K^S}) : K$ is an n -Kummer extension. By Theorem 15.14, Theorem 15.12 and Corollary 15.24 we have

$$\text{Gal}(K(\sqrt[n]{K^S}) : K) \cong K^S K^{*n} / K^{*n} \cong K^S / (K^S \cap K^{*n}) = K^S / (K^S)^n \cong (\mathbb{Z}/n)^{\#(S)}.$$

For each $a \in K^S$ and $\mathfrak{p} \in P$ it follows from Corollary 15.16 that \mathfrak{p} does not ramify in $K(\sqrt[n]{a})$. Hence none of the $\mathfrak{p} \notin S$ ramify in $K(\sqrt[n]{K^S})$. \square

15.26 Theorem. *Let the number field K contain μ_n and let S be a finite saturated collection of primes of K containing all prime divisors of $n\mathcal{O}_K$ and such that $\mathcal{C}^S(K)$ is trivial. Then for \mathfrak{m} a modulus of K with prime divisors the primes in S , the finite ones with a sufficiently large exponent, the field $K(\sqrt[n]{K^S})$ is the class field for ${}_n\mathcal{H}_{\mathfrak{m}}(K)$.*

PROOF. Put $L = K(\sqrt[n]{K^S})$. By Proposition 15.25 all in L ramifying primes of K are in S . Artin's Reciprocity Law (Theorem 14.16) implies that $\mathcal{H}(L : K) \subseteq \mathcal{H}_{\mathfrak{m}}(K)$. Because n is an exponent of $\text{Gal}(L : K)$, and therefore of $\mathcal{H}(L : K)$ as well, we have $\mathcal{H}(L : K) \subseteq {}_n\mathcal{H}_{\mathfrak{m}}(K)$. By Proposition 15.25 $\#(\mathcal{H}(L : K)) = n^{\#(S)}$. So it suffices to show that $\#({}_n\mathcal{H}_{\mathfrak{m}}(K)) = n^{\#(S)}$.

The modulus \mathfrak{m} is such that $\mathbb{I}^{\mathfrak{m}}(K) = \mathbb{I}^S(K)$. Let the map $f : K^* \rightarrow \mathbb{I}^{\mathfrak{m}}(K)$ be the composition of $K^* \rightarrow \mathbb{I}(K)$, $a \mapsto a\mathcal{O}_K$ and the projection $\mathbb{I}(K) \rightarrow \mathbb{I}^{\mathfrak{m}}(K)$. For $a \in K^*$ write $a\mathcal{O}_K = \mathfrak{a}\mathfrak{a}_0$ with $\mathfrak{a} \in \mathbb{I}^{\mathfrak{m}}(K)$ and $v_{\mathfrak{p}}(\mathfrak{a}_0) = 0$ for all $\mathfrak{p} \in P$, where again P is the complement of S in $\mathcal{P}(K)$. Then $f(a) = \mathfrak{a}$. The cokernel of f is isomorphic to $\mathcal{C}(K_P) (= \mathcal{C}^S(K))$, a trivial group because K_P is a principal ideal domain. So f is surjective.

Consider the following commutative diagram with exact rows

$$\begin{array}{ccccccc}
 1 & \longrightarrow & \frac{K^{*n}K_{\mathfrak{m}}^1}{K^{*n}} & \longrightarrow & \frac{K^*}{K^{*n}} & \longrightarrow & \frac{K^*}{K^{*n}K_{\mathfrak{m}}^1} \longrightarrow 1 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 1 & \longrightarrow & \frac{\mathbb{I}^{\mathfrak{m}}(K)^n\mathcal{S}_{\mathfrak{m}}(K)}{\mathbb{I}^{\mathfrak{m}}(K)^n} & \longrightarrow & \frac{\mathbb{I}^{\mathfrak{m}}(K)}{\mathbb{I}^{\mathfrak{m}}(K)^n} & \longrightarrow & \frac{\mathbb{I}^{\mathfrak{m}}(K)}{\mathbb{I}^{\mathfrak{m}}(K)^n\mathcal{S}_{\mathfrak{m}}(K)} \longrightarrow 1
 \end{array}$$

in which the vertical maps are induced by f . Note that they are surjective. In particular the left most vertical map is surjective and from this it follows that we can complete the diagram to the diagram with exact rows and columns on top of the next page. For the middle vertical exact sequence note that the cohomology groups of a cyclic group of order n acting trivially the short exact sequence

$$1 \longrightarrow K^S \longrightarrow K^* \longrightarrow \mathbb{I}^{\mathfrak{m}}(K) \longrightarrow 1$$

yields the exactness of

$$1 \longrightarrow H^0(K^S) \longrightarrow H^0(K^*) \longrightarrow H^0(\mathbb{I}^{\mathfrak{m}}(K)) \longrightarrow 1.$$

Furthermore, we have $K^{*n}K^S/K^{*n} \cong K^S/K^S \cap K^{*n} = K^S/(K^S)^n$.

$$\begin{array}{ccccccc}
 & & 1 & & 1 & & 1 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 1 & \longrightarrow & \frac{K^{*n}K^S \cap K^{*n}K_m^1}{K^{*n}} & \longrightarrow & \frac{K^{*n}K^S}{K^{*n}} & \longrightarrow & \frac{K^{*n}K^S K_m^1}{K^{*n}K_m^1} \longrightarrow 1 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 1 & \longrightarrow & \frac{K^{*n}K_m^1}{K^{*n}} & \longrightarrow & \frac{K^*}{K^{*n}} & \longrightarrow & \frac{K^*}{K^{*n}K_m^1} \longrightarrow 1 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 1 & \longrightarrow & \frac{\mathbb{I}^m(K)^n \mathbb{S}_m(K)}{\mathbb{I}^m(K)^n} & \longrightarrow & \frac{\mathbb{I}^m(K)}{\mathbb{I}^m(K)^n} & \longrightarrow & \frac{\mathbb{I}^m(K)}{\mathbb{I}^m(K)^n \mathbb{S}_m(K)} \longrightarrow 1 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & 1 & & 1 & & 1
 \end{array}$$

So for the order of ${}_n\mathcal{H}_m(K)$ we have, using Proposition 15.19 and Corollary 15.24

$$\begin{aligned}
 \#({}_n\mathcal{H}_m(K)) &= \#(\mathbb{I}^m(K)/\mathbb{I}^m(K)^n \mathbb{S}_m(K)) = \frac{\#(K^*/K^{*n}K_m^1)}{\#(K^{*n}K_P^*K_m^1/K^{*n}K_m^1)} \\
 &= \frac{\#(K^*/K^{*n}K_m^1)}{\#(K^S/(K^S)^n)} \cdot \#((K^{*n}K^S \cap K^{*n}K_m^1)/K^{*n}) \\
 &= n^s \cdot \#((K^{*n}K^S \cap K^{*n}K_m^1)/K^{*n}).
 \end{aligned}$$

It suffices to show that $K^{*n}K^S \cap K^{*n}K_m^1 \subseteq K^{*n}$ or, what amounts to the same, $K^S \cap K^{*n}K_m^1 \subseteq K^{*n}$. Let $b \in K^S \cap K^{*n}K_m^1$. We show that the extension $K(\sqrt[n]{b}) : K$ is unramified. For $\mathfrak{p} \in P$ we have $v_{\mathfrak{p}}(b) = 0$ (because $b \in K^S$) and $v_{\mathfrak{p}}(n) = 0$ (because $\mathfrak{p} \notin S$). By Corollary 15.16 \mathfrak{p} does not ramify in $K(\sqrt[n]{b})$. For finite $\mathfrak{p} \in S$ we have $b \in K^{*n}K_{\mathfrak{p}}^1 \subseteq K_{\mathfrak{p}}^{*n}(1 + \hat{\mathfrak{p}}^r) = K_{\mathfrak{p}}^{*n}$ and therefore, \mathfrak{p} splits completely in $K(\sqrt[n]{b})$. Finally for real infinite \mathfrak{p} and $n = 2$ we have $b \in K^{*2}K_{\{\mathfrak{p}\}}^1 \subseteq K_{\mathfrak{p}}^{*2}K_{\mathfrak{p}}^1 = K_{\mathfrak{p}}^1$ and from this it follows that \mathfrak{p} does not ramify.

Since $K(\sqrt[n]{b}) : K$ is an unramified abelian extension, Artin's Reciprocity Law implies that its conductor is trivial. Hence the group

$$\mathbb{I}(K)/N_K^{K(\sqrt[n]{b})}(\mathbb{I}(K(\sqrt[n]{b})))\mathbb{P}(K)$$

is of order $[K(\sqrt[n]{b}) : K]$. Let $\mathfrak{a} \in \mathbb{I}(K)$. Since K_P is a principal ideal domain we can write $\mathfrak{a} = \mathfrak{a}_0 \cdot c\mathcal{O}_K$ with $c \in K^*$ and $\mathfrak{a}_0 \in \mathbb{I}(K)$ such that $v_{\mathfrak{p}}(\mathfrak{a}_0) = 0$ for all $\mathfrak{p} \in P$. All finite \mathfrak{p} in S split completely in $K(\sqrt[n]{b})$, so we have $\mathfrak{a}_0 \in N_K^{K(\sqrt[n]{b})}(\mathbb{I}(K(\sqrt[n]{b})))$. Therefore, $[K(\sqrt[n]{b}) : K] = 1$, that is $\sqrt[n]{b} \in K^*$. Hence $b \in K^{*n}$. \square

15.27 Existence Theorem. *For every finite group of Dirichlet characters of a number field there is a class field.*

PROOF. Let K be a number field and X a finite group of Dirichlet characters of K . Let n be an exponent of X . Put $K' = K(\zeta_n)$. Then $Y := \nu_{K'}^X(X)$ is a finite group of Dirichlet characters of K' and n is an exponent of this homomorphic image of X as well. Let \mathfrak{f} be the conductor of Y . Choose a finite saturated collection S of primes of K' such that

- a) S contains all prime divisors of $n\mathcal{O}_{K'}$,
- b) $\mathcal{C}^S(K')$ is trivial,
- c) S contains all prime divisors of \mathfrak{f} .

By Theorem 15.26 for moduli \mathfrak{m} with prime divisors the primes in S and the finite ones with sufficiently large exponents in \mathfrak{m} , there is a class field for the group ${}_n\mathcal{H}_{\mathfrak{m}}(K')$. Let, moreover, the exponents of the finite prime divisors of \mathfrak{m} be such that $\mathfrak{f} \mid \mathfrak{m}$. Then $Y \subseteq {}_n\mathcal{H}_{\mathfrak{m}}(K')$. By Proposition 15.1 there is a class field for Y and, finally, there is a class field for X by Theorem 15.7. \square

15.28 Notation. Let X be a finite group of Dirichlet characters of a number field K . The class field for X is denoted by K_X .

The Existence Theorem was the main still missing part of the Classification Theorem announced in section 13.5.

15.29 Classification Theorem. *Let K be a number field. The following maps form a one-to-one correspondence between abelian number field extensions $L : K$ and finite subgroups of $\mathcal{H}(K)$:*

$$\begin{array}{ccc}
 \begin{array}{c} \text{abelian} \\ \text{extensions of } K \end{array} & \longleftrightarrow & \begin{array}{c} \text{finite groups of} \\ \text{Dirichlet characters of } K \end{array} \\
 L : K & \longmapsto & \mathcal{H}(L : K) \\
 K_X : K & \longleftarrow & X
 \end{array}$$

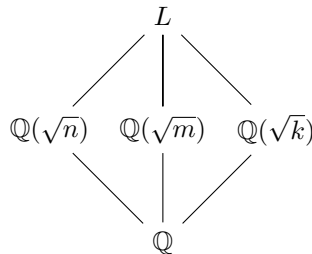
The maps $L \mapsto \mathcal{H}(L : K)$ and $X \mapsto K_X : K$ are inverses of each other and they preserve the ordering given by inclusion. The prime divisors of the conductor of $\mathcal{H}(L : K)$ are ramifying primes. For \mathfrak{m} a modulus divisible by the conductor of $\mathcal{H}(L : K)$ and all ramifying primes, the Artin map $\varphi_K^{(L)} : \mathbb{I}^{\mathfrak{m}}(K) \rightarrow \text{Gal}(L : K)$ induces an isomorphism $\check{\varphi}_K^{(L)} : \text{Gal}(L : K)^{\vee} \xrightarrow{\sim} \mathcal{H}(L : K)$.

PROOF. The groups $\mathcal{H}(L : K)$ were defined in Definition 13.34 and according to Theorem 13.44 they are finite. Lemma 14.22 implies that the map $(L : K) \mapsto \mathcal{H}(L : K)$ is injective. The existence of class fields now shows that it is a bijection. From Lemma 13.35 it follows that the maps preserve the ordering by inclusion. The statement concerning the Artin map is Artin's Reciprocity Law. \square

The first proof of the Classification Theorem was by Takagi in 1920. However, he had a different notion of class field: L is the class field of $\mathcal{C}_m(L : K)$ if $L : K$ is abelian and $\#(\mathcal{C}_m(L : K)) = [L : K]$. Later, Artin introduced the Artin map and proved the Artin Reciprocity Law: the Artin map induces an isomorphism $\mathcal{C}_m(L : K) \xrightarrow{\sim} \text{Gal}(L : K)$.

The values of Dirichlet characters of an abelian extension on nonramifying primes describe their splitting behavior in the extension. Theorems in the sections 15.6 and 15.5 give extra information, especially for the ramifying primes.

15.30 Example. In section 4.9 the 2-rank of the ideal class group of a quadratic number field K has been computed (Theorems 4.73 and 4.81). This was done by counting the number of elements of ${}_2\mathcal{C}(\mathcal{O}_K)$ using the theory behind the algorithms for the computation of the ideal class group of a quadratic number field. Here we use $\mathcal{C}(K)/\mathcal{C}(K)^2$ instead. This group corresponds to the group ${}_2\mathcal{H}(K)$. Let's first consider ${}_2\mathcal{H}_\infty(K)$. The nontrivial elements of this group correspond to quadratic extensions $L : K$ in which the finite primes do not ramify. Since $\text{Gal}(K : \mathbb{Q})$ acts on $\mathcal{C}_\infty(K)$ by inversion, the action of $\text{Gal}(K : \mathbb{Q})$ on ${}_2\mathcal{H}_\infty(K)$ is trivial. By Proposition 15.6 this means that the extensions $L : \mathbb{Q}$ are Galois extensions. By Corollary 7.49 they are noncyclic. Set $K = \mathbb{Q}(\sqrt{m})$ with $m \in \mathbb{Z}$ squarefree $\neq 0, 1$. Then we have



where, since finite primes of K do not ramify in L , $\text{gcd}(D_n, D_k) = 1$. This means that $D_m = D_n D_k$. So the number of quadratic extensions of K which are unramified outside ∞ is equal to the number of ways D_m is the product of two nontrivial discriminants. This number is $2^{r(D_m)-1} - 1$, where $r(D_m)$ is the number of prime divisors of D_m . It follows that the 2-rank of $\mathcal{C}_\infty(K)$ is equal to $r(D_m) - 1$. For $m < 0$ we have $\mathcal{C}(K) = \mathcal{C}_\infty(K)$, so this is the 2-rank of $\mathcal{C}(K)$ as well.

Now let m be positive. For the 2-rank of $\mathcal{C}(K)$ there is the extra condition that D_n and D_k have to be positive. For this use Lemma 4.10. The discriminant D_n is positive if and only if the number of prime divisors $\equiv 3 \pmod{4}$ of n is even. If m has no such prime divisors, that is if m is the sum of two squares, then there is no extra condition needed. So in this case the 2-rank of $\mathcal{C}(K)$ is $r(D_m) - 1$. Otherwise the 2-rank is $r(D_m) - 2$.

15.4 Chebotarev's Density Theorem

In section 13.4 we considered the L -series of a Dirichlet character χ of a number field K . The series converges absolutely on the half-plane $\Re(s) > 1$ and it was shown that it has a prolongation to a meromorphic function on $\Re(s) > 1 - \frac{1}{[K:\mathbb{Q}]}$. For χ the principal character it is the Dedekind zeta function of K , which has a simple pole at $s = 1$. For $\chi \neq 1$ the function is analytic on $\Re(s) > 1 - \frac{1}{[K:\mathbb{Q}]}$ (Proposition 13.41). As was the case with nonprincipal Dirichlet characters of \mathbb{Q} , its nonvanishing at $z = 1$, which we are able to prove at this stage, has many consequences.

15.31 Theorem. *Let χ be a nonprincipal Dirichlet character of a number field K . Then $L(1, \chi) \neq 0$.*

PROOF. Let X be the nontrivial group $\langle \chi \rangle$ of Dirichlet characters of K . Put $L = K_X$. Then $X = \mathcal{H}(L : K)$. Let P be the set of prime ideals of K which split completely in L . Then by Theorem 8.37 we have $\delta(P) = \frac{1}{n}$, where $n = [L : K] = \#(X) = o(\chi)$. By Artin's Reciprocity Theorem P is the set of nonramifying primes \mathfrak{p} of K satisfying $\chi(\mathfrak{p}) = 1$. So by Corollary 13.43 we have $L(1, \chi) \neq 0$. \square

This implies a generalization of Dirichlet's theorem on primes in an arithmetic progression. We need a generalization of Lemma 9.51.

15.32 Lemma. *Let X be a finite group of Dirichlet characters of a number field K , \mathfrak{f} the conductor of X and $\mathfrak{a} \in \mathbb{I}^{\mathfrak{f}}(K)$. Then*

$$\sum_{\chi \in X} \chi(\mathfrak{a}) = \begin{cases} \#(X) & \text{if } \chi(\mathfrak{a}) = 1 \text{ for all } \chi \in X, \\ 0 & \text{otherwise.} \end{cases}$$

PROOF. For all $\chi \in X$ we have $\chi(\mathfrak{a}) \neq 0$, since $\mathfrak{a} \in \mathbb{I}^{\mathfrak{f}}(K)$. If $\chi_1(\mathfrak{a}) \neq 1$ for some $\chi_1 \in X$, then from

$$\chi_1(\mathfrak{a}) \sum_{\chi \in X} \chi(\mathfrak{a}) = \sum_{\chi \in X} \chi_1 \chi(\mathfrak{a}) = \sum_{\chi \in X} \chi(\mathfrak{a})$$

follows that $\sum_{\chi \in X} \chi(\mathfrak{a}) = 0$. \square

15.33 Theorem. Let X be a finite group of Dirichlet characters of a number field K , \mathfrak{f} the conductor of X , $\mathfrak{a} \in \mathbb{I}^{\mathfrak{f}}(K)$ and P the set of finite primes of K with $\chi(\mathfrak{p}) = \chi(\mathfrak{a})$ for all $\chi \in X$. Then $\delta(P) = \frac{1}{\#(X)}$.

PROOF. By Proposition 8.31

$$\log L(s, \chi) \sim \sum_{\mathfrak{p}} \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s}$$

for all $\chi \in X$. Now apply Lemma 15.32:

$$\sum_{\chi \in X} \overline{\chi(\mathfrak{a})} \log L(s, \chi) \sim \sum_{\chi \in X} \sum_{\mathfrak{p}} \frac{\overline{\chi(\mathfrak{a})} \chi(\mathfrak{p})}{N(\mathfrak{p})^s} = \sum_{\mathfrak{p}} \sum_{\chi \in X} \frac{\overline{\chi(\mathfrak{a})} \chi(\mathfrak{p})}{N(\mathfrak{p})^s} = \sum_{\mathfrak{p} \in P} \frac{\#(X)}{N(\mathfrak{p})^s}.$$

By Theorem 15.31

$$\sum_{\chi \in X} \overline{\chi(\mathfrak{a})} \log L(s, \chi) = \log \zeta_K(s) + \sum_{\substack{\chi \in X \\ \chi \neq 1}} \overline{\chi(\mathfrak{a})} \log L(s, \chi) \sim \log \zeta_K(s).$$

Finally by Proposition 8.33

$$\sum_{\mathfrak{p} \in P} \frac{1}{N(\mathfrak{p})^s} \sim \frac{\log \zeta_K(s)}{\#(X)} \sim \frac{-\log(s-1)}{\#(X)}.$$

Hence $\delta(P) = \frac{1}{\#(X)}$. □

A direct consequence is Chebotarev's Density Theorem for abelian extensions, which is a stronger version of the Frobenius Density Theorem for abelian extensions (Theorem 8.31).

15.34 Theorem. Let $L : K$ be an abelian number field extension, $\sigma \in \text{Gal}(L : K)$ and P be the collection of nonramifying finite primes \mathfrak{p} of K for which $\varphi_{\mathfrak{p}}^{(L)} = \sigma$. Then $\delta(P) = \frac{1}{[L:K]}$.

PROOF. Let $\mathfrak{a} \in \mathbb{I}^{\mathfrak{f}}(K)$, where \mathfrak{f} is the conductor of $L : K$, such that $\varphi_K^{(L)}(\mathfrak{a}) = \sigma$. Then by Artin's Reciprocity Theorem $\varphi_{\mathfrak{p}}^{(L)} = \sigma$ if and only if $\chi(\mathfrak{p}) = \chi(\mathfrak{a})$ for all $\chi \in \mathcal{H}(L : K)$. By Theorem 15.33 we have $\delta(P) = \frac{1}{[L:K]}$. □

Chebotarev's Density Theorem applies to Galois extensions of number fields in general.

15.35 Theorem (Chebotarev). Let $L : K$ be a Galois extension of number fields, $G = \text{Gal}(L : K)$, $\sigma \in G$, C the conjugacy class in G of σ and P the collection of nonramifying finite primes \mathfrak{p} of K above which there is a prime \mathfrak{q} of L with $\varphi_K^{(L)}(\mathfrak{q}) = \sigma$. Then $\delta(P) = \frac{\#(C)}{[L:K]}$.

PROOF. Let $\mathfrak{p} \in \text{Max}(\mathcal{O}_K)$ nonramifying in L and $\mathfrak{q} \in \text{Max}(\mathcal{O}_L)$ such that $\mathfrak{q} \cap K = \mathfrak{p}$ and $\varphi_K^{(L)}(\mathfrak{q}) = \sigma$. Put $Z = \langle \sigma \rangle$. As was shown in the proof of Proposition 7.54 the primes of L^σ above \mathfrak{p} of residue class degree 1 over K correspond to right cosets $Z\tau$ with $\tau Z\tau^{-1} = Z$. For such a τ we have

$$\varphi_{\tau(\mathfrak{q}) \cap L^\sigma}^{(L)} = \varphi_{L^\sigma}^{(L)}(\tau(\mathfrak{q})) = \varphi_K^{(L)}(\tau(\mathfrak{q})) = \tau\varphi_K^{(L)}(\mathfrak{q})\tau^{-1} = \tau\sigma\tau^{-1}.$$

Hence the number of primes \mathfrak{p}' of L^σ above \mathfrak{p} such that $f_K(\mathfrak{p}') = 1$ and $\varphi_{\mathfrak{p}'}^{(L)} = \sigma$ is equal to the number of cosets $\langle \sigma \rangle\tau$ with $\tau\sigma\tau^{-1} = \sigma$. This is the number $[C_G(\sigma) : \langle \sigma \rangle]$, where $C_G(\sigma) = \{ \tau \in G \mid \sigma\tau = \tau\sigma \}$. Hence for P' the set of primes \mathfrak{p}' of L^σ above a prime $\mathfrak{p} \in P$ such that $f_K(\mathfrak{p}') = 1$ and $\varphi_{\mathfrak{p}'}^{(L)} = \sigma$ we have

$$\delta(P') = [C_G(\sigma) : \langle \sigma \rangle] \cdot \delta(P).$$

For Q the set of primes \mathfrak{p}' of L^σ which do not ramify in L and satisfy $\varphi_{\mathfrak{p}'}^{(L)} = \sigma$ we have by Theorem 15.34

$$\delta(Q) = \frac{1}{[L : L^\sigma]} = \frac{1}{o(\sigma)}.$$

Because $P' \subseteq Q$ and $Q \setminus P'$ consists, apart from some ramified primes, of primes \mathfrak{p}' with $f_K(\mathfrak{p}') > 1$, the sets P' and Q have equal Dirichlet density. So finally

$$\begin{aligned} \delta(P) &= \frac{\delta(P')}{[C_G(\sigma) : \langle \sigma \rangle]} = \frac{\delta(Q)}{[C_G(\sigma) : \langle \sigma \rangle]} \\ &= \frac{1}{o(\sigma) \cdot [C_G(\sigma) : \langle \sigma \rangle]} = \frac{1}{\#(C_G(\sigma))} = \frac{\#(C)}{[L : K]}. \quad \square \end{aligned}$$

15.5 The Complete Splitting Theorem

Dirichlet characters of \mathbb{Q} describe the splitting behavior of prime numbers in abelian number fields. The analogy for Dirichlet characters of a number field K is not yet fully established: a prime \mathfrak{p} of K not in the conductor of an abelian extension $L : K$ might ramify in L . For such a prime we would have $\chi(\mathfrak{p}) \neq 0$ for all $\chi \in \mathcal{H}(L : K)$. We will see that this cannot happen. A crucial step in the proof is the Complete Splitting Theorem, which we will prove in this section by first proving it for Kummer extensions, in which case it is a consequence of the following refinement of Theorem 15.26.

15.36 Theorem. *Let the number field K contain μ_n and let S be a finite saturated collection of primes of K containing all prime divisors of $n\mathcal{O}_K$ and such that $\mathcal{C}^S(K)$ is trivial. Let S be the disjoint union of S_1 and S_2 . For $j = 1, 2$ let \mathfrak{m}_j be a modulus of K with prime divisors the primes in S_j , the finite ones with a sufficiently large exponent in \mathfrak{m}_j . Put*

$$W_1 = K^{*n} K^S \cap K^{*n} K_{\mathfrak{m}_2}^1 \quad \text{and} \quad W_2 = K^{*n} K^S \cap K^{*n} K_{\mathfrak{m}_1}^1.$$

Then the fields $L_1 = K(\sqrt[n]{W_1})$ and $L_2 = K(\sqrt[n]{W_2})$ are the class fields for respectively

$$X_1 = \{ \chi \in {}_n\mathcal{H}_{\mathfrak{m}_1}(K) \mid \chi(\mathfrak{p}) = 1 \text{ for all finite } \mathfrak{p} \text{ in } S_2 \}$$

and

$$X_2 = \{ \chi \in {}_n\mathcal{H}_{\mathfrak{m}_2}(K) \mid \chi(\mathfrak{p}) = 1 \text{ for all finite } \mathfrak{p} \text{ in } S_1 \}.$$

Moreover, the splitting behavior of the primes in S in the fields L_1 and L_2 is as follows:

- a) The primes in S_1 split completely in L_2 and the primes which ramify in L_2 belong to S_2 .
- b) The primes in S_2 split completely in L_1 and the primes which ramify in L_1 belong to S_1 .

PROOF. The extensions $L_j : K$ are n -Kummer extensions:

$$K^{*n} \subseteq W_j \subseteq K^{*n}K^S \subseteq K^*$$

and the index of K^{*n} in $K^{*n}K^S$ is finite.

First we prove the assertions about the splitting behavior of the primes in S in the fields L_1 and L_2 . Let $\mathfrak{p} \in S_1$ and $a \in W_2$. Then in particular $a \in K^{*n}K_{\mathfrak{m}_1}^1$. We will show that \mathfrak{p} splits completely in $K(\sqrt[n]{a})$. From this the complete splitting in L_2 follows, because this field is the composite of such fields $K(\sqrt[n]{a})$. We can assume that $a \in K_{\mathfrak{m}_1}^1$. In case \mathfrak{p} is finite take the exponent k of \mathfrak{p} in \mathfrak{m}_1 large enough such that in the completion $K_{\mathfrak{p}}$ we have: $K_{\mathfrak{p}^k}^1 \subseteq 1 + \hat{\mathfrak{p}}^k \subseteq K_{\mathfrak{p}}^{*n}$. This is possible by Theorem 11.22. Since $a \in K_{\mathfrak{p}^k}^1$, it follows that for a prime \mathfrak{q} of $K(\sqrt[n]{a})$ above \mathfrak{p} we have

$$K(\sqrt[n]{a})_{\mathfrak{q}} = K_{\mathfrak{p}}(\sqrt[n]{a}) = K_{\mathfrak{p}}.$$

Hence $Z_{\mathfrak{p}}^{(K(\sqrt[n]{a}))} = \text{Gal}(K(\sqrt[n]{a})_{\mathfrak{q}} : K_{\mathfrak{p}}) = \{1\}$. For \mathfrak{p} infinite we only have to consider \mathfrak{p} real and $n = 2$. In this case it follows from $\mathbb{R}(\sqrt{a}) = \mathbb{R}$. By symmetry the primes in S_2 split completely in L_1 .

The field L_1 is a subfield of the field $K(\sqrt[n]{K^S})$, so by Proposition 15.25 the primes which ramify in L_1 belong to S and since the primes in S_2 split completely in L_1 , they belong to S_1 . Again by symmetry the primes which ramify in L_2 belong to S_2 .

Since $L_1 : K$ is an n -Kummer extension and because all primes which ramify in L_1 are contained in S_1 , by Artin's Reciprocity Law we can assume that \mathfrak{m}_1 is a modulus for $L_1 : K$. Then $\mathcal{H}(L_1 : K) \subseteq {}_n\mathcal{H}_{\mathfrak{m}_1}(K)$ and since all finite primes in S_2 split completely in L_1 , we have $\mathcal{H}(L_1 : K) \subseteq X_1$. By symmetry $\mathcal{H}(L_2 : K) \subseteq X_2$.

We have to show that equality holds and for this it suffices to show that $[L_j : K] = \#(X_j)$ for $j = 1, 2$.

Put $\mathfrak{m} = \mathfrak{m}_1\mathfrak{m}_2$ and let, as in the proof of Theorem 15.26, $f: K^* \rightarrow \mathbb{I}^{\mathfrak{m}}(K)$ be the composition of $K^* \rightarrow \mathbb{I}(K)$ and the projection $\mathbb{I}(K) \rightarrow \mathbb{I}^{\mathfrak{m}}(K)$. For $b \in K_{\mathfrak{m}_1}^1$ write $b\mathcal{O}_K = \mathfrak{b}_2\mathfrak{b}_3$ with $\mathfrak{b}_2 \in \mathbb{I}^{S_2}(K)$ and $\mathfrak{b}_3 \in \mathbb{I}^{\mathfrak{m}}(K)$. Then $f(b) \equiv \mathfrak{b}_3 = b\mathcal{O}_K \cdot \mathfrak{b}_2^{-1} \in (\mathbb{S}_{\mathfrak{m}_1}(K)\mathbb{I}^{S_2})$. It follows that f induces a map from $K^{*n}K_{\mathfrak{m}_1}^1/K^{*n}$ to $(\mathbb{I}^{\mathfrak{m}_1}(K)^n\mathbb{S}_{\mathfrak{m}_1}(K)\mathbb{I}^{S_2}) \cap \mathbb{I}^{\mathfrak{m}}(K)/\mathbb{I}^{\mathfrak{m}}(K)^n$. So we have a commutative diagram with exact rows

$$\begin{array}{ccccccc} 1 & \longrightarrow & \frac{K^{*n}K_{\mathfrak{m}_1}^1}{K^{*n}} & \longrightarrow & \frac{K^*}{K^{*n}} & \longrightarrow & \frac{K^*}{K^{*n}K_{\mathfrak{m}_1}^1} \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \downarrow \\ 1 & \longrightarrow & \frac{(\mathbb{I}^{\mathfrak{m}_1})^n\mathbb{S}_{\mathfrak{m}_1}\mathbb{I}^{S_2} \cap \mathbb{I}^{\mathfrak{m}}}{(\mathbb{I}^{\mathfrak{m}})^n} & \longrightarrow & \frac{\mathbb{I}^{\mathfrak{m}}}{(\mathbb{I}^{\mathfrak{m}})^n} & \longrightarrow & \frac{\mathbb{I}^{\mathfrak{m}}}{(\mathbb{I}^{\mathfrak{m}_1})^n\mathbb{S}_{\mathfrak{m}_1}\mathbb{I}^{S_2} \cap \mathbb{I}^{\mathfrak{m}}} \longrightarrow 1 \end{array}$$

in which the vertical maps are induced by f . In the bottom row the notation is simplified by deleting (K) in all cases. The middle vertical map is surjective and so is the one on the right. We show that also the vertical map on the left is surjective. For this let $\mathfrak{a} \in \mathbb{I}^{\mathfrak{m}_1}(K)$, $b \in K_{\mathfrak{m}_1}^1$ and $\mathfrak{c} \in \mathbb{I}^{S_2}(K)$ such that $\mathfrak{a}^n \cdot b\mathcal{O}_K \cdot \mathfrak{c} \in \mathbb{I}^{\mathfrak{m}}(K)$. Write $\mathfrak{a} = \mathfrak{a}_2\mathfrak{a}_3$ and $b\mathcal{O}_K = \mathfrak{b}_2\mathfrak{b}_3$, where $\mathfrak{a}_2, \mathfrak{b}_2 \in \mathbb{I}^{S_2}(K)$ and $\mathfrak{a}_3, \mathfrak{b}_3 \in \mathbb{I}^{\mathfrak{m}}(K)$. Then $\mathfrak{a}^n \cdot b\mathcal{O}_K \cdot \mathfrak{c} = \mathfrak{a}_2^n\mathfrak{b}_2\mathfrak{c} \cdot \mathfrak{a}_3^n\mathfrak{b}_3$ and since this is an element of $\mathbb{I}^{\mathfrak{m}}(K)$ we have $\mathfrak{a}_2^n\mathfrak{b}_2\mathfrak{c} = 1$ and $\mathfrak{a}^n \cdot b\mathcal{O}_K \cdot \mathfrak{c} = \mathfrak{a}_3^n\mathfrak{b}_3$. Write $\mathfrak{a}_3 = \mathfrak{a}_{12} \cdot a\mathcal{O}_K$ with $\mathfrak{a}_{12} \in \mathbb{I}^S(K)$ and $a \in K^*$. Then $\mathfrak{a}^n b\mathcal{O}_K = (a\mathcal{O}_K)^n \cdot b\mathcal{O}_K = \mathfrak{a}_3^n \mathfrak{a}_{12}^{-n} \mathfrak{b}_2\mathfrak{b}_3$. Hence $f(\mathfrak{a}^n b) = \mathfrak{a}_3^n \mathfrak{b}_3$.

It follows that we can complete the diagram to the diagram with exact rows and columns on top of the next page. The group X_1 is the bottom right entry in the diagram and $K^{*n}K^S \cap K^{*n}K_{\mathfrak{m}_1}^1 = W_2$. So, as in the proof of Theorem 15.26, for the orders of the groups we have

$$\begin{aligned} \#(X_1) &= \#(\mathbb{I}^{\mathfrak{m}}(K)/(\mathbb{I}^{\mathfrak{m}_1}(K)^n\mathbb{S}_{\mathfrak{m}_1}(K)\mathbb{I}^{S_2}(K) \cap \mathbb{I}^{\mathfrak{m}}(K))) \\ &= \frac{\#(K^*/K^{*n}K_{\mathfrak{m}_1}^1)}{\#(K^{*n}K^S/K^{*n})} \cdot \#(W_2/K^{*n}) = \frac{\#(K^*/K^{*n}K_{\mathfrak{m}_1}^1)}{n^s} \cdot [L_2 : K], \end{aligned}$$

where $s = \#(S)$. By symmetry we have an analogous formula for $\#(X_2)$. Hence

$$\begin{aligned} \#(X_1) \cdot \#(X_2) &= \frac{\#(K^*/K^{*n}K_{\mathfrak{m}_1}^1)}{n^s} \cdot [L_2 : K] \cdot \frac{\#(K^*/K^{*n}K_{\mathfrak{m}_2}^1)}{n^s} \cdot [L_1 : K] \\ &= \frac{\#(K^*/K^{*n}K_{\mathfrak{m}_1}^1) \cdot \#(K^*/K^{*n}K_{\mathfrak{m}_2}^1)}{n^{2s}} \cdot [L_1 : K] \cdot [L_2 : K] \\ &= \frac{\#(K^*/K^{*n}K_{\mathfrak{m}}^1)}{n^{2s}} \cdot [L_1 : K] \cdot [L_2 : K] = [L_1 : K] \cdot [L_2 : K]. \end{aligned}$$

Since $[L_j : K] \leq \#(X_j)$ for $j = 1, 2$, it follows that $[L_j : K] = \#(X_j)$. \square

$$\begin{array}{ccccccc}
 & & 1 & & 1 & & 1 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 1 & \longrightarrow & \frac{K^{*n} K^S \cap K^{*n} K_{\mathfrak{m}_1}^1}{K^{*n}} & \longrightarrow & \frac{K^{*n} K^S}{K^{*n}} & \longrightarrow & \frac{K^{*n} K^S K_{\mathfrak{m}_1}^1}{K^{*n} K_{\mathfrak{m}_1}^1} \longrightarrow 1 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 1 & \longrightarrow & \frac{K^{*n} K_{\mathfrak{m}_1}^1}{K^{*n}} & \longrightarrow & \frac{K^*}{K^{*n}} & \longrightarrow & \frac{K^*}{K^{*n} K_{\mathfrak{m}_1}^1} \longrightarrow 1 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 1 & \longrightarrow & \frac{(\mathbb{I}^{\mathfrak{m}_1})^n \mathbb{S}_{\mathfrak{m}_1} \mathbb{I}^{S_2} \cap \mathbb{I}^{\mathfrak{m}}}{(\mathbb{I}^{\mathfrak{m}})^n} & \longrightarrow & \frac{\mathbb{I}^{\mathfrak{m}}}{(\mathbb{I}^{\mathfrak{m}})^n} & \longrightarrow & \frac{\mathbb{I}^{\mathfrak{m}}}{(\mathbb{I}^{\mathfrak{m}_1})^n \mathbb{S}_{\mathfrak{m}_1} \mathbb{I}^{S_2} \cap \mathbb{I}^{\mathfrak{m}}} \longrightarrow 1 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & 1 & & 1 & & 1
 \end{array}$$

From this the Complete Splitting Theorem follows for the special case of a Kummer extension:

15.37 Proposition. *Let $L : K$ be an n -Kummer extension of number fields and \mathfrak{p} a finite prime of K such that $\chi(\mathfrak{p}) = 1$ for all $\chi \in \mathcal{H}(L : K)$. Then \mathfrak{p} splits completely in L .*

PROOF. We use the notations of Theorem 15.36. Take $S_2 = \{\mathfrak{p}\}$. Since $\mathfrak{p} \nmid \mathfrak{f}_K(L)$ we can take S_1 and \mathfrak{m}_1 such that $\mathfrak{f}_K(L) \mid \mathfrak{m}_1$. Then

$$\mathcal{H}(L : K) \subseteq \{\chi \in {}_n\mathcal{H}_{\mathfrak{m}_1}(K) \mid \chi(\mathfrak{p}) = 1\} = X_1 = \mathcal{H}(L_1 : K)$$

and therefore $L \subseteq L_1$. By Theorem 15.36 the prime \mathfrak{p} splits completely in L_1 and hence it does so in L . \square

For infinite primes:

15.38 Proposition. *Let $L : K$ be an n -Kummer extension of number fields and \mathfrak{p} an infinite prime of K such that $\mathfrak{p} \nmid \mathfrak{f}_K(L)$. Then \mathfrak{p} does not ramify in L .*

PROOF. Similar to the proof of Theorem 15.37. Here we have

$$\mathcal{H}(L : K) \subseteq {}_n\mathcal{H}_{\mathfrak{m}_1}(K) = X_1 = \mathcal{H}(L_1 : K).$$

Again it follows that \mathfrak{p} splits completely in L , that is it does not ramify in L . \square

We generalize these two propositions to abelian number field extensions in general.

15.39 Complete Splitting Theorem. *Let $L : K$ be an abelian extension of number fields and \mathfrak{p} a finite prime of K such that $\chi(\mathfrak{p}) = 1$ for all $\chi \in \mathcal{H}(L : K)$. Then \mathfrak{p} splits completely in L .*

PROOF. By induction on $[L : K]$. If $[L : K] > 1$, there is an intermediate field K' such that $L : K'$ is of prime degree, say $[L : K'] = q$. Since $\mathcal{H}(K' : K) \subset \mathcal{H}(L : K)$, we may assume that \mathfrak{p} splits completely in K' . Let \mathfrak{p}' be any prime of K' above \mathfrak{p} . The extension $L(\zeta_q) : K'(\zeta_q)$ is a q -Kummer extension. Let \mathfrak{p}'' be a prime of $K'(\zeta_q)$ above \mathfrak{p}' . By the Translation Theorem 14.25 Dirichlet characters of $L(\zeta_q) : K'(\zeta_q)$ are of the form $\nu_{K'(\zeta_q)}^{K'}(\chi')$, where $\chi' \in \mathcal{H}(L : K')$. By the same theorem $\chi' = \nu_{K'}^K(\chi)$ for a $\chi \in \mathcal{H}(L : K)$. The value of $\nu_{K'(\zeta_q)}^{K'}(\chi')$ on \mathfrak{p}'' is trivial (put $f = f_{\mathfrak{p}'}^{(K'(\zeta_q))}$):

$$(\nu_{K'(\zeta_q)}^{K'}(\chi'))(\mathfrak{p}'') = \chi'(\mathfrak{p}')^f = (\nu_{K'}^K(\chi))(\mathfrak{p}')^f = \chi(\mathfrak{p})^f = 1.$$

By Proposition 15.37 the prime \mathfrak{p}'' splits completely in $L(\zeta_q)$. Since $[K'(\zeta_q) : K']$ is a divisor of $q - 1$, the prime \mathfrak{p}' splits completely in L . It follows that \mathfrak{p} splits completely in L . \square

For infinite primes:

15.40 Theorem. *Let $L : K$ be an abelian extension of number fields and \mathfrak{p} an infinite prime of K such that $\mathfrak{p} \nmid \mathfrak{f}_K(L)$. Then \mathfrak{p} does not ramify in L .*

PROOF. By induction on $[L : K]$. If $[L : K] > 1$, there is an intermediate field K' such that $L : K'$ is of prime degree, say $[L : K'] = q$. Since $\mathcal{H}(L : K') \subset \mathcal{H}(L : K)$, we may assume that \mathfrak{p} does not ramify in K' . If q is an odd prime, infinite primes of K' do not ramify in L . If $q = 2$, the extension $L : K'$ is a 2-Kummer extension. For \mathfrak{p}' any prime of K' above \mathfrak{p} we have $\mathfrak{p}' \nmid \mathfrak{f}_{K'}(L)$. By Proposition 15.38 the prime \mathfrak{p}' does not ramify in L . So \mathfrak{p} does not ramify in L . \square

Otherwise put: if \mathfrak{p} is an in L ramifying infinite prime of K , the prime \mathfrak{p} is a divisor of the conductor $\mathfrak{f}_K(L)$. We will see that this holds for finite primes as well. This will be shown in the next section.

15.6 Local Artin maps

In this section $L : K$ is an abelian number field extension, \mathfrak{p} a prime of K and \mathfrak{q} a prime of L above \mathfrak{p} . We fix a modulus \mathfrak{n} for $L : K$ such that $\mathfrak{p} \mid \mathfrak{n}$ and write $\mathfrak{n} = \mathfrak{p}^t \mathfrak{m}$, where $\mathfrak{p} \nmid \mathfrak{m}$.

The Artin map $\varphi_K^{(L)}$ will be used for the construction of a homomorphism

$$\vartheta_{\mathfrak{p}}^{(L)} : K_{\mathfrak{p}}^* \rightarrow Z_{\mathfrak{p}}^{(L)},$$

the *local Artin map* at the prime \mathfrak{p} . Thus we have a map $\vartheta_{\mathfrak{p}}^{(L)} : K_{\mathfrak{p}}^* \rightarrow \text{Gal}(L_{\mathfrak{q}} : K_{\mathfrak{p}})$ for the abelian extension $L_{\mathfrak{q}} : K_{\mathfrak{p}}$ of local fields. In the next chapter it will be shown that it depends only on the local field extension. Local Artin maps behave in local class field theory as Artin maps do in the global theory.

15.41 Notation. The homomorphism

$$K_m^1 \rightarrow \text{Gal}(L : K), \quad a \mapsto \begin{cases} \varphi_K^{(L)}(a\mathfrak{p}^{-v_{\mathfrak{p}}(a)})^{-1} & \text{if } \mathfrak{p} \text{ is finite,} \\ \varphi_K^{(L)}(a\mathcal{O}_K)^{-1} & \text{if } \mathfrak{p} \text{ is infinite} \end{cases}$$

is denoted by $\vartheta^{(L)}$. It is the composition of

$$i: K_m^1 \rightarrow \mathbb{I}^m(K), \quad a \mapsto a\mathcal{O}_K,$$

the projection

$$p: \mathbb{I}^m(K) \rightarrow \mathbb{I}^n(K),$$

the Artin map

$$\varphi_K^{(L)}|_n: \mathbb{I}^n(K) \rightarrow \text{Gal}(L : K)$$

and inversion in $\text{Gal}(L : K)$.

For infinite \mathfrak{p} the order of the automorphism $\vartheta^{(L)}(a)$ is at most 2; it can only be 2 for \mathfrak{p} real infinite.

15.42 Theorem. $\vartheta^{(L)}(K_m^1) = Z_{\mathfrak{p}}^{(L)}$.

PROOF. First we show that $\vartheta^{(L)}(K_m^1) \subseteq Z_{\mathfrak{p}}^{(L)}$. Let $a \in K_m^1$. Put $Z = Z_{\mathfrak{p}}^{(L)}$. The modulus \mathfrak{m} is a modulus for $L^Z : K$. Since $a\mathcal{O}_K \in \mathbb{S}_{\mathfrak{m}}(K)$ we have for infinite \mathfrak{p}

$$\vartheta^{(L)}(a)|_{L^Z} = \varphi_K^{(L)}(a\mathcal{O}_K)^{-1}|_{L^Z} = \varphi_K^{(L^Z)}(a\mathcal{O}_K)^{-1} = 1_{L^Z}$$

and for finite \mathfrak{p}

$$\vartheta^{(L)}(a)|_{L^Z} = \varphi_K^{(L)}(a\mathfrak{p}^{-v_{\mathfrak{p}}(a)})^{-1}|_{L^Z} = \varphi_K^{(L^Z)}(a\mathcal{O}_K)^{-1}\varphi_K^{(L^Z)}(\mathfrak{p})^{v_{\mathfrak{p}}(a)} = 1_{L^Z}.$$

Put $A = \vartheta^{(L)}(K_m^1)$ and consider the extension $L^A : K$. We will show that \mathfrak{p} splits completely in L^A . This will imply that $L^A \subseteq L^Z$ and hence $A = Z$.

First the case of an infinite prime \mathfrak{p} . We have to show that it does not ramify in L^A . Let $\mathfrak{a} \in \mathbb{S}_{\mathfrak{m}}(K) \cap \mathbb{I}^n(K) = \mathbb{S}_{\mathfrak{m}}(K)$, say $\mathfrak{a} = a\mathcal{O}_K$ with $a \in K_m^1$. Then

$$\varphi_K^{(L)}(\mathfrak{a})|_{L^A} = \vartheta^{(L)}(a)|_{L^A} = 1_{L^A}.$$

This holds for all $\mathfrak{a} \in \mathbb{S}_{\mathfrak{m}}(K)$, so

$$\mathbb{S}_{\mathfrak{m}}(K) \cap \mathbb{I}^n(K) \subseteq N_K^{L^A}(\mathbb{I}^n(L^A))\mathbb{S}_n(K),$$

which implies that $\mathcal{H}(L^A : K) \subseteq \mathcal{H}_{\mathfrak{m}}(K)$. In particular $\mathfrak{f}_K(L^A) | \mathfrak{m}$ and so $\mathfrak{p} \nmid \mathfrak{f}_K(L^A)$. By Theorem 15.40 the infinite prime \mathfrak{p} does not ramify in L^A .

Now let \mathfrak{p} be finite and $\mathfrak{a} \in \langle \mathfrak{p} \rangle \mathbb{S}_m(K) \cap \mathbb{I}^n(K)$, say $\mathfrak{a} = a\mathcal{O}_K \mathfrak{p}^k$ with $a \in K_m^1$. Then

$$\varphi_K^{(L)}(\mathfrak{a})|_{L^A} = \vartheta^{(L)}(a)^{-1}|_{L^A} = 1_{L^A}.$$

This holds for all $\mathfrak{a} \in \langle \mathfrak{p} \rangle \mathbb{S}_m(K) \cap \mathbb{I}^n(K)$ and hence

$$\langle \mathfrak{p} \rangle \mathbb{S}_m(K) \cap \mathbb{I}^n(K) \subseteq N_K^{L^A}(\mathbb{I}^n(L^A))\mathbb{S}_n(K),$$

which now implies that $\mathcal{H}(L^A : K) \subseteq \{\chi \in \mathcal{H}_m(K) \mid \chi(\mathfrak{p}) = 1\}$. It follows that $f_K(L^A) \mid m$ and $\chi(\mathfrak{p}) = 1$ for all $\chi \in \mathcal{H}(L^A : K)$, which by Theorem 15.39 implies that \mathfrak{p} splits completely in L^A . \square

The isomorphism $K^*/K_n^1 \xrightarrow{\sim} K^*/K_m^1 \times K^*/K_{\mathfrak{p}^t}^1$ induces an isomorphism $K_m^1/K_n^1 \xrightarrow{\sim} K^*/K_{\mathfrak{p}^t}^1$ and the inclusion $K^* \rightarrow K_{\mathfrak{p}}^*$ induces for finite \mathfrak{p} an isomorphism

$$K^*/K_{\mathfrak{p}^t}^1 \xrightarrow{\sim} K_{\mathfrak{p}}^*/(1 + \hat{\mathfrak{p}}^t),$$

and for \mathfrak{p} real infinite

$$K^*/K_{\mathfrak{p}}^1 \xrightarrow{\sim} K_{\mathfrak{p}}^*/K_{\mathfrak{p}}^+,$$

where $K_{\mathfrak{p}}^+ = \{\alpha \in K_{\mathfrak{p}}^* \mid \sigma_{\mathfrak{p}}(\alpha) > 0\}$. The composition of these two isomorphisms is an isomorphism

$$\eta: K_m^1/K_n^1 \xrightarrow{\sim} K_{\mathfrak{p}}^*/(1 + \hat{\mathfrak{p}}^t), \quad \text{respectively} \quad \eta: K_m^1/K_n^1 \xrightarrow{\sim} K_{\mathfrak{p}}^*/K_{\mathfrak{p}}^+.$$

For $a \in K_n^1$ we have $\vartheta^{(L)}(a) = \varphi_K^{(L)}(a\mathcal{O}_K)^{-1} = 1_L$, so $\vartheta^{(L)}$ induces a map $\bar{\vartheta}^{(L)}: K_m^1/K_n^1 \rightarrow Z_{\mathfrak{p}}^{(L)}$.

15.43 Definition. The composition

$$K_{\mathfrak{p}}^* \longrightarrow K_{\mathfrak{p}}^*/(1 + \hat{\mathfrak{p}}^t) \xrightarrow[\sim]{\eta^{-1}} K_m^1/K_n^1 \xrightarrow{\bar{\vartheta}^{(L)}} Z_{\mathfrak{p}}^{(L)} \quad \text{for } \mathfrak{p} \text{ finite,}$$

respectively

$$K_{\mathfrak{p}}^* \longrightarrow K_{\mathfrak{p}}^*/K_{\mathfrak{p}}^+ \xrightarrow[\sim]{\eta^{-1}} K_m^1/K_n^1 \xrightarrow{\bar{\vartheta}^{(L)}} Z_{\mathfrak{p}}^{(L)} \quad \text{for } \mathfrak{p} \text{ real infinite,}$$

is called the *local Artin map* at \mathfrak{p} and is denoted by $\vartheta_{\mathfrak{p}}^{(L)}$. It is a surjective map, because $\vartheta^{(L)}(K_m^1) = Z_{\mathfrak{p}}^{(L)}$ (Theorem 15.42).

In the construction of the map $\vartheta^{(L)}$ the modulus \mathfrak{n} has been used. The map $\vartheta^{(L)}$ is defined on K_m^1 , so its domain depends on \mathfrak{n} . It is easily seen however that $\vartheta_{\mathfrak{p}}^{(L)}$ does not depend on the choice of the modulus \mathfrak{n} (exercise 7).

If a finite prime \mathfrak{p} does not ramify in L , the decomposition group $Z_{\mathfrak{p}}^{(L)}$ is generated by $\varphi_{\mathfrak{p}}^{(L)}$, the Frobenius automorphism of \mathfrak{p} in $\text{Gal}(L : K)$. So in this case $\vartheta_{\mathfrak{p}}^{(L)}(a)$ is a power of $\varphi_{\mathfrak{p}}^{(L)}$ for each $a \in K_{\mathfrak{p}}^*$:

15.44 Proposition. *Let \mathfrak{p} be a finite prime of K which does not ramify in L . Then for each $a \in K_{\mathfrak{p}}^*$ we have*

$$\vartheta_{\mathfrak{p}}^{(L)}(a) = (\varphi_{\mathfrak{p}}^{(L)})^{v_{\mathfrak{p}}(a)}.$$

PROOF. Since \mathfrak{p} does not ramify we can choose $\mathfrak{n} = \mathfrak{m}\mathfrak{p}$ with \mathfrak{m} a modulus for $L : K$. Let $a \in K_{\mathfrak{p}}^*$. There is a $b \in K^*$ with $b \equiv a \pmod{1 + \hat{\mathfrak{p}}}$. Take $c \in K^*$ such that

$$c \equiv \begin{cases} 1 & \pmod{K_{\mathfrak{m}}^1}, \\ b & \pmod{K_{\mathfrak{p}}^1}. \end{cases}$$

Then $v_{\mathfrak{p}}(c) = v_{\mathfrak{p}}(b) = v_{\mathfrak{p}}(a)$ and $c\mathcal{O}_K \in \mathbb{S}_{\mathfrak{m}}(K)$. By the construction of $\vartheta_{\mathfrak{p}}^{(L)}$ we have

$$\vartheta_{\mathfrak{p}}^{(L)}(a) = \vartheta^{(L)}(c) = \varphi_K^{(L)}(c\mathfrak{p}^{-v_{\mathfrak{p}}(c)})^{-1} = \varphi_K^{(L)}(c\mathcal{O}_K)^{-1} \varphi_K^{(L)}(\mathfrak{p})^{v_{\mathfrak{p}}(c)} = (\varphi_{\mathfrak{p}}^{(L)})^{v_{\mathfrak{p}}(a)}. \quad \square$$

The consistency property of the (global) Artin map implies a consistency property for the local Artin map:

15.45 Proposition (Consistency property). *Let L' be an intermediate field of $L : K$ and \mathfrak{p}' the prime of L' below \mathfrak{q} . Then $\vartheta_{\mathfrak{p}'}^{(L')}(\alpha) = \vartheta_{\mathfrak{p}}^{(L)}(\alpha)|_{L'}$ for all $\alpha \in K_{\mathfrak{p}}^*$.*

PROOF. The modulus \mathfrak{n} for $L : K$ is a modulus for $L' : K$ as well. Let $a \in K_{\mathfrak{m}}^1$ and put $a\mathcal{O}_K = \mathfrak{p}^t \mathfrak{a}$ with $\mathfrak{a} \in \mathbb{I}^{\mathfrak{n}}(K)$. Then by the consistency property (Lemma 13.53)

$$\vartheta^{(L')}(\mathfrak{a}) = \varphi_K^{(L')}(\mathfrak{a})^{-1} = (\varphi_K^{(L)}(\mathfrak{a})|_{L'})^{-1} = \vartheta^{(L)}(\mathfrak{a})|_{L'}. \quad \square$$

The behavior of the local Artin map under base field extensions follows from the behavior of the global Artin map:

15.46 Proposition. *Let $K' : K$ be a number field extension, \mathfrak{q}' a prime of LK' above \mathfrak{q} and \mathfrak{p}' the prime of K' below \mathfrak{q}' . Then*

$$\vartheta_{\mathfrak{p}'}^{(LK')}(\alpha)|_L = \vartheta_{\mathfrak{p}}^{(L)}(N_{\mathfrak{p}'}^{\mathfrak{p}'}(\alpha)) \quad \text{for all } \alpha \in K_{\mathfrak{p}'}^*.$$

PROOF. The modulus \mathfrak{n} for $L : K$ is a modulus for $LK' : K'$ as well (Proposition 14.11). Let $\alpha \in K_{\mathfrak{p}'}^*$. Put $e = e_K(\mathfrak{p}')$ and $f = f_K(\mathfrak{p}')$. Choose a $\beta \in K'^*$ such that $\beta \equiv \alpha \pmod{1 + \hat{\mathfrak{p}'}^{te}}$. Choose a $\gamma \in K'^*$ such that

$$\gamma \equiv \begin{cases} 1 & \pmod{K_{\mathfrak{m}}'^1}, \\ \beta & \pmod{K_{\mathfrak{p}'te}'^1}, \\ 1 & \pmod{K_{\mathfrak{r}te(\mathfrak{r})}'^1} \quad \text{for all } \mathfrak{r} \neq \mathfrak{p}' \text{ above } \mathfrak{p} \text{ (where } e(\mathfrak{r}) = e_K(\mathfrak{r}) \text{)}. \end{cases}$$

Then $N_K^{K'}(\gamma) \in K_{\mathfrak{m}}^1$ and $N_K^{K'}(\gamma) \equiv N_K^{K'}(\beta) \pmod{K_{\mathfrak{p}te}^1}$. By definition of $\vartheta_{\mathfrak{p}}^{(L)}$ we have $\vartheta_{\mathfrak{p}}^{(L)}(N_{\mathfrak{p}'}^{\mathfrak{p}'}(\alpha)) = \vartheta^{(L)}(N_K^{K'}(\gamma))$. By construction of γ we have $\gamma\mathcal{O}_{K'} = \mathfrak{p}'^s \mathfrak{a}$

with $\mathfrak{a} \in \mathbb{I}^n(K')$ and $s \in \mathbb{Z}$. Then $N_K^{K'}(\gamma) = \mathfrak{p}^{fs} N_K^{K'}(\mathfrak{a})$ and $N_K^{K'}(\mathfrak{a}) \in \mathbb{I}^n(K)$. By definition of the local Artin map:

$$\vartheta_{\mathfrak{p}'}^{(LK')}(\alpha) = \varphi_{K'}^{(LK')}(\mathfrak{a})^{-1} \quad \text{and} \quad \vartheta_{\mathfrak{p}}^{(L)}(N_{\mathfrak{p}}^{\mathfrak{p}'}(\alpha)) = \varphi_K^{(L)}(N_K^{K'}(\mathfrak{a}))^{-1}.$$

By Lemma 13.54 $\varphi_{K'}^{(LK')}(\mathfrak{a})|_L = \varphi_K^{(L)}(N_K^{K'}(\mathfrak{a}))$ and so $\vartheta_{\mathfrak{p}'}^{(LK')}(\alpha)|_L = \vartheta_{\mathfrak{p}}^{(L)}(N_{\mathfrak{p}}^{\mathfrak{p}'}(\alpha))$. \square

15.47 Proposition. $(K_{\mathfrak{p}}^* : N_{\mathfrak{p}}^{\mathfrak{q}}(L_{\mathfrak{q}}^*)) = [L_{\mathfrak{q}} : K_{\mathfrak{p}}]$.

PROOF. If $L \neq K$, choose an intermediate field $M \neq K$ of $L : K$ such that $M : K$ is cyclic and put $\mathfrak{r} = \mathfrak{q} \cap M$. Then $N_{\mathfrak{p}}^{\mathfrak{q}} = N_{\mathfrak{p}}^{\mathfrak{r}} N_{\mathfrak{p}}^{\mathfrak{q}}$ and so the following sequence of cokernels is exact

$$M_{\mathfrak{r}}^*/N_{\mathfrak{r}}^{\mathfrak{q}}(L_{\mathfrak{q}}^*) \longrightarrow K_{\mathfrak{p}}^*/N_{\mathfrak{p}}^{\mathfrak{q}}(L_{\mathfrak{q}}^*) \longrightarrow K_{\mathfrak{p}}^*/N_{\mathfrak{p}}^{\mathfrak{r}}(M_{\mathfrak{r}}^*) \longrightarrow 1.$$

By Theorem 12.22 the order of the third group is $[M_{\mathfrak{r}} : K_{\mathfrak{p}}]$, because $M_{\mathfrak{r}} : K_{\mathfrak{p}}$ is cyclic. By induction we may assume that the order of the first group is $[L_{\mathfrak{q}} : M_{\mathfrak{r}}]$. It follows that the order of $K_{\mathfrak{p}}^*/N_{\mathfrak{p}}^{\mathfrak{q}}(L_{\mathfrak{q}}^*)$ equals $[L_{\mathfrak{q}} : K_{\mathfrak{p}}]$, because it is at least $[L_{\mathfrak{q}} : K_{\mathfrak{p}}]$. \square

15.48 Theorem. $\text{Ker}(\vartheta_{\mathfrak{p}}^{(L)}) = N_{\mathfrak{p}}^{\mathfrak{q}}(L_{\mathfrak{q}}^*)$.

PROOF. Because $\vartheta_{\mathfrak{p}}^{(L)} : K_{\mathfrak{p}}^* \rightarrow Z_{\mathfrak{p}}^{(L)}$ is surjective, $Z_{\mathfrak{p}}^{(L)} \cong \text{Gal}(L_{\mathfrak{q}} : K_{\mathfrak{p}})$ and $[K_{\mathfrak{p}}^* : N_{\mathfrak{p}}^{\mathfrak{q}}(L_{\mathfrak{q}}^*)] = [L_{\mathfrak{q}} : K_{\mathfrak{p}}]$, it suffices to show that $N_{\mathfrak{p}}^{\mathfrak{q}}(L_{\mathfrak{q}}^*) \subseteq \text{Ker}(\vartheta_{\mathfrak{p}}^{(L)})$. For this, take $K' = L$ in Proposition 15.46: for each $\alpha \in L_{\mathfrak{q}}^*$ we have $\vartheta_{\mathfrak{p}}^{(L)}(N_{\mathfrak{p}}^{\mathfrak{q}}(\alpha)) = 1$ and so $N_{\mathfrak{p}}^{\mathfrak{q}}(\alpha) \in \text{Ker}(\vartheta_{\mathfrak{p}}^{(L)})$. \square

15.49 Theorem. *Let M be an intermediate field of $L : K$ and \mathfrak{r} the prime of M below \mathfrak{q} . Then the local Artin maps induce an isomorphism of short exact sequences*

$$\begin{array}{ccccccc} 1 & \longrightarrow & M_{\mathfrak{r}}^*/N_{\mathfrak{r}}^{\mathfrak{q}}(L_{\mathfrak{q}}^*) & \xrightarrow{N_{\mathfrak{p}}^{\mathfrak{r}}} & K_{\mathfrak{p}}^*/N_{\mathfrak{p}}^{\mathfrak{q}}(L_{\mathfrak{q}}^*) & \longrightarrow & K_{\mathfrak{p}}^*/N_{\mathfrak{p}}^{\mathfrak{r}}(M_{\mathfrak{r}}^*) \longrightarrow 1 \\ & & \sim \downarrow \vartheta_{\mathfrak{r}}^{(L)} & & \sim \downarrow \vartheta_{\mathfrak{p}}^{(L)} & & \sim \downarrow \vartheta_{\mathfrak{p}}^{(M)} \\ 1 & \longrightarrow & Z_{\mathfrak{r}}^{(L)} & \xrightarrow{\subseteq} & Z_{\mathfrak{p}}^{(L)} & \xrightarrow{\cdot|_M} & Z_{\mathfrak{p}}^{(M)} \longrightarrow 1 \end{array}$$

PROOF. The vertical maps are isomorphisms by Theorem 15.48. Commutativity of the diagram follows from Proposition 15.45. \square

15.50 Lemma. *A finite prime \mathfrak{p} does not ramify in L if and only if $\mathcal{O}_{\mathfrak{p}}^* \subseteq N_{\mathfrak{p}}^q(L_q^*)$.*

PROOF. If \mathfrak{p} does not ramify, then the group $\text{Gal}(L_q : K_{\mathfrak{p}}) = Z_{\mathfrak{p}}^{(L)}$ is cyclic. By Theorem 12.23 $H^0(\mathcal{O}_{\mathfrak{q}}^*) = 1$. Let $a \in \mathcal{O}_{\mathfrak{p}}^*$. Then

$$a \in \text{Ker}(\Delta_{\mathcal{O}_{\mathfrak{q}}^*}) = \text{Im}(N_{\mathcal{O}_{\mathfrak{q}}^*}) = N_{\mathfrak{p}}^q(\mathcal{O}_{\mathfrak{q}}^*).$$

Conversely, assume $\mathcal{O}_{\mathfrak{p}}^* \subseteq N_{\mathfrak{p}}^q(L_q^*)$, put $e = e_{\mathfrak{p}}^{(L)}$ and $f = f_{\mathfrak{p}}^{(L)}$ and consider the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{O}_{\mathfrak{q}}^* & \longrightarrow & L_{\mathfrak{q}}^* & \xrightarrow{v_{\mathfrak{q}}} & \mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow N_{\mathfrak{p}}^q & & \downarrow N_{\mathfrak{p}}^q & & \downarrow f & & \\ 1 & \longrightarrow & \mathcal{O}_{\mathfrak{p}}^* & \longrightarrow & K_{\mathfrak{p}}^* & \xrightarrow{v_{\mathfrak{p}}} & \mathbb{Z} & \longrightarrow & 0 \end{array}$$

The map $N_{\mathfrak{p}}^q: \mathcal{O}_{\mathfrak{q}}^* \rightarrow \mathcal{O}_{\mathfrak{p}}^*$ is surjective: if $a \in \mathcal{O}_{\mathfrak{p}}^*$ and $a = N_{\mathfrak{p}}^q(\alpha)$ with $\alpha \in L_{\mathfrak{q}}^*$, then $0 = v_{\mathfrak{p}}(a) = v_{\mathfrak{p}}(N_{\mathfrak{p}}^q(\alpha)) = f v_{\mathfrak{q}}(\alpha)$ and so $v_{\mathfrak{q}}(\alpha) = 0$. The diagram shows that $ef = \#(K_{\mathfrak{p}}^*/N_{\mathfrak{p}}^q(L_{\mathfrak{q}}^*)) = f$. Hence $e = 1$. □

Now we can show that the prime divisors of the conductor are the ramifying primes. This generalizes this property for the base field \mathbb{Q} (Proposition 9.39).

15.51 Theorem. *If \mathfrak{p} ramifies in L , then $\mathfrak{p} \mid f_K(L)$.*

PROOF. For infinite \mathfrak{p} this is Theorem 15.40. Suppose \mathfrak{p} is finite and $\mathfrak{p} \nmid f_K(L)$. Then $\mathcal{H}(L : K) \subseteq \mathcal{H}_{\mathfrak{m}}(K)$ and so

$$\mathbb{S}_{\mathfrak{m}}(K) \cap \mathbb{I}^n(K) \subseteq N_K^L(\mathbb{I}^n(L))\mathbb{S}_{\mathfrak{n}}(L) = \text{Ker}(\varphi_K^{(L)}|_{\mathfrak{n}}).$$

It follows that $K_{\mathfrak{m}}^1 \cap K_{\{\mathfrak{p}\}}^* \subseteq \text{Ker}(\vartheta^{(L)})$. Hence by Theorem 15.48

$$\mathcal{O}_{\mathfrak{p}}^* \subseteq \text{Ker}(\vartheta_{\mathfrak{p}}^{(L)}) = N_{\mathfrak{p}}^q(L_q^*).$$

So by Lemma 15.50 \mathfrak{p} does not ramify in L . □

As a consequence of this theorem we can generalize Theorem 9.48:

15.52 Theorem. *Let $L : K$ be an abelian extension of number fields. Then*

$$\zeta_L(s) = \prod_{\chi \in \mathcal{H}(L:K)} L(s, \chi).$$

PROOF. The proof is a direct generalization of the proof of Theorem 9.48. It uses the product representations of the Dirichlet series and that a finite prime \mathfrak{p} of K ramifies in L if and only if $\chi(\mathfrak{p}) = 0$ for some $\chi \in \mathcal{H}(L : K)$. □

The following proposition identifies the exponent of finite prime divisors of the conductor.

15.53 Proposition. *Let \mathfrak{p} be finite and ramifying in L . Then $v_{\mathfrak{p}}(\mathfrak{f}_K(L)) = s$, where $s \in \mathbb{N}^*$ is the least integer with $1 + \hat{\mathfrak{p}}^s \subseteq N_{\mathfrak{p}}^{\mathfrak{q}}(L_{\mathfrak{q}}^*)$.*

PROOF. The following are equivalent:

$$\begin{aligned} & \mathfrak{p}^s \mid \mathfrak{f}_K(L), \\ & \mathcal{H}(L : K) \subseteq \mathcal{H}_{\mathfrak{p}^s \mathfrak{m}}(K), \\ & \mathbb{S}_{\mathfrak{p}^s \mathfrak{m}}(K) \subseteq N_K^L(\mathbb{I}^n(L))\mathbb{S}_n(K), \\ & \mathbb{S}_{\mathfrak{p}^s \mathfrak{m}}(K) \subseteq \text{Ker}(\varphi_K^{(L)}|_{\mathfrak{n}}), \\ & K_{\mathfrak{p}^s \mathfrak{m}}^1 \subseteq \text{Ker}(\vartheta^{(L)}), \\ & 1 + \hat{\mathfrak{p}}^s \subseteq \text{Ker}(\vartheta_{\mathfrak{p}}^{(L)}), \\ & 1 + \hat{\mathfrak{p}}^s \subseteq N_{\mathfrak{p}}^{\mathfrak{q}}(L_{\mathfrak{q}}^*). \end{aligned} \quad \square$$

So the conductor is determined locally. The following notation is useful for a characterization of the conductor.

15.54 Notation. Let $n \in \mathbb{N}$. The open subgroup $U_{\mathfrak{p}}^{(n)}$ of $K_{\mathfrak{p}}^*$ is defined by

$$U_{\mathfrak{p}}^{(n)} = \begin{cases} \mathcal{O}_{\mathfrak{p}}^* & \text{if } n = 0 \text{ and } \mathfrak{p} \text{ is finite,} \\ K_{\mathfrak{p}}^* & \text{if } n = 0 \text{ and } \mathfrak{p} \text{ is infinite,} \\ 1 + \hat{\mathfrak{p}}^n & \text{if } n > 0 \text{ and } \mathfrak{p} \text{ is finite,} \\ K_{\mathfrak{p}}^+ & \text{if } n = 1 \text{ and } \mathfrak{p} \text{ is real infinite} \\ K_{\mathfrak{p}}^* & \text{if } n = 1 \text{ and } \mathfrak{p} \text{ is complex infinite.} \end{cases}$$

15.55 Definition and notation. For \mathfrak{p} a prime of K and s the least integer such that $U_{\mathfrak{p}}^{(s)} \subseteq N_{\mathfrak{p}}^{\mathfrak{q}}(L_{\mathfrak{q}}^*)$ the modulus \mathfrak{p}^s of K is called the *local conductor* at \mathfrak{p} of $L : K$. Notation $\mathfrak{f}_{\mathfrak{p}}(L) = \mathfrak{p}^s$.

So the conductor is the product of the local conductors:

15.56 Theorem. $\mathfrak{f}_K(L) = \prod_{\mathfrak{p} \in \mathcal{P}(K)} \mathfrak{f}_{\mathfrak{p}}(L)$. □

15.7 Generalized Artin maps and the group transfer

Let $K' : K$ be a number field extension and $\chi \in \mathcal{H}(K')$. There is a modulus \mathfrak{m} of K such that, as a modulus of K' it is a multiple of the conductor of χ . The Dirichlet character χ is equivalent to a Dirichlet pre-character χ' modulo \mathfrak{m} . Then $\chi j_{K'}^K$ is a Dirichlet pre-character modulo \mathfrak{m} of K . Thus the injective map $j_{K'}^K : \mathbb{I}^+(K) \rightarrow \mathbb{I}^+(K')$ induces a homomorphism from the group of pre-characters

modulo \mathfrak{m} of K' to those of K . For Dirichlet characters we use the following notation:

15.57 Notation. Let $K' : K$ be a number field extension. The homomorphism $\mathcal{H}(K') \rightarrow \mathcal{H}(K)$ induced by injective map $j_{K'}^K : \mathbb{I}^+(K) \rightarrow \mathbb{I}^+(K')$ is denoted by $\iota_{K'}^K$.

For abelian extensions $L : K$ of number fields we have the Fundamental Equality $\#(\mathcal{H}(L : K)) = [L : K] = \#(\text{Gal}(L : K))$. The following application of the Existence Theorem tells us in particular that $\#(\mathcal{H}(L : K)) < [L : K]$ for nonabelian Galois extensions $L : K$.

15.58 Proposition. Let $L : K$ be a Galois extension of number fields, $G = \text{Gal}(L : K)$ and $X = \mathcal{H}(L : K)$. Then $K_X = L^{G'}$, or equivalently $\mathcal{H}(L : K) = \mathcal{H}(L^{G'} : K)$.

PROOF. The fields $L^{G'}$ and K_X both are intermediate fields of $L : K$ and since $K_X : K$ is abelian we have $K_X \subseteq L^{G'}$. Hence

$$X = \mathcal{H}(K_X : K) \subseteq \mathcal{H}(L^{G'} : K) \subseteq \mathcal{H}(L : K) = X$$

and so $K_X = L^{G'}$. □

For $L : K$ a Galois extension of number fields, $G = \text{Gal}(L : K)$, $\mathfrak{p} \in \text{Max}(\mathcal{O}_K)$ not ramifying in L , up to conjugation the Frobenius automorphism $\varphi_K(\mathfrak{q}) \in G$ does not depend on the choice of a $\mathfrak{q} \in \text{Max}(\mathcal{O}_L)$ above \mathfrak{p} (Proposition 7.75):

$$\varphi_K(\tau(\mathfrak{q})) = \tau\varphi_K(\mathfrak{q})\tau^{-1} \quad \text{for all } \tau \in G.$$

So in this situation we can define a generalized version of the Artin map:

15.59 Definition. The *generalized Frobenius automorphism* $\varphi_{\mathfrak{p}}^{(L)} \in G/G'$ is defined by

$$\varphi_{\mathfrak{p}}^{(L)} = \overline{\varphi_K(\mathfrak{q})},$$

where $\mathfrak{q} \in \text{Max}(\mathcal{O}_L)$ above \mathfrak{p} . (Under the isomorphism $G/G' \xrightarrow{\sim} \text{Gal}(L^{G'} : K)$ it maps to $\varphi_{\mathfrak{p}}^{(L^{G'})}$.) The prime ideals of \mathcal{O}_K which do not ramify in L form a basis of the group $\mathbb{I}^L(K)$. The *generalized Artin map* $\varphi_K^{(L)}$ is the group homomorphism determined by sending the basis elements to the generalized Frobenius automorphisms:

$$\varphi_K^{(L)} : \mathbb{I}^L(K) \rightarrow G/G', \quad \mathfrak{a} \mapsto \prod_{\mathfrak{p}|\mathfrak{a}} (\varphi_{\mathfrak{p}}^{(L)})^{v_{\mathfrak{p}}(\mathfrak{a})}.$$

By definition we have a commutative triangle

$$\begin{array}{ccc}
 & & G/G' \\
 \varphi_K^{(L)} \nearrow & & \downarrow \sim \\
 \mathbb{I}^L(K) & & \text{Gal}(L^{G'} : K) \\
 \varphi_K^{(L^{G'})} \searrow & & \\
 & &
 \end{array}$$

Let \mathfrak{f} be the conductor of $\mathcal{H}(L^{G'} : K) = \mathcal{H}(L : K)$ and \mathfrak{m} a modulus divisible by \mathfrak{f} and all in L ramifying primes of K . Then the commutative triangle induces

$$\begin{array}{ccc}
 & & G/G' \\
 \varphi_K^{(L)} \nearrow & & \downarrow \sim \\
 \mathcal{C}_m(L^{G'} : K) & & \text{Gal}(L^{G'} : K) \\
 \varphi_K^{(L^{G'})} \searrow & \sim & \\
 & &
 \end{array}$$

and subsequently

$$\begin{array}{ccc}
 & & G^\vee \\
 \check{\varphi}_K^{(L)} \nearrow & & \uparrow \sim \\
 \mathcal{H}(L : K) = \mathcal{H}(L^{G'} : K) & & \text{Gal}(L^{G'} : K)^\vee \\
 \check{\varphi}_K^{(L^{G'})} \searrow & \sim & \\
 & &
 \end{array}$$

The isomorphism $\check{\varphi}_K^{(L)}$ thus defined is determined by $\check{\varphi}_K^{(L)}(\xi)(\mathfrak{p}) = \xi(\varphi_K(\mathfrak{q}))$ for all $\xi \in G^\vee$ and all nonramifying $\mathfrak{p} \in \text{Max}(\mathcal{O}_K)$ and $\mathfrak{q} \in \text{Max}(\mathcal{O}_L)$ above \mathfrak{p} .

15.60 Definition. The map $\check{\varphi}_K^{(L)} : \text{Gal}(L : K)^\vee \xrightarrow{\sim} \mathcal{H}(L : K)$ defined above is called the *generalized dual Artin map* of the Galois extension $L : K$.

Now let $L : K$ be a Galois extension of number fields and K' an intermediate field of this extension. Put $G = \text{Gal}(L : K)$ and $H = \text{Gal}(L : K')$. The inclusion map $K \rightarrow K'$ induces an injective homomorphism of fractional ideals

$$j_{K'}^K : \mathbb{I}^L(K) \rightarrow \mathbb{I}^L(K'), \quad \mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_{K'}.$$

We will show that there is a homomorphism $V_H^G: G/G' \rightarrow H/H'$, depending only on the group G and the subgroup H of G , which is via the generalized Artin maps compatible with $j_{K'}^K$ (Theorem 15.63). This group homomorphism is well-known in group theory. It is known as the transfer from G to H .

First we define this group transfer. Let G be a group and H a subgroup of finite index n in G . The group G acts from the right on the set of right cosets of H in G :

$$(H\tau) \cdot \sigma = H\tau\sigma.$$

Let T be a set of representatives of the right cosets. For $\tau \in T$ and $\sigma \in G$ there is a unique $\tau_\sigma \in T$ such that $H\tau\sigma = H\tau_\sigma$. Thus the action of G on the right cosets induces a right action of G on the set T :

$$\tau \cdot \sigma = \tau_\sigma.$$

Since $H\tau\sigma = H\tau_\sigma$, we have $\tau\sigma\tau_\sigma^{-1} \in H$.

15.61 Lemma. *The map*

$$G \rightarrow H/H', \quad \sigma \mapsto \prod_{\tau \in T} \overline{\tau\sigma\tau_\sigma^{-1}}$$

is a group homomorphism and does not depend on the system T of representatives of the right cosets of H in G .

PROOF. Let also R be a system of representatives of the right cosets. For each $\rho \in R$ there is a unique $\tau \in T$ such that $H\rho = H\tau$. So we have a bijection $f: R \rightarrow T$ given by $H\rho = Hf(\rho)$. Let $\sigma \in G$. For each ρ it follows from

$$Hf(\rho_\sigma) = H\rho_\sigma = H\rho\sigma = Hf(\rho)\sigma = Hf(\rho)_\sigma$$

that $f(\rho_\sigma) = f(\rho)_\sigma$. Modulo H' we have

$$\begin{aligned} \prod_{\tau \in T} \tau\sigma\tau_\sigma^{-1} &\equiv \prod_{\rho \in R} f(\rho)\sigma f(\rho)_\sigma^{-1} = \prod_{\rho \in R} f(\rho)\rho^{-1}\rho\sigma\rho_\sigma^{-1}\rho_\sigma f(\rho)_\sigma^{-1} \\ &\equiv \left(\prod_{\rho \in R} f(\rho)\rho^{-1} \right) \left(\prod_{\rho \in R} \rho\sigma\rho_\sigma^{-1} \right) \left(\prod_{\rho \in R} \rho_\sigma f(\rho_\sigma)^{-1} \right) \equiv \prod_{\rho \in R} \rho\sigma\rho_\sigma^{-1}. \end{aligned}$$

The products in these formulas are well defined because modulo H' the group is abelian. For the last congruence above the equality $\{\rho_\sigma \mid \rho \in R\} = R$ is used. Hence the map does not depend on the choice of the representatives. Let $\sigma_1, \sigma_2 \in G$. For each $\tau \in T$

$$H\tau_{\sigma_1\sigma_2} = H\tau\sigma_1\sigma_2 = H\tau_{\sigma_1}\sigma_2 = H(\tau_{\sigma_1})_{\sigma_2}$$

and so $\tau_{\sigma_1\sigma_2} = (\tau_{\sigma_1})_{\sigma_2}$. Then from

$$\prod_{\tau \in T} \tau\sigma_1\sigma_2\tau_{\sigma_1\sigma_2}^{-1} = \prod_{\tau \in T} \tau\sigma_1\tau_{\sigma_1}^{-1}\tau_{\sigma_1}\sigma_2(\tau_{\sigma_1})_{\sigma_2}^{-1} \equiv \left(\prod_{\tau \in T} \tau\sigma_1\tau_{\sigma_1}^{-1} \right) \left(\prod_{\tau \in T} \tau_{\sigma_1}\sigma_2(\tau_{\sigma_1})_{\sigma_2}^{-1} \right)$$

$$\equiv \left(\prod_{\tau \in T} \tau \sigma_1 \tau_{\sigma_1}^{-1} \right) \left(\prod_{\tau \in T} \tau \sigma_2 \tau_{\sigma_2}^{-1} \right)$$

follows that the map is a group homomorphism. □

This lemma justifies the following definition.

15.62 Definition. Let G be a group, H a subgroup of G of finite index and T a set of representatives of the right cosets of H in G . The homomorphism

$$V_H^G : G/G' \rightarrow H/H', \quad \bar{\sigma} \mapsto \prod_{\tau \in T} \overline{\tau \sigma \tau_{\sigma}^{-1}}$$

is called the *transfer* from G to H . (Verlagerung is German for transfer.)

15.63 Proposition. Let $L : K$ be a Galois extension of number fields, K' an intermediate field of $L : K$, $G = \text{Gal}(L : K)$ and $H = \text{Gal}(L : K')$. Then the following diagram commutes:

$$\begin{array}{ccc} \mathbb{I}^L(K') & \xrightarrow{\varphi_{K'}^{(L)}} & H/H' \\ \uparrow j_{K'}^K & & \uparrow V_H^G \\ \mathbb{I}^L(K) & \xrightarrow{\varphi_K^{(L)}} & G/G' \end{array}$$

PROOF. Let $\mathfrak{p} \in \text{Max}(\mathcal{O}_K)$ be such that \mathfrak{p} does not ramify in L and let $\mathfrak{q} \in \text{Max}(\mathcal{O}_L)$ be above \mathfrak{p} . Put $\sigma = \varphi_K^{(L)}(\mathfrak{q})$. Then $\varphi_{K'}^{(L)}(\mathfrak{p}) = \bar{\sigma}$ and $j_{K'}^K(\mathfrak{p}) = \mathfrak{p}\mathcal{O}_{K'}$. We have to prove that $\varphi_{K'}^{(L)}(\mathfrak{p}\mathcal{O}_{K'}) = V_H^G(\bar{\sigma})$. Theorem 7.53 describes the prime ideals of $\mathcal{O}_{K'}$ above \mathfrak{p} . The group $Z = Z_K(\mathfrak{q}) = \langle \sigma \rangle$ acts from the right on the set of right cosets of H in G . Let r be the number of orbits of this action and $H\tau_1, \dots, H\tau_r$ a system of representatives of these orbits. Then the prime ideal factorization of $\mathfrak{p}\mathcal{O}_{K'}$ is

$$\mathfrak{p}\mathcal{O}_{K'} = (\tau_1(\mathfrak{q}) \cap K') \cdots (\tau_r(\mathfrak{q}) \cap K')$$

and $f_K(\tau_j(\mathfrak{q}) \cap K') = \#([H\tau_j])$. Put $f_j = \#([H\tau_j])$. Then

$$\begin{aligned} \varphi_{K'}^{(L)}(\mathfrak{p}\mathcal{O}_{K'}) &= \prod_{j=1}^r \overline{\varphi_{K'}^{(L)}(\tau_j(\mathfrak{q}) \cap K')} = \prod_{j=1}^r \overline{(\varphi_K^{(L)}(\tau_j(\mathfrak{q}))^{f_j}} = \prod_{j=1}^r \overline{(\tau_j \sigma \tau_j^{-1})^{f_j}} \\ &= \prod_{j=1}^r \overline{\tau_j \sigma^{f_j} \tau_j^{-1}}. \end{aligned}$$

The collection of right cosets of H in G is the union of the r orbits under the action of Z . The orbits are:

$$\begin{array}{ccccccc} H\tau_1, & H\tau_1\sigma, & \dots, & H\tau_1\sigma^{f_1-1} \\ H\tau_2, & H\tau_2\sigma, & \dots, & H\tau_1\sigma^{f_2-1} \\ & & \vdots & \\ H\tau_r, & H\tau_r\sigma, & \dots, & H\tau_r\sigma^{f_r-1}. \end{array}$$

The $\tau_j\sigma^i$ with $1 \leq j \leq r$ and $0 \leq i \leq f_j - 1$ form a system of representatives of the right cosets of H . For $0 \leq i \leq f_j - 2$ the representative $\tau_j\sigma^i$ maps under right multiplication by σ to the representative $\tau_j\sigma^{i+1}$, so for these representatives there is no contribution to the product that defines the transfer of σ . Therefore,

$$V_H^G(\bar{\sigma}) = \prod_{j=1}^r \overline{(\tau_j\sigma^{f_j-1}\sigma)\tau_j^{-1}} = \prod_{j=1}^r \overline{\tau_j\sigma^{f_j}\tau_j^{-1}}. \quad \square$$

It follows that for the generalized dual Artin maps we have:

15.64 Theorem. *In the notation of Proposition 15.63: the following square is commutative:*

$$\begin{array}{ccc} H^\vee & \xrightarrow[\sim]{\check{\varphi}_{K'}^{(L)}} & \mathcal{H}(L : K') \\ (V_H^G)^\vee \downarrow & & \downarrow \iota_K^{K'} \\ G^\vee & \xrightarrow[\sim]{\check{\varphi}_K^{(L)}} & \mathcal{H}(L : K) \end{array} \quad \square$$

The homomorphism $\iota_K^{K'}$ is determined by

$$\iota_K^{K'}(\chi)(\mathfrak{p}) = \chi(\mathfrak{p}\mathcal{O}_{K'})$$

for all $\chi \in \mathcal{H}(L : K')$ and all $\mathfrak{p} \in \text{Max}(\mathcal{O}_K)$ which do not ramify in L . It is a map from a finite subgroup of $\mathcal{H}(K')$ to $\mathcal{H}(K)$. For a given $\chi \in \mathcal{H}(K')$, one can take $L : K$ to be the normal closure of $K'_\chi : K$, where K'_χ is the class field for $\langle \chi \rangle$ over K' . Then $\chi \in \langle \chi \rangle = \mathcal{H}(K'_\chi : K') \subseteq \mathcal{H}(L : K')$. So the map $\iota_K^{K'} : \mathcal{H}(K') \rightarrow \mathcal{H}(K)$ is via the generalized dual Artin maps closely related to normal extensions $L : K$ having K' as an intermediate field.

15.8 The Hilbert class field

Let K be a number field. Unramified abelian extensions $L : K$ are the extensions having the trivial modulus (1) as conductor. By the Classification Theorem the maximal one among these corresponds to $\mathcal{H}_{(1)}(K)$ and via Artin's Reciprocity Theorem to the ideal class group of K .

15.65 Definition. Let K be a number field. The ray class field for $\mathcal{H}_{(1)}(K)$ is called the *Hilbert class field* of K .

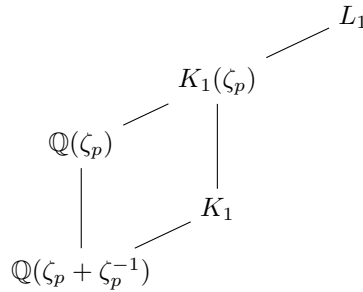
Thus, if K_1 is the Hilbert class field of K , we have isomorphisms

$$\varphi_K^{(K_1)} : \mathcal{C}(K) \xrightarrow{\sim} \text{Gal}(K_1 : K) \quad \text{and} \quad \check{\varphi}_K^{(K_1)} : \text{Gal}(K_1 : K)^\vee \xrightarrow{\sim} \mathcal{H}_{(1)}(K).$$

The following proposition illustrates the use of the existence of Hilbert class fields.

15.66 Proposition. *Let p be an odd prime. The group $\mathcal{C}(\mathbb{Q}(\zeta_p + \zeta_p^{-1}))$ is a homomorphic image of $\mathcal{C}(\mathbb{Q}(\zeta_p))$. In particular $h_p^+ \mid h_p$.*

PROOF. Put $K = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$. Let K_1 be the Hilbert class field of K and \mathfrak{p} the prime of K above p . Then \mathfrak{p} does not ramify in K_1 and totally ramifies in $\mathbb{Q}(\zeta_p) = K(\zeta_p)$. It follows that $K(\zeta_p) \cap K_1 = K$ and that $K_1(\zeta_p) : K(\zeta_p)$ is an unramified abelian extension with $\text{Gal}(K_1(\zeta_p) : K(\zeta_p)) \cong \text{Gal}(K_1 : K) \cong \mathcal{C}(K)$. Let L_1 be the Hilbert class field of $K(\zeta_p)$. Then $K_1(\zeta_p)$ is an intermediate field of $L_1 : K(\zeta_p)$. So $\mathcal{C}(K)$ is a homomorphic image of $\mathcal{C}(K(\zeta_p))$. \square



Using the transfer map for ideal class groups it is clear that the odd part of $\mathcal{C}(\mathbb{Q}(\zeta_p + \zeta_p^{-1}))$ is a homomorphic image of the odd part of $\mathcal{C}(\mathbb{Q}(\zeta_p))$. So the extra information given by this proposition concerns the 2-primary parts of these groups.

The action of a Galois group on the ideal class group translates into an extension of Galois groups:

15.67 Proposition. *Let $K : K_0$ be a Galois extension of number fields and K_1 the Hilbert class field of K . Then $K_1 : K_0$ is a Galois extension. The action of $\text{Gal}(K : K_0)$ on $\text{Gal}(K_1 : K_0)$ is via $\varphi_K^{(K_1)}$ compatible with the action on $\mathcal{C}(K)$.*

PROOF. This follows directly from Proposition 15.6: for each $\tau \in \text{Gal}(K : K_0)$ we have $\tau^*(\mathcal{H}_{(1)}(K)) = \mathcal{H}_{(1)}(K)$. \square

The strength of the Classification Theorem is illustrated by the following computation of the 2-rank of the ideal class groups of quadratic number fields. A much more elementary computation was given in chapter 4. Another proof, using more algebraic number theory, but no class field theory, is in the exercises 8 and 9 of chapter 12.

15.68 Application. Let K be a quadratic number field, τ its nontrivial automorphism and K_1 its Hilbert class field. Unramified quadratic extensions of K correspond to elements of order 2 in $\mathcal{H}_{(1)}(K)$. The 2-rank of $\mathcal{C}(K)$ is equal to the 2-rank of $\mathcal{H}_{(1)}(K)$. By Proposition 15.67 $K_1 : \mathbb{Q}$ is a Galois extension. The action of τ on $\mathcal{H}_{(1)}(K)$ is by inversion, so for each unramified quadratic extension $L : K$ we have $\tau^*(\mathcal{H}(L : K)) = \mathcal{H}(L : K)$ and, as a consequence, the extension $L : \mathbb{Q}$ is abelian. Since a prime number dividing $\text{disc}(K)$ ramifies in such L , the groups $\text{Gal}(L : K)$ and the inertia group of this prime number are different subgroups of order 2 of $\text{Gal}(L : \mathbb{Q})$. On the other hand each prime number which ramifies in K also ramifies in exactly one of the two other quadratic number fields contained in L . Prime numbers which do not ramify in K , do not ramify in the other subfields as well. Put $D = \text{disc}(K)$ and

$$D = u \cdot \prod_{p|D \text{ odd}} p^*,$$

where the product is over the odd prime divisors of D and $u \in \{1, -4, 8, -8\}$. Consider the set

$$P = \begin{cases} \{p^* \mid p \text{ odd prime divisor of } D\} & \text{if } u = 1, \\ \{p^* \mid p \text{ odd prime divisor of } D\} \cup \{u\} & \text{if } u \neq 1. \end{cases}$$

Set $r = \#(P)$ and let s be the number of negative elements of P . The quadratic field is real if and only if s is even. If either s is odd or $s = 0$, then the number of unramified quadratic extensions of K is equal to the number of bipartitions of P . In this case $\#(\mathcal{H}_{(1)}(K)) = 2^{r-1}$, that is the 2-rank of $\mathcal{C}(K)$ is $r - 1$. For s even and $s > 0$ the number of unramified quadratic extensions of K is equal to the number of bipartitions of P into two subsets, both containing an even number of negative elements. In this special case the 2-rank of $\mathcal{C}(K)$ is $r - 2$.

The Principal Ideal Theorem

Let K_1 be the Hilbert class field of the number field K . The Principal Ideal Theorem (Theorem 15.74) states that for every ideal \mathfrak{a} of \mathcal{O}_K the induced ideal $j_{K_1}^K(\mathfrak{a}) = \mathfrak{a}\mathcal{O}_{K_1}$ is a principal ideal. Alternatively: the homomorphism

$$j_{K_1}^K : \mathcal{C}(K) \rightarrow \mathcal{C}(K_1)$$

is trivial. Let K_2 be the Hilbert class field of K_1 .

15.69 Proposition. *The extension $K_2 : K$ is a Galois extension and $K_2^{G'} = K_1$, where $G = \text{Gal}(K_2 : K)$.*

PROOF. By Proposition 15.67 $K_2 : K$ is a Galois extension. The extension $K_2 : K$ is unramified and hence $K_2^{G'} : K$ is both abelian and unramified. So $K_2^{G'} \subseteq K_1$, that is $G' \supseteq \text{Gal}(K_2 : K_1)$. Because $K_1 : K$ is abelian, we also have $\text{Gal}(K_2 : K_1) \supseteq G'$. \square

By Theorem 15.64 and Proposition 15.58 we have a commutative square

$$\begin{array}{ccc}
 (G')^\vee & \xrightarrow[\sim]{\check{\varphi}_{K_1}^{(K_2)}} & \mathcal{H}(K_2 : K_1) = \mathcal{H}_1(K_1) \\
 \downarrow (V_{G'}^G)^\vee & & \downarrow \iota_K^{K_1} \\
 G^\vee & \xrightarrow[\sim]{\check{\varphi}_K^{(K_2)}} & \mathcal{H}(K_2 : K) = \mathcal{H}(K_2^{G'} : K) = \mathcal{H}(K_1 : K) = \mathcal{H}_1(K)
 \end{array}$$

Thus the Principal Ideal Theorem is translated into pure group theory: the transfer $V_{G'}^G : G/G' \rightarrow G'/G''$ has to be the trivial homomorphism.

We will show that indeed the transfer from a finite group to its commutator subgroup is trivial (Theorem 15.73). In the remaining part of this section G is a finite group. We will use the group ring $\mathbb{Z}[G]$ and its augmentation ideal $I(G) = \text{Ker}(\mathbb{Z}[G] \rightarrow \mathbb{Z})$.

15.70 Lemma. *The map $\delta : G \rightarrow I(G)$, $\sigma \mapsto \sigma - 1$ induces an isomorphism $\delta_* : G/G' \xrightarrow{\sim} I(G)/I(G)^2$.*

PROOF. The identity

$$\sigma_1 \sigma_2 - 1 = (\sigma_1 - 1) + (\sigma_2 - 1) + (\sigma_1 - 1)(\sigma_2 - 1) \tag{15.2}$$

in $I(G)$ shows that δ induces a homomorphism $G \rightarrow I(G)/I(G)^2$ and since $I(G)/I(G)^2$ is abelian, we have a homomorphism

$$\delta_* : G/G' \rightarrow I(G)/I(G)^2, \quad \bar{\sigma} \mapsto \overline{\sigma - 1},$$

where $\bar{\sigma}$ denotes the coset $G'\sigma$ and $\overline{\sigma - 1}$ the residue class of $\sigma - 1$ modulo $I(G)^2$. The set G is a \mathbb{Z} -basis of $\mathbb{Z}[G]$ and so $\{\sigma - 1 \mid \sigma \in G \setminus \{1\}\}$ is a \mathbb{Z} -basis of $I(G)$. Clearly δ_* is surjective and by identity (15.2) the homomorphism $I(G) \rightarrow G/G'$ determined by $\sigma - 1 \mapsto \bar{\sigma}$ induces an inverse. \square

Now let H be a subgroup of G and R a set of representatives of the right cosets of H in G such that $1 \in R$.

15.71 Lemma. *The inclusion map $I(H) \rightarrow I(H) + I(H)I(G)$ induces an isomorphism*

$$I(H)/I(H)^2 \xrightarrow{\sim} (I(H) + I(H)I(G))/I(H)I(G).$$

PROOF. First we show that

$$\{(\tau - 1)\rho \mid \tau \in H \setminus \{1\}, \rho \in R\}$$

is a \mathbb{Z} -basis of $I(H) + I(H)I(G)$. From $1 \in R$ and the identity

$$(\tau - 1)\rho = (\tau - 1) + (\tau - 1)(\rho - 1)$$

follows that the elements $(\tau - 1)\rho$ are in $I(H) + I(H)I(G)$. They generate it as a \mathbb{Z} -module:

$$(\tau_1 - 1)(\tau_2\rho - 1) = (\tau_1\tau_2 - 1)\rho - (\tau_2 - 1)\rho - (\tau_1 - 1). \quad (15.3)$$

Classes of $I(H) + I(H)I(G)$ modulo $I(H)I(G)$ are represented by elements of $I(H)$. So we have a surjective homomorphism

$$I(H)/I(H)^2 \longrightarrow (I(H) + I(H)I(G))/I(H)I(G)$$

and from identity (15.3) follows that the homomorphism $I(H) + I(H)I(G) \rightarrow I(H)$, $(\tau - 1)\rho \mapsto \tau - 1$ induces an inverse:

$$\begin{aligned} (\tau_1 - 1)(\tau_2\rho - 1) &\mapsto (\tau_1\tau_2 - 1) - (\tau_2 - 1) - (\tau_1 - 1) \\ &= (\tau_1 - 1)(\tau_2 - 1) \in I(H)^2. \end{aligned} \quad \square$$

The transfer translates via the isomorphisms given by the lemmas into a homomorphism $f: I(H)/I(H)^2 \rightarrow (I(H) + I(H)I(G))/I(H)I(G)$:

$$\begin{array}{ccc} G/G' & \xrightarrow{V_H^G} & H/H' \\ \downarrow \sim & & \downarrow \sim \\ & & I(H)/I(H)^2 \\ & & \downarrow \sim \\ I(G)/I(G)^2 & \xrightarrow{f} & (I(H) + I(H)I(G))/I(H)I(G) \end{array}$$

The transfer is given by $V_H^G(\bar{\sigma}) = \prod_{\rho \in R} \overline{\rho\sigma\rho\sigma^{-1}}$ and so

$$f(\overline{\sigma - 1}) = \sum_{\rho \in R} \overline{\rho\sigma\rho\sigma^{-1}} - 1.$$

Modulo $I(H)I(G)$ we have

$$\begin{aligned} \sum_{\rho \in R} (\rho\sigma\rho_\sigma^{-1} - 1) &\equiv \sum_{\rho \in R} (\rho\sigma\rho_\sigma^{-1} - 1)\rho_\sigma = \sum_{\rho \in R} \rho\sigma - \sum_{\rho \in R} \rho_\sigma = \sum_{\rho \in R} \rho\sigma - \sum_{\rho \in R} \rho \\ &\equiv \sum_{\rho \in R} \rho(\sigma - 1). \end{aligned}$$

Hence:

15.72 Proposition. *The homomorphism f in the commutative diagram above is given by*

$$f(\overline{\sigma - 1}) = \overline{\sum_{\rho \in R} \rho(\sigma - 1)}. \quad \square$$

15.73 Theorem. *The transfer $V_{G'}^G: G/G' \rightarrow G'/G''$ is the trivial homomorphism.*

PROOF. Let $\sigma_1, \dots, \sigma_n$ generate the group G . Then the homomorphism $\mathbb{Z}^n \rightarrow G/G'$ given by $e_i \mapsto \overline{\sigma_i}$ for $i = 1, \dots, n$ is surjective and we have a short exact sequence

$$0 \longrightarrow \mathbb{Z}^n \xrightarrow{(m_{ik})} \mathbb{Z}^n \longrightarrow G/G' \longrightarrow 1,$$

where the (m_{ik}) stands for left multiplication by a matrix $(m_{ik}) \in M_n(\mathbb{Z})$. Then $\det(m_{ik}) = \pm \#(G/G')$ and by replacing one of the generators by its inverse we can assume that $\det(m_{ik}) = \#(G/G')$. Then for $k = 1, \dots, n$:

$$\prod_{i=1}^n \sigma_i^{m_{ik}} = \tau_k \in G'.$$

From the identities

$$\begin{aligned} \sigma_1\sigma_2 - 1 &= (\sigma_1 - 1) + \sigma_1(\sigma_2 - 1) \\ \sigma^{-1} - 1 &= -\sigma^{-1}(\sigma - 1) \end{aligned}$$

follows that in $\mathbb{Z}[G]$

$$\left(\prod_{i=1}^n \sigma_i^{m_{ik}} \right) - 1 = \sum_{i=1}^n \mu_{ik}(\sigma_i - 1)$$

with $\mu_{ik} \equiv m_{ik} \pmod{I(G)}$ and since $\tau_k \in G'$

$$\tau_k - 1 = \sum_{i=1}^n \alpha_{ik}(\sigma_i - 1)$$

with $\alpha_{ik} \equiv 0 \pmod{I(G)}$. So we can assume that

$$\left(\prod_{i=1}^n \sigma_i^{m_{ik}} \right) - 1 = \sum_{i=1}^n \mu_{ik}(\sigma_i - 1) = 0$$

with $\mu_{ik} \equiv m_{ik} \pmod{I(G)}$. The group ring $\mathbb{Z}[G/G']$ is commutative and $G \rightarrow G/G'$ induces an isomorphism $\mathbb{Z}[G]/I(G')\mathbb{Z}[G]$. Let $(\lambda_{kj}) \in M_n(\mathbb{Z}[G])$ be such that $(\overline{\lambda_{kj}}) \in M_n(\mathbb{Z}[G]/I(G')\mathbb{Z}[G])$ is the adjoint matrix of $(\overline{\mu_{ik}})$ and let $\mu \in \mathbb{Z}[G]$ be such that $\det(\overline{\mu_{ik}}) = \overline{\mu} \in \mathbb{Z}[G]/I(G')\mathbb{Z}[G]$. The transpose of the adjoint is the adjoint of the transpose:

$$\sum_{k=1}^n \lambda_{kj} \mu_{ik} \equiv \begin{cases} \mu & \pmod{I(G')\mathbb{Z}[G]} \text{ if } i = j, \\ 0 & \pmod{I(G')\mathbb{Z}[G]} \text{ otherwise.} \end{cases}$$

Then for $j = 1, \dots, n$

$$\mu(\sigma_j - 1) = \sum_{i,k} \lambda_{kj} \mu_{ik} (\sigma_i - 1) \equiv 0 \pmod{I(G')I(G)}$$

and so $\mu(\sigma - 1) \equiv 0 \pmod{I(G')I(G)}$ for all $\sigma \in G$. The element $\overline{\mu} \in \mathbb{Z}[G/G']$ is invariant under right multiplication by elements of G/G' and therefore $\overline{\mu} = a \sum_{\rho \in R} \overline{\rho} \in \mathbb{Z}[G/G']$ for an $a \in \mathbb{Z}$. Application of the augmentation $\varepsilon: \mathbb{Z}[G/G'] \rightarrow \mathbb{Z}$ yields

$$\varepsilon(\overline{\mu}) = a \cdot \#(R) = a \cdot [G : G'].$$

By definition of μ we also have

$$\overline{\mu} = \det(\overline{\mu_{ik}}) \equiv \det(m_{ik}) = [G : G'] \pmod{I(G)}.$$

Hence $a = 1$ and so by Proposition 15.73 with $H = G'$ for every $\sigma \in G$:

$$f(\overline{\sigma - 1}) = \overline{\sum_{\rho \in R} \rho(\sigma - 1)} = \overline{\mu(\sigma - 1)} = 0.$$

So f is the zero map. □

As remarked above this implies the main result of this section:

15.74 Principal Ideal Theorem. *For every number field K and every ideal \mathfrak{a} of \mathcal{O}_K , the ideal $\mathfrak{a}\mathcal{O}_{K_1}$ of the ring of integers of the Hilbert class field K_1 of K is a principal ideal.* □

Starting with a number field K one can form the *class field tower*

$$K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \dots \subseteq K_n \subseteq K_{n+1} \subseteq \dots, \tag{15.4}$$

in which each field is followed by its Hilbert class field. Philipp Furtwängler posed the question whether this tower stabilizes: is there an n such that $K_{n+1} = K_n$? For such n all ideals of \mathcal{O}_{K_n} are principal, not only those coming from K . In 1964 Golod and Shafarevich showed (in [13]) that the tower does not stabilize for number fields K in which sufficiently many prime numbers ramify.

EXERCISES

- Show that $\mathbb{Q}(i, \sqrt{5})$ is the Hilbert class field of $\mathbb{Q}(\sqrt{-5})$.
- The extension $\mathbb{Q}(\sqrt{7}, i) : \mathbb{Q}(\sqrt{7})$ corresponds to a group of Dirichlet characters of $\mathbb{Q}(\sqrt{7})$ of order 2. Determine the quadratic Dirichlet character in this group.
- Let $K = \mathbb{Q}(\sqrt[3]{7})$, $\vartheta = \zeta_7 + \zeta_7^{-1}$ and $L = \mathbb{Q}(\vartheta)$.
 - Show that 7 totally ramifies in both K and L .
 - Let \mathfrak{p} and \mathfrak{q} be the unique primes of respectively K and L above 7. Show that $K_{\mathfrak{p}} : \mathbb{Q}_7$ and $L_{\mathfrak{q}} : \mathbb{Q}_7$ are 3-Kummer extensions.
 - Prove that $K_{\mathfrak{p}} = L_{\mathfrak{q}}$. (Hint: use $\mathfrak{q} = (\vartheta - 2)$ and $\mathfrak{q}^3 = (7)$.)
 - Show that $K(\vartheta)$ is the Hilbert class field of K . (See exercise 4 of chapter 14 and Example 5.22.)
- Compute $\mathbb{Q}_7^*/\mathbb{Q}_7^{*3}$.
 - How many Galois extensions $K : \mathbb{Q}_7$ of degree 3 are there? For each of them give an $\alpha \in K$ such that $K = \mathbb{Q}_7(\alpha)$ and $\alpha^3 \in \mathbb{Q}_7$.
- Determine the number of Galois extensions $K : \mathbb{Q}_7$ of degree 5.
- Let $\alpha \in \mathbb{R}$ such that $\alpha^3 = \alpha + 1$. As remarked in Example 13.56 the field $\mathbb{Q}(\alpha, \sqrt{-23})$ is the Hilbert class field of $\mathbb{Q}(\sqrt{-23})$. Show that 2 splits in $\mathbb{Q}(\alpha, \sqrt{-23})$ as the product of two principal prime ideals.
- Show that the local Artin map $\vartheta_{\mathfrak{p}}^{(L)}$ does not depend on the choice of the modulus \mathfrak{n} used in its construction.
- Show that the extensions $K_n : K$ in the class field tower (15.4) are Galois extensions.
- ([9], Theorem 1) Let K_1 and K_2 be number fields with $\text{disc}(K_1)$ and $\text{disc}(K_2)$ relatively prime. Suppose that $K_1 : \mathbb{Q}$ and $K_2 : \mathbb{Q}$ are Galois extensions.
 - Prove that the map

$$(\text{tr}_{K_1}^{K_1 K_2}, \text{tr}_{K_2}^{K_1 K_2}) : \mathcal{C}\ell(K_1 K_2) \longrightarrow \mathcal{C}\ell(K_1) \times \mathcal{C}\ell(K_2)$$

is surjective. (Hint: look at the Hilbert class fields of K_1 and K_2 .)

- Let $m_1, m_2 \in \mathbb{N}^*$ be relatively prime and put $m = m_1 m_2$. Show that the ideal class group of $\mathbb{Q}(\zeta_m)$ contains a subgroup isomorphic to the product of the ideal class groups of $\mathbb{Q}(\zeta_{m_1})$ and $\mathbb{Q}(\zeta_{m_2})$.
- ([9], Theorem 2) Let K be a complex biquadratic field and let K_1, K_2 and K_3 be its quadratic subfields, say K_1 is the real quadratic subfield. Assume that $\text{gcd}(\text{disc}(K_1), \text{disc}(K_2)) = 1$. Set $H = \text{Gal}(K : K_3)$. Prove that the following sequence is exact

$$1 \longrightarrow \mathcal{C}\ell(K)^H \longrightarrow \mathcal{C}\ell(K_1) \times \mathcal{C}\ell(K_2) \xrightarrow{(\text{tr}_{K_1}^K, \text{tr}_{K_2}^K)} \mathcal{C}\ell(K) \longrightarrow 1$$

15 *The Classification Theorem*

and that the Hasse index of K equals 1. (Hints: exercise 9, Example 9.57 and exercise 5 of chapter 14)

16 Local Class Fields and Symbols

Classical reciprocity laws involve power residue symbols such as the Legendre symbol in the quadratic case for \mathbb{Q} . Reciprocity laws for power residue symbols can be obtained from product formulas for Hilbert symbols. In section 16.3 Hilbert symbols are treated and in the last section some classical reciprocity laws are derived.

Hilbert symbols are based on the local Artin maps for Kummer extensions. Local Artin maps have been defined in section 15.6. In section 16.1 it is shown that they depend only on the extension of the local fields. Their role in local class field theory is similar to the role of Artin maps in global class field theory (see Theorem 16.15). Local Artin maps can be interpreted as norm residue symbols and in section 16.2 it is shown that for a given abelian extension of number fields their product over all primes of the base field is trivial (Theorem 16.22). The product formula for Hilbert symbols is a consequence of this.

16.1 Local class fields

In this section we fix a prime number p . In section 15.6 the local Artin map

$$\vartheta_{\mathfrak{p}}^{(L)} : K_{\mathfrak{p}}^* \rightarrow Z_{\mathfrak{p}}^{(L)}$$

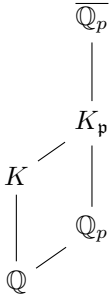
has been constructed for an abelian number field extension $L : K$ and a prime \mathfrak{p} of K above p . For a prime \mathfrak{q} of L above \mathfrak{p} we have

$$\text{Gal}(L_{\mathfrak{q}} : K_{\mathfrak{p}}) \xrightarrow{\sim} Z_K(\mathfrak{q}) = Z_{\mathfrak{p}}^{(L)},$$

where the map is the restriction of automorphisms of $L_{\mathfrak{q}}$ to L . Via this isomorphism we have a map

$$\vartheta_{\mathfrak{p}}^{(L)} : K_{\mathfrak{p}}^* \rightarrow \text{Gal}(L_{\mathfrak{q}} : K_{\mathfrak{p}}),$$

also denoted by $\vartheta_{\mathfrak{p}}^{(L)}$, for the abelian extension $L_{\mathfrak{q}} : K_{\mathfrak{p}}$ of local fields. For its construction the number field extension $L : K$ has been used. First we will show that each finite abelian extension of local fields is of this type and that the map does not depend on the choice of the number field extension.



Let's fix an algebraic closure $\overline{\mathbb{Q}_p}$ of \mathbb{Q}_p . For a number field K and a prime \mathfrak{p} above p , we can assume that the completion $K_{\mathfrak{p}}$ has \mathbb{Q}_p as a subfield. The extension $K_{\mathfrak{p}} : \mathbb{Q}_p$ is finite, so we can also assume that $K_{\mathfrak{p}}$ is contained in $\overline{\mathbb{Q}_p}$.

In this section all number fields are assumed to be subfields of a fixed algebraic closure $\overline{\mathbb{Q}_p}$ of \mathbb{Q}_p . Thus every number field has a designated prime \mathfrak{p} above p . Its completion $K_{\mathfrak{p}}$ is assumed to be a subfield of $\overline{\mathbb{Q}_p}$ as well.

16.1 Notation. We write \hat{K} for the completion of a number field K contained in $\overline{\mathbb{Q}_p}$ with respect to its designated prime \mathfrak{p} above p . So $\hat{K} = K_{\mathfrak{p}}$.

The completion of the composite of number fields is the composite of their completions:

16.2 Lemma. Let K_1 and K_2 be number fields. Then $\widehat{K_1 K_2} = \hat{K}_1 \hat{K}_2$.

PROOF. From $K_1, K_2 \subseteq K_1 K_2$ follows that $\hat{K}_1, \hat{K}_2 \subseteq \widehat{K_1 K_2}$. On the other hand $K_1, K_2 \subseteq \hat{K}_1 \hat{K}_2$ and so $K_1 K_2 \subseteq \hat{K}_1 \hat{K}_2$, which implies $\widehat{K_1 K_2} \subseteq \hat{K}_1 \hat{K}_2$. \square

Though completion commutes with composition, it does not commute with intersection: 3 remains prime in $\mathbb{Q}(i)$ and also in $\mathbb{Q}(\sqrt{2})$. Their intersection is \mathbb{Q} , but their completions both equal the unique unramified extension of \mathbb{Q}_p of degree 2.

The next lemma shows in particular that abelian extensions of local fields are obtained by completing abelian number field extensions:

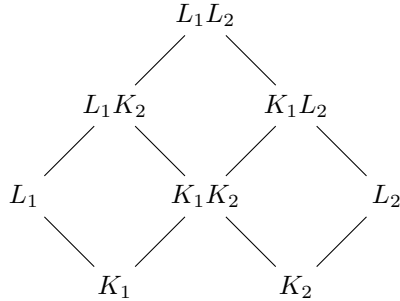
16.3 Lemma. Let $E : F$ be a finite Galois extension of local fields. Then there is a Galois extension $L : K$ of number fields such that $E = \hat{L}$, $F = \hat{K}$ and $\text{Gal}(E : F) \xrightarrow{\sim} \text{Gal}(L : K)$.

PROOF. Let E be a finite extension of \mathbb{Q}_p for a prime number p . By Corollary 11.5 $E = \hat{M}$ for some number field M . Set $G = \text{Gal}(E : F)$ and let L be the composite of the fields $\sigma(M)$ for all $\sigma \in G$. Then $E \supseteq L \supseteq M$ and so $E = \hat{L}$. Put $K = L^G$. Then $\hat{K} \subseteq F$ and so $[E : F] \leq [\hat{L} : \hat{K}] \leq [L : K] = \#(G) = [E : F]$. Hence $F = \hat{K}$ and $\text{Gal}(E : F) \xrightarrow{\sim} \text{Gal}(L : K)$. \square

The local Artin map does not depend on the choice of the number field extension:

16.4 Proposition. Let $E : F$ be an abelian extension of local fields and $L_1 : K_1$ and $L_2 : K_2$ abelian number field extensions such that $E = \hat{L}_1 = \hat{L}_2$ and $F = \hat{K}_1 = \hat{K}_2$. Let \mathfrak{p}_1 and \mathfrak{p}_2 be the designated primes of K_1 respectively K_2 . Then $\vartheta_{\mathfrak{p}_1}^{(L_1)} = \vartheta_{\mathfrak{p}_2}^{(L_2)}$.

PROOF. Consider the diagram below of number field extensions. The extensions $L_1K_2 : K_1K_2$ and $K_1L_2 : K_1K_2$ are abelian and so is their composite $L_1L_2 : K_1K_2$. Let \mathfrak{p}_{12} be the designated prime of K_1K_2 . Then for all $\alpha \in F = \widehat{K_1K_2}$ we have:



$$\begin{aligned}
 \vartheta_{\mathfrak{p}_{12}}^{(L_1L_2)}(\alpha) &= \vartheta_{\mathfrak{p}_{12}}^{(L_1L_2)}(\alpha)|_{\widehat{L_1K_2}} && (\widehat{L_1K_2} = E) \\
 &= \vartheta_{\mathfrak{p}_{12}}^{(L_1K_2)}(\alpha) && \text{(Proposition 15.45)} \\
 &= \vartheta_{\mathfrak{p}_{12}}^{(L_1K_2)}(\alpha)|_{\hat{L}_1} && (\hat{L}_1 = E = \widehat{L_1K_2}) \\
 &= \vartheta_{\mathfrak{p}_1}^{(L_1)}(\mathbb{N}_{\mathfrak{p}_1}^{\mathfrak{p}_{12}}(\alpha)) && \text{(Proposition 15.46)} \\
 &= \vartheta_{\mathfrak{p}_1}^{(L_1)}(\alpha) && (\widehat{K_1K_2} = \hat{K}_1 = F).
 \end{aligned}$$

By symmetry $\vartheta_{\mathfrak{p}_{12}}^{(L_1L_2)}(\alpha) = \vartheta_{\mathfrak{p}_2}^{(L_2)}(\alpha)$. □

So the following definition is justified:

16.5 Definition and notation. Let $E : F$ be an abelian extension of local fields. Then the *Artin map*

$$\vartheta_F^{(E)} : F^* \rightarrow \text{Gal}(E : F)$$

of $E : F$ is defined to be the local Artin map $\vartheta_{\mathfrak{p}}^{(L)}$, where $L : K$ is any abelian number field extension such that $\hat{L} = E$, $\hat{K} = F$ and \mathfrak{p} is the designated prime of K .

The local Artin map $\vartheta_{\mathfrak{p}}^{(L)} : K_{\mathfrak{p}}^* \rightarrow Z_{\mathfrak{p}}^{(L)}$ is surjective and its kernel is $\mathbb{N}_{\mathfrak{p}}^{\mathfrak{q}}(L_{\mathfrak{q}}^*)$. So we have:

16.6 Theorem. Let $E : F$ be an abelian extension of local fields. Then $\vartheta_F^{(E)}$ induces an isomorphism $F^*/\mathbb{N}_F^E(E^*) \xrightarrow{\sim} \text{Gal}(E : F)$. □

The consistency property for local Artin maps and their behavior under base field extensions (Propositions 15.45 and 15.46) are easily translated:

16.7 Proposition. *Let $E : F$ be an abelian extension of local fields.*

(i) *Let E' an intermediate field of the extension $E : F$. Then for all $\alpha \in F^*$*

$$\vartheta_F^{(E')}(\alpha) = \vartheta_F^{(E)}(\alpha)|_{E'}.$$

(ii) *Let $F' : F$ be an extension of local fields. Then for all $\alpha \in F'^*$*

$$\vartheta_{F'}^{(EF')}(\alpha)|_E = \vartheta_F^{(E)}(N_F^{F'}(\alpha)).$$

PROOF.

(i) Take L such that $\hat{L} = E$ and subsequently the subfields K and L' of L which are invariant under $\text{Gal}(E : F)$ and $\text{Gal}(E : E')$ respectively. Then $F = \hat{K}$, $E' = \hat{K}'$ and

$$\vartheta_F^{(E')}(\alpha) = \vartheta_{\mathfrak{p}}^{(L')}(\alpha) = \vartheta_{\mathfrak{p}}^{(L)}(\alpha)|_{\hat{K}'} = \vartheta_F^{(E)}(\alpha)|_{E'}.$$

(ii) Take an abelian number field extension $L : K$ such that $\hat{L} = E$ and $\hat{K} = F$. Let K' be a number field such that $\hat{K}' = F'$. Then $EF' = \hat{L}\hat{K}' = \widehat{LK'}$ (Lemma 16.2) and so

$$\vartheta_{F'}^{(EF')}(\alpha)|_E = \vartheta_{\mathfrak{p}'}^{(LK')}(\alpha)|_{\hat{L}} = \vartheta_{\mathfrak{p}}^{(L)}(N_{\mathfrak{p}'}^{\mathfrak{p}}(\alpha)) = \vartheta_F^{(E)}(N_F^{F'}(\alpha)). \quad \square$$

16.8 Notation. Because of the consistency property (Proposition 16.7(i)) we will often replace the upper index of ϑ in $\vartheta_F^{(E)}(\alpha)(\beta)$ by $(*)$: $*$ stands for any E such that $E : F$ is an abelian extension with $\beta \in E$. In chapter 19 we will omit the upper index: $\vartheta_F(\alpha)$ is there interpreted as an automorphism of $\overline{\mathbb{Q}_p} : F$.

For unramified extensions the local Artin map is given by the Frobenius automorphism. This is a direct consequence of Proposition 15.44.

16.9 Proposition. *Let $E : F$ be an unramified abelian extension of local fields. Then $\vartheta_F^{(E)}(\alpha) = (\varphi_F^{(E)})^{v(\alpha)}$ for all $\alpha \in F^*$. In particular, $\mathcal{O}_F^* \subseteq \text{Ker}(\vartheta_F^{(E)})$. \square*

Local class field theory is about a one-to-one correspondence between abelian extensions of a local fields F and subgroups of F^* of finite index. Each abelian extension $E : F$ determines the subgroup $N_F^E(E^*)$ of index $[E : F]$.

16.10 Proposition. *Let F be a local field and $E_1 : F$ and $E_2 : F$ abelian extensions. Then*

$$E_1 \subseteq E_2 \iff N_F^{E_1}(E_1^*) \supseteq N_F^{E_2}(E_2^*).$$

PROOF.

\Rightarrow : This follows from $N_F^{E_1}N_{E_1}^{E_2} = N_F^{E_2}$.

\Leftarrow : Put $E = E_1 E_2$ and $E' = E_1 \cap E_2$. Let $\alpha \in \text{Ker}(\vartheta_F^{(E_1)}) \cap \text{Ker}(\vartheta_F^{(E_2)})$. Then by the consistency property (Proposition 16.7(i)) we have:

$$\vartheta_F^{(E)}(\alpha)|_{E_1} = \vartheta_F^{(E_1)}(\alpha) = 1 \quad \text{and} \quad \vartheta_F^{(E)}(\alpha)|_{E_2} = \vartheta_F^{(E_2)}(\alpha) = 1.$$

It follows that $\text{Ker}(\vartheta_F^{(E)}) = \text{Ker}(\vartheta_F^{(E_1)}) \cap \text{Ker}(\vartheta_F^{(E_2)})$, that is $N_F^E(E^*) = N_F^{E_1}(E_1^*) \cap N_F^{E_2}(E_2^*)$. Suppose $N_F^{E_1}(E_1^*) \supseteq N_F^{E_2}(E_2^*)$. Then $N_F^E(E^*) = N_F^{E_2}(E_2^*)$ and so by Theorem 16.6 $[E : F] = [E_2 : F]$. It follows that $E = E_2$, that is $E_1 \subseteq E_2$. \square

So the map

$$\begin{array}{ccc} \text{abelian} & & \text{subgroups of } F^* \\ \text{extensions of } F & \xrightarrow{\quad} & \text{of finite index} \\ E : F & \longmapsto & N_F^E(E^*) \end{array}$$

is injective. We will show its surjectivity: the existence theorem for local class field theory. The proof is along the lines of the proof in the global case, but is much simpler.

16.11 Definition. Let X be a subgroup of F^* of finite index. If $E : F$ is an abelian extension of F such that $N_F^E(E^*) = X$, then E is called the *class field* for X . Notation: $E = F_X$.

16.12 Lemma. Let $E : F$ be an abelian extension of local fields and X a subgroup of F^* such that $N_F^E(E^*) \subseteq X \subseteq F^*$. Then there is a class field for X .

PROOF. Put $H = \vartheta_F^{(E)}(X) \subseteq G = \text{Gal}(E : F)$ and $E' = E^H$. It will follow that E' is the class field for X . For $\alpha \in F^*$ we have:

$$\begin{aligned} \alpha \in X &\iff \vartheta_F^{(E)}(\alpha) \in H \iff \vartheta_F^{(E)}(\alpha)|_{E'} = 1 \iff \vartheta_F^{(E')}(\alpha) = 1 \\ &\iff \alpha \in \text{Ker}(\vartheta_F^{(E')}) \iff \alpha \in N_F^{E'}(E'^*). \end{aligned} \quad \square$$

16.13 Lemma. Let $F' : F$ be an abelian extension of local fields and X a subgroup of F^* of finite index. Assume that there is a class field for the subgroup

$$X' = (N_F^{F'})^{-1}(X) = \{ \alpha \in F'^* \mid N_F^{F'}(\alpha) \in X \}$$

of F'^* . Then there is a class field for X .

PROOF. Let E be the class field for X' . From

$$N_F^E(E^*) = N_F^{F'} N_{F'}^E(E^*) = N_F^{F'}(X') \subseteq X$$

and Lemma 16.12 follows that it suffices to show that $E : F$ is an abelian extension. Let σ be an embedding of E in the chosen algebraic closure of F such that its restriction to F is the identity. Put $H = \text{Gal}(E : F')$. Then $\sigma H \sigma^{-1} = \text{Gal}(\sigma(E) : F')$ and $\sigma(E)$ is the class field for $\sigma(X')$: for $\alpha \in E^*$ we have

$$N_{F'}^{\sigma(E)}(\sigma(\alpha)) = \prod_{\tau \in H} \sigma \tau \sigma^{-1}(\sigma(\alpha)) = \sigma \left(\prod_{\tau \in H} \tau(\alpha) \right) = \sigma(N_{F'}^E(\alpha)) \in \sigma(X').$$

Because $F' : F$ is a Galois extension we have $\sigma(F') = F'$ and therefore, $N_{F'}^{E'}(\alpha) = N_{F'}^{E'}(\sigma(\alpha))$ for all $\alpha \in F'$. So $\sigma(\beta) = \beta$ for all $\beta \in X'$. In particular $\sigma(X') = X'$ and by Proposition 16.10 $\sigma(E) = E$. It follows that $E : F$ is a Galois extension and that $\text{Gal}(F' : F)$ operates trivially on $\text{Gal}(E : F')$. For $F' : F$ cyclic this means that $\text{Gal}(E : F)$ is abelian. The general case of $F' : F$ being abelian follows by induction in the same way as in the proof of Theorem 15.7. \square

16.14 Local Existence Theorem. *Let F be a local field and X a subgroup of F^* of finite index. Then there is a class field for X .*

PROOF. Let n be an exponent of the finite group F^*/X . By Lemma 16.13 we may assume that F contains a primitive n -th root of unity. By Corollary 11.23 the index $(F^* : F^{*n})$ is finite. By Lemma 16.12 it suffices to prove that there is a class field for F^{*n} . Let E be the n -Kummer extension corresponding to F^{*n} . By Theorem 15.14 we have $(F^* : F^{*n}) = [E : F]$ and by Theorem 12.22 $(F^* : N_F^E(E^*)) = [E : F]$. Since $F^{*n} \subseteq N_F^E(E^*)$, it follows that $F^{*n} = N_F^E(E^*)$. So E is the class field for F^* . \square

Summarizing we have:

16.15 Local Classification Theorem. *For F a local field we have a one-to-one correspondence*

$$\begin{array}{ccc} \text{abelian} & & \text{subgroups of } F^* \\ \text{extensions of } F & \longleftrightarrow & \text{of finite index} \\ \\ E : F & \longmapsto & N_F^E(E^*) \\ \\ F_X : F & \longleftarrow & X \end{array}$$

The local Artin map $\vartheta_F^{(F_X)} : F^* \rightarrow \text{Gal}(F_X : F)$ induces an isomorphism $F^*/X \xrightarrow{\sim} \text{Gal}(F_X : F)$. \square

We have seen in section 15.6 that the conductor of an abelian number field extension is the product of local conductors (Theorem 15.56). Now it is clear that these local conductors are conductors in the sense of local class field theory.

16.16 Notation. Let F be a local field and $i \in \mathbb{N}$. The open subgroup $U_F^{(i)}$ of F^* is defined by

$$U_F^{(i)} = \begin{cases} \mathcal{O}_F^* & \text{if } i = 0, \\ 1 + \mathfrak{p}_F^i & \text{if } i > 0. \end{cases}$$

So for the \mathfrak{p} -adic completion $K_{\mathfrak{p}}$ of a number field K we have $U_{K_{\mathfrak{p}}}^{(i)} = U_{\mathfrak{p}}^{(i)}$. See Notation 15.54.

16.17 Definition and notation. Let $E : F$ an abelian extension of local fields. There is a least $s \in \mathbb{N}$ such that $U_F^{(s)} \subseteq N_F^E(E^*)$. The ideal \mathfrak{p}_F^s of \mathcal{O}_F is called the *conductor* of $E : F$. Notation: $\mathfrak{f}_F(E)$.

For $L : K$ an abelian extension of number fields, \mathfrak{p} a finite prime of K and \mathfrak{q} a prime of L above \mathfrak{p} we have $\mathfrak{f}_{K_{\mathfrak{p}}}(L_{\mathfrak{q}}) \cap K = \mathfrak{f}_{\mathfrak{p}}(L)$. See Definition 15.55.

16.18 Proposition. Let $E : F$ be an unramified abelian extension of local fields of degree n . Then

$$N_F^E(E^*) = \mathcal{O}_F^* F^{*n}.$$

PROOF. By Proposition 16.9 we have $\mathcal{O}_F^* \subseteq \text{Ker}(\vartheta_F^{(E)}) = N_F^E(E^*)$ and hence $\mathcal{O}_F^* F^{*n} \subseteq N_F^E(E^*)$. Equality holds because both groups are of index n in F^* . \square

We have already seen that for each $n \in \mathbb{N}^*$ there is a unique unramified abelian extension of degree n of a given local field F (Corollary 11.13). The proposition tells us to which subgroup of index n of F^* this extension corresponds.

16.19 Proposition. Let $E : F$ be an abelian extension of local fields. Then $E : F$ is totally ramified if and only if $N_F^E(E^*)$ contains a uniformizer of v_F .

PROOF. We have a commutative square

$$\begin{array}{ccc} E^* & \xrightarrow{v_E} & \mathbb{Z} \\ \downarrow N_F^E & & \downarrow f_F^{(E)} \\ F^* & \xrightarrow{v_F} & \mathbb{Z} \end{array}$$

The map v_E is surjective, so the composition $v_F N_F^E$ is surjective if and only if $f_F^{(E)} = 1$. \square

Our construction of the local Artin map is based on the (global) Artin map for a number field extension. In modern approaches it is the other way round using a direct construction in the local situation. The local Artin maps do not depend on the construction: they are unique in the following sense.

16.20 Theorem. Let F be a local field and $(\psi^{(E)})$ a collection of maps

$$\psi^{(E)}: F^* \rightarrow \text{Gal}(E : F) \quad (\text{one for each abelian extension } E : F)$$

satisfying

- a) **reciprocity:** For each abelian extension $E : F$ the homomorphism $\psi^{(E)}$ induces an isomorphism

$$F^* / \mathbb{N}_F^E(E^*) \xrightarrow{\sim} \text{Gal}(E : F).$$

- b) **consistency:** For each abelian extension $E : F$ and each intermediate field E' of $E : F$

$$\psi^{(E')}(\alpha) = \psi^{(E)}(\alpha)|_{E'} \quad \text{for all } \alpha \in F^*.$$

- c) **frobenius:** For each unramified abelian extension $E : F$

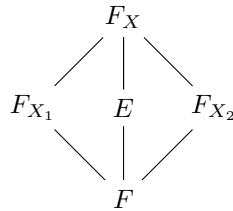
$$\psi^{(E)}(\alpha) = (\varphi_F^{(E)})^{v_F(\alpha)} \quad \text{for each } \alpha \in F^*.$$

Then $\psi^{(E)} = \vartheta_F^{(E)}$ for all abelian extensions $E : F$.

PROOF. Let $\pi \in F^*$ be a uniformizer of v_F and $E : F$ an abelian extension of degree n and conductor \mathfrak{p}_F^t . The group $X = (1 + \mathfrak{p}_F^t) \cdot \langle \pi^n \rangle \subseteq F^*$ is contained in $\mathbb{N}_F^E(E^*)$ and is of finite index in F^* . It is the intersection of two subgroups of F^* of finite index:

$$X = X_1 \cap X_2 \quad \text{with } X_1 = (1 + \mathfrak{p}_F^t) \cdot \langle \pi \rangle \text{ and } X_2 = \mathcal{O}_F^* \cdot \langle \pi^n \rangle.$$

Then $X_1 X_2 = \mathcal{O}_F^* \cdot \langle \pi \rangle = F^*$. So we have the following diagram of abelian field extensions



with $\text{Gal}(F_X : F) \xrightarrow{\sim} \text{Gal}(F_{X_1} : F) \times \text{Gal}(F_{X_2} : F)$. By a) and c)

$$\psi^{(F_{X_1})}(\pi) = 1 = \vartheta_F^{(F_{X_1})}(\pi) \quad \text{and} \quad \psi^{(F_{X_2})}(\pi) = \varphi_F^{(F_{X_2})} = \vartheta_F^{(F_{X_2})}(\pi).$$

So by b)

$$\psi^{(E)}(\pi) = \psi^{F_X}(\pi)|_E = \vartheta_F^{(F_X)}(\pi)|_E = \vartheta_F^{(E)}(\pi).$$

It follows that $\psi^{(E)}$ and $\vartheta_F^{(E)}$ agree on uniformizers. The group F^* is generated by uniformizers: for $\alpha \in F^*$ we have

$$\alpha = (\alpha\pi^{-v(\alpha)+1})\pi^{v(\alpha)-1}.$$

Hence $\psi^{(E)} = \vartheta_F^{(E)}$ for all abelian extensions $E : F$. □

16.2 Norm residue symbols

For a given abelian number field extension $L : K$ any local Artin map can be applied to the nonzero elements of the base field K and take values in the Galois group of $L : K$. In this section it is shown that the product of these values over all primes of K is trivial. This result is independent of the previous section. Only section 15.6 is used.

16.21 Definition. Let $L : K$ be an abelian number field extension and \mathfrak{p} a prime of K . The composition

$$K^* \xrightarrow{\subset} K_{\mathfrak{p}}^* \xrightarrow{\vartheta_{\mathfrak{p}}^{(L)}} Z_{\mathfrak{p}}^{(L)} \xrightarrow{\subseteq} \text{Gal}(L : K)$$

is called the *norm residue symbol* at \mathfrak{p} . The following notation is often used: for $a \in K^*$

$$\left(\frac{a, L : K}{\mathfrak{p}} \right) = \vartheta_{\mathfrak{p}}^{(L)}(a).$$

So by Theorem 15.48 we have

$$\left(\frac{a, L : K}{\mathfrak{p}} \right) = 1 \iff a \in N_{\mathfrak{p}}^{\mathfrak{q}}(L_{\mathfrak{q}}^*),$$

where \mathfrak{q} is a prime of L above \mathfrak{p} . An $a \in K^*$ is said to be a *local norm* at \mathfrak{p} if $a \in N_{\mathfrak{p}}^{\mathfrak{q}}(L_{\mathfrak{q}}^*)$.

The construction of the local Artin maps $\vartheta_{\mathfrak{p}}^{(L)}$ leads to a *product formula* for norm residue symbols:

16.22 Theorem. Let $L : K$ be an abelian extension of number fields and $a \in K^*$. Then

$$\prod_{\mathfrak{p}} \left(\frac{a, L : K}{\mathfrak{p}} \right) = 1.$$

PROOF. The product is a finite one: for finite nonramifying \mathfrak{p} with $v_{\mathfrak{p}}(a) = 0$ we have $\left(\frac{a, L : K}{\mathfrak{p}} \right) = 1$. Choose a modulus \mathfrak{m} for $L : K$ such that $\mathfrak{p} \mid \mathfrak{m}$ for all finite

primes \mathfrak{p} of K with $v_{\mathfrak{p}}(a) \neq 0$. Let $\mathfrak{m} = \mathfrak{p}_1^{k_1} \cdots \mathfrak{p}_s^{k_s}$, where $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ are different primes of K and put $\mathfrak{m}_i = \mathfrak{m}\mathfrak{p}_i^{-k_i}$. By Lemma 13.19 there are $a_i \in K^*$ such that

$$a_i \equiv \begin{cases} a & (\text{mod } K_{\mathfrak{p}_i}^{1, k_i}), \\ 1 & (\text{mod } K_{\mathfrak{m}_i}^1). \end{cases}$$

Then

$$a_1 \cdots a_s \equiv a \pmod{K_{\mathfrak{m}}^1}.$$

Let

$$\mathfrak{a}_i = \begin{cases} a_i \mathfrak{p}_i^{-v_{\mathfrak{p}_i}(a)} & \text{if } \mathfrak{p}_i \text{ is finite,} \\ a_i \mathcal{O}_K & \text{if } \mathfrak{p}_i \text{ is infinite.} \end{cases}$$

Then

$$\vartheta_{\mathfrak{p}_i}^{(L)}(a) = \vartheta_{\mathfrak{p}_i}^{(L)}(a_i) = \vartheta^{(L)}(a_i) = \varphi_K^{(L)}(\mathfrak{a}_i)^{-1}$$

and

$$a_1 \cdots a_s \mathcal{O}_K = a_1 \mathcal{O}_K \cdots a_s \mathcal{O}_K = \mathfrak{p}_1^{v_{\mathfrak{p}_1}(a)} \cdots \mathfrak{p}_s^{v_{\mathfrak{p}_s}(a)} \cdot \mathfrak{a}_1 \cdots \mathfrak{a}_s = a \cdot \mathfrak{a}_1 \cdots \mathfrak{a}_s.$$

Hence

$$\mathfrak{a}_1 \cdots \mathfrak{a}_s = \frac{a_1 \cdots a_s}{a} \mathcal{O}_K \in \mathbb{S}_{\mathfrak{m}}(K)$$

and so

$$\prod_{\mathfrak{p}} \left(\frac{a, L : K}{\mathfrak{p}} \right) = \prod_{i=1}^s \vartheta_{\mathfrak{p}_i}^{(L)}(a) = \prod_{i=1}^s \varphi_K^{(L)}(\mathfrak{a}_i)^{-1} = \varphi_K^{(L)}(\mathfrak{a}_1 \cdots \mathfrak{a}_s)^{-1} = 1. \quad \square$$

16.3 Hilbert symbols

In this section local fields with residue class fields of characteristic a prime number p are considered to be subfields of a fixed algebraic closure $\overline{\mathbb{Q}_p}$ of the p -adic field \mathbb{Q}_p . In section 16.1 we defined Artin maps $\vartheta_F^{(E)} : E^* \rightarrow \text{Gal}(E : F)$ by considering number fields with designated prime ideals.

For infinite primes \mathfrak{p} we fix the algebraic closure $\overline{\mathbb{Q}_{\infty}}$ to be the field \mathbb{C} . A number field with a designated infinite prime is then just a subfield of \mathbb{C} . For the extension $\mathbb{C} : \mathbb{R}$ we have a map

$$\vartheta_{\mathbb{R}}^{(\mathbb{C})} : \mathbb{R}^* \rightarrow \text{Gal}(\mathbb{C} : \mathbb{R}), \quad \alpha \mapsto \begin{cases} 1 & \text{if } \alpha > 0, \\ \tau & \text{if } \alpha < 0, \end{cases}$$

where τ is complex conjugation. Then for an abelian extension $L : K$ of number fields and \mathfrak{p} a real infinite prime of K we have $\vartheta_{\mathfrak{p}}^{(L)}(\alpha) = \sigma_{\mathfrak{q}}^{-1} \vartheta_{\mathbb{R}}^{(\mathbb{C})}(\sigma_{\mathfrak{p}}(\alpha)) \sigma_{\mathfrak{q}}$, where \mathfrak{q} is a prime of L above \mathfrak{p} .

In general, if K is a field containing a primitive n -th root of unity and $b \in K^*$, then the extension $K(\sqrt[n]{b}) : K$ is a Galois extension and

$$\text{Gal}(K(\sqrt[n]{b}) : K) \rightarrow \mu_n, \quad \sigma \mapsto \frac{\sigma(\sqrt[n]{b})}{\sqrt[n]{b}} \tag{16.1}$$

is an injective group homomorphism. (The group μ_n is the cyclic group of n -th roots of unity of K .) We use this for the construction of a symbol on a local field.

16.23 Definition. Let F be a local field with $\mu_n \subset F$. The map

$$F^* \times F^* \rightarrow \mu_n, \quad (\alpha, \beta) \mapsto \frac{\vartheta_F^{(*)}(\alpha)(\sqrt[n]{\beta})}{\sqrt[n]{\beta}}$$

is called the n -th Hilbert symbol on F . Notation:

$$(\alpha, \beta)_n = \frac{\vartheta_F^{(*)}(\alpha)(\sqrt[n]{\beta})}{\sqrt[n]{\beta}}.$$

(See Notation 16.8 for the $\vartheta_F^{(*)}$ notation.) Similarly, for the field \mathbb{R} we have

$$\mathbb{R}^* \times \mathbb{R}^* \rightarrow \mu_2, \quad (\alpha, \beta) \mapsto \frac{\vartheta_{\mathbb{R}}^{(\mathbb{C})}(\alpha)(\sqrt{\beta})}{\sqrt{\beta}} =: (\alpha, \beta)_2.$$

16.24 Definition. Let K be a number field containing μ_n . For \mathfrak{p} a prime of K , the n -th Hilbert symbol on the completion $K_{\mathfrak{p}}$ restricts to a symbol on K , the n -th Hilbert symbol on K at \mathfrak{p} :

$$K^* \times K^* \rightarrow \mu_n, \quad (a, b) \mapsto (a, b)_n = \frac{\vartheta_{\mathfrak{p}}^{(*)}(a)(\sqrt[n]{b})}{\sqrt[n]{b}},$$

where $*$ stands for a number field containing $K(\sqrt[n]{b})$. This symbol will be denoted by $\left(\frac{a, b}{\mathfrak{p}}\right)_n$.

16.25 Proposition. Hilbert symbols on \mathbb{C} are trivial. For the quadratic Hilbert symbol on \mathbb{R} we have for $\alpha, \beta \in \mathbb{R}^*$

$$(\alpha, \beta)_2 = -1 \iff \alpha < 0 \text{ and } \beta < 0.$$

PROOF. Equivalent are:

$$(\alpha, \beta)_2 = -1,$$

$$\vartheta_{\mathbb{R}}^{(*)}(\alpha) \neq 1 \text{ and } \alpha \notin \mathbb{R}^{*+},$$

$$\beta < 0 \text{ and } \alpha < 0. \quad \square$$

The dependency on n is as one might expect:

16.26 Proposition. *Let F be a local field with $\mu_n \subset F$ and let $m \mid n$. Then for all $\alpha, \beta \in F^*$:*

$$(\alpha, \beta)_m = (\alpha, \beta)_n^{n/m}.$$

PROOF. $(\alpha, \beta)_n^{n/m} = \frac{(\vartheta_F^{(*)}(\alpha)(\sqrt[n]{\beta}))^{n/m}}{(\sqrt[n]{\beta})^{n/m}} = \frac{\vartheta_F^{(*)}(\alpha)(\sqrt[m]{\beta})}{\sqrt[m]{\beta}} = (\alpha, \beta)_m. \quad \square$

The product formula for local Artin maps (Theorem 16.22) yields a product formula for Hilbert symbols:

16.27 Theorem. *Let K be a number field containing the n -th roots of unity and let $a, b \in K^*$. Then*

$$\prod_{\mathfrak{p}} \left(\frac{a, b}{\mathfrak{p}} \right)_n = 1,$$

where the product is over all primes of K .

PROOF. The product formula for local Artin maps for the Galois extension $K(\sqrt[n]{b}) : K$

$$\prod_{\mathfrak{p}} \vartheta_{\mathfrak{p}}^{(K(\sqrt[n]{b}))}(a) = 1$$

is via the group homomorphism (16.1) translated into a product formula for Hilbert symbols. \square

16.28 Proposition. *Hilbert symbols are bilinear.*

PROOF. Let F be a local field containing μ_n . Because for each $\beta \in F^*$ the map $\vartheta_F^{(F(\sqrt[n]{\beta}))}$ is a homomorphism, the Hilbert symbol is linear in the first variable:

$$(\alpha_1\alpha_2, \beta)_n = (\alpha_1, \beta)_n(\alpha_2, \beta)_n.$$

For $\beta_1, \beta_2 \in F^*$ take $E = F(\sqrt[n]{\beta_1}, \sqrt[n]{\beta_2})$. Since $\vartheta_F^{(E)}(\alpha)$ is an automorphism of E for each $\alpha \in F^*$, the Hilbert symbol is linear in the second variable:

$$(\alpha, \beta_1\beta_2)_n = (\alpha, \beta_1)_n(\alpha, \beta_2)_n.$$

For the symbol $(\alpha, \beta)_2$ on \mathbb{R} bilinearity is easily verified. \square

16.29 Proposition. *Let F be a local field containing μ_n . Then $(1 - \alpha, \alpha)_n = 1$ for all $\alpha \in F^* \setminus \{1\}$.*

PROOF. Put $\gamma = \sqrt[n]{\alpha}$ and $E = F(\gamma)$. The homomorphism

$$\text{Gal}(E : F) \rightarrow \mu_n = \langle \zeta_n \rangle, \quad \sigma \mapsto \frac{\sigma(\gamma)}{\gamma}$$

is injective. Let $d = \#(\text{Gal}(E : F))$ and choose $\sigma \in \text{Gal}(E : F)$ such that $\sigma(\gamma) = \zeta_d \gamma$. From

$$X^n - \alpha = \prod_{i=1}^n (X - \zeta_n^i \gamma)$$

follows that $1 - \alpha$ is a norm:

$$\begin{aligned} 1 - \alpha &= \prod_{i=1}^n (1 - \zeta_n^i \gamma) = \prod_{k=1}^{n/d} \prod_{j=1}^d (1 - \zeta_d^j \zeta_n^k \gamma) = \prod_{k=1}^{n/d} N_F^E (1 - \zeta_n^k \gamma) \\ &= N_F^E \left(\prod_{k=1}^{n/d} (1 - \zeta_n^k \gamma) \right). \end{aligned}$$

The proposition follows from Theorem 15.48:

$$1 - \alpha \in N_F^E(F(\gamma)^*) = \text{Ker}(\vartheta_F^{(E)}) \quad \square.$$

Clearly, for the symbol $(\alpha, \beta)_2$ on \mathbb{R} we also have $(1 - \alpha, \alpha) = 1$: the real numbers α and $1 - \alpha$ cannot be both negative.

For fields K bilinear pairings on K^* satisfying the identity of this proposition occur frequently. They have a special name.

16.30 Definition. Let K be a field and A a (multiplicative) abelian group. A *Steinberg symbol* on K with values in A is a mapping $s : K^* \times K^* \rightarrow A$ satisfying

- (SS1) $s(a_1 a_2, b) = s(a_1, b) s(a_2, b)$ for all $a_1, a_2, b \in K^*$,
- (SS2) $s(a, b_1 b_2) = s(a, b_1) s(a, b_2)$ for all $a, b_1, b_2 \in K^*$,
- (SS3) $s(1 - a, a) = 1$ for all $a \in K^* \setminus \{1\}$.

Steinberg symbols arise in algebraic K-theory, a part of algebra that started around 1970. A central part of algebraic K-theory is about abelian groups $K_n(R)$ for $n \in \mathbb{N}$ and R a ring. For $n \leq 2$ good references for this theory are [29], [2] (for $n = 0, 1$) and [26]. It's a theorem of Matsumoto that for a field F , the group $K_2(F)$ has a presentation given by generators

$$\{a, b\} \quad (a, b \in F^*)$$

(the notation $\{a, b\}$ is a 'symbol' notation, not the set-notation) and relations

- $\{a_1, b\} \{a_2, b\} = \{a_1 a_2, b\}$ for all $a_1, a_2, b \in F^*$,
- $\{a, b_1 b_2\} = \{a, b_1\} \{a, b_2\}$ for all $a, b_1, b_2 \in F^*$,
- $\{1 - a, a\} = 1$ for all $a \in F^* \setminus \{1\}$.

(For an obvious reason in algebraic K-theory one tends to denote fields by F rather than K .) So the map $(a, b) \mapsto \{a, b\}$ is a Steinberg symbol on F , in fact it is the ‘universal’ Steinberg symbol on F . By the way, the groups $K_0(F)$ and $K_1(F)$ are \mathbb{Z} and F^* respectively.

Consequences of the axioms for Steinberg symbols:

16.31 Theorem. *Let s be a Steinberg symbol on a field K with values in an abelian group A . Then*

$$(SS4) \quad s(-a, a) = 1 \text{ for all } a \in K^*,$$

$$(SS5) \quad s(b, a) = s(a, b)^{-1} \text{ for all } a, b \in K^*,$$

$$(SS6) \quad s(a, a) = s(a, -1) \text{ for all } a \in K^*,$$

$$(SS7) \quad s(a, b) = s(a, a+b)s(a+b, b)s(a+b, -1) \text{ for all } a, b \in K^* \text{ with } a \neq -b.$$

PROOF.

(SS4) For $a = 1$ this follows from (SS2). For $a \neq 1$ use $-a = \frac{1-a}{1-\frac{1}{a}}$:

$$\begin{aligned} s(-a, a) &= s\left(\frac{1-a}{1-\frac{1}{a}}, a\right) = s\left(1-a, a\right)s\left(1-\frac{1}{a}, a\right)^{-1} && (SS1) \\ &= s\left(1-\frac{1}{a}, \frac{1}{a}\right) && (SS3) \text{ and } (SS2) \\ &= 1 && (SS3). \end{aligned}$$

(SS5) Apply (SS4) three times:

$$\begin{aligned} s(b, a) &= s(b, a)s(-a, a)^{-1} && (SS4) \\ &= s(b, a)s\left(-\frac{1}{a}, a\right) && (SS1) \\ &= s\left(-\frac{b}{a}, a\right) && (SS1) \\ &= s\left(-\frac{b}{a}, a\right)s\left(-\frac{b}{a}, \frac{b}{a}\right) && (SS4) \\ &= s\left(-\frac{b}{a}, b\right) && (SS2) \\ &= s(-b, b)s(a, b)^{-1} && (SS1) \\ &= s(a, b)^{-1} && (SS4). \end{aligned}$$

(SS6)

$$\begin{aligned} s(a, a) &= s(a, -a)s(a, -1) && (SS2) \\ &= s(a, -1) && (SS4). \end{aligned}$$

(SS7) Put $c = a + b$. Then

$$\begin{aligned} 1 &= s\left(\frac{a}{c}, \frac{b}{c}\right) && \text{(SS3)} \\ &= s(a, b)s(a, c)^{-1}s(c, b)^{-1}s(c, c) && \text{(SS1) and (SS2)} \\ &= s(a, b)s(a, c)^{-1}s(c, b)^{-1}s(c, -1)^{-1} && \text{(SS2) and (SS6).} \quad \square \end{aligned}$$

16.32 Definition. Let F be a field with a discrete valuation v , valuation ring R and maximal ideal \mathfrak{p} . The *tame symbol* on the discretely valued field F is the map

$$F^* \times F^* \rightarrow (R/\mathfrak{p})^*: (a, b) \mapsto (a, b)_v = (-1)^{v(a)v(b)} b^{v(a)} a^{-v(b)} + \mathfrak{p}.$$

Since $v(b^{v(a)} a^{-v(b)}) = v(a)v(b) - v(b)v(a) = 0$, we have

$$(-1)^{v(a)v(b)} b^{v(a)} a^{-v(b)} \in R^*$$

and so $(a, b)_v \in (R/\mathfrak{p})^* = R^*/(1 + \mathfrak{p})$.

16.33 Proposition. *Tame symbols are Steinberg symbols.*

PROOF. Tame symbols are obviously bilinear, so it remains to show that they satisfy (SS3). Let F be a discretely valued field as in Definition 16.32 and $a, b \in F^*$ such that $a + b = 1$. The proof of $(a, b)_v = 1$ is by case distinction.

$v(a) > 0$: Then $v(b) = 0$, so $(-1)^{v(a)v(b)} = 1$ and $b^{v(a)} a^{-v(b)} = b^{-v(a)} = (1 - a)^{v(a)} \equiv 1 \pmod{\mathfrak{p}}$.

$v(b) > 0$: As the case $v(a) > 0$.

$v(a) < 0$: Then $v(b) = v(1 - a) = v(a)$ and so $b^{v(a)} a^{-v(b)} = (ba^{-1})^{v(a)} = (a^{-1} - 1)^{v(a)} \equiv (-1)^{v(a)} = (-1)^{v(a)v(b)} \pmod{\mathfrak{p}}$.

$v(b) < 0$: As the case $v(a) < 0$.

$v(a) = v(b) = 0$: In this case the condition is trivially satisfied. □

Tame symbols on a local field are essentially Hilbert symbols:

16.34 Theorem. *Let F be a local field. Under the isomorphism $\mu_{q-1} \xrightarrow{\sim} (k_F)^*, \zeta \mapsto \bar{\zeta} (= \zeta + \mathfrak{p})$, where $q = \#(k_F)$, the Hilbert symbol $(\alpha, \beta)_{q-1}$ maps to the tame symbol $(\alpha, \beta)_v$.*

PROOF. Choose $\pi \in F$ with $v(\pi) = 1$. Both symbols are Steinberg symbols, so by bilinearity and anti-symmetry it suffices to consider the cases (α, β) , (π, β) and (π, π) , where $\alpha, \beta \in \mathcal{O}_F^*$. By (SS4) the last case can be replaced by $(\pi, -1)$. Thus only two cases remain. In both cases put $E = F(\sqrt[q-1]{\beta})$. By Lemma 15.15 the extension $E : F$ is unramified. Hence by Proposition 16.9 $\vartheta_F^{(E)}(\gamma) = (\varphi_F^{(E)})^{v(\gamma)}$ for all $\gamma \in F^*$.

(α, β) with $\alpha, \beta \in \mathcal{O}_F^*$:

By definition of the tame symbol $(\alpha, \beta)_v = \bar{1}$. Since $v(\alpha) = 0$, we have $\vartheta_F^{(E)}(\alpha) = 1_E$ and so $\vartheta_F^{(E)}(\alpha)(\sqrt[q]{\beta}) = \sqrt[q]{\beta}$. Hence $(\alpha, \beta)_{q-1} = 1$.

(π, β) with $\beta \in \mathcal{O}_F^*$:

Again by definition of the tame symbol $(\pi, \beta)_v = \bar{\beta}$. The Hilbert symbol is defined by

$$\vartheta_F^{(E)}(\pi)(\sqrt[q]{\beta}) = (\pi, \beta)_{q-1} \sqrt[q]{\beta}.$$

Modulo \mathfrak{p}_E we have

$$\vartheta_F^{(E)}(\pi)(\sqrt[q]{\beta}) = \varphi_F^{(E)}(\sqrt[q]{\beta}) \equiv \sqrt[q]{\beta^q} \pmod{\mathfrak{p}_E}.$$

Hence

$$\sqrt[q]{\beta^q} \equiv (\pi, \beta)_{q-1} \sqrt[q]{\beta} \pmod{\mathfrak{p}_E}$$

and division by $\sqrt[q]{\beta}$ yields:

$$\beta \equiv (\pi, \beta)_{q-1} \pmod{\mathfrak{p}_E \cap F}. \quad \square$$

In the notation introduced on page 282:

$$(\alpha, \beta)_{q-1} = \omega_F((\alpha, \beta)_v).$$

So the Hilbert symbols on a local field F are all powers of the Hilbert symbol $(\alpha, \beta)_m$, where $m = \#(\mu(F))$ (Proposition 16.26) and $(\alpha, \beta)_{\frac{m}{q-1}}$ corresponds to the tame symbol. Let's call Hilbert symbols $(\alpha, \beta)_n$ with $n \mid q-1$ tame Hilbert symbols, and the others wild Hilbert symbols. So tame Hilbert symbols are essentially powers of tame symbols:

16.35 Corollary. *In the notation of Theorem 16.34: for $n \mid q-1$ the Hilbert symbol $(\alpha, \beta)_n$ is related to the tame symbol $(\alpha, \beta)_v$ by*

$$(\alpha, \beta)_n \equiv (\alpha, \beta)_v^{\frac{q-1}{n}} \pmod{\mathfrak{p}_F} \quad \text{for all } \alpha, \beta \in F^*.$$

In particular for a number field K , a finite prime \mathfrak{p} of K and $n \mid \#(\mu(K))$:

$$\left(\frac{a, b}{\mathfrak{p}}\right)_n \equiv (a, b)_{v_{\mathfrak{p}}}^{\frac{N(\mathfrak{p})-1}{n}} \quad \text{for all } a, b \in K^* \quad \square$$

In algebraic K-theory one has the following short exact sequence for a number field F :

$$1 \longrightarrow K_2(\mathcal{O}_F) \longrightarrow K_2(F) \xrightarrow{(\tau_{\mathfrak{p}})_{\mathfrak{p}}} \bigoplus_{\mathfrak{p} \in \text{Max}(\mathcal{O}_F)} (\mathcal{O}_F/\mathfrak{p})^* \longrightarrow 1, \quad (16.2)$$

where the $\tau_{\mathfrak{p}}$ are given by the tame symbols $(a, b) \mapsto (a, b)_{v_{\mathfrak{p}}}$. The group $K_2(\mathcal{O}_F)$ is finite by a theorem of Garland. It is known as the *tame kernel* of F . It measures how far Steinberg symbols differ from tame symbols. At each of the three places

in the short exact sequence the exactness is far from trivial when starting from the elementary definitions of K -groups as given in [29] or [26]. Hilbert symbols are more general than tame symbols. For these we have an exact sequence

$$K_2(F) \longrightarrow \bigoplus_{\substack{\mathfrak{p} \text{ finite or} \\ \text{real infinite}}} \mu(F_{\mathfrak{p}}) \longrightarrow \mu(F) \longrightarrow 1.$$

This is known as *Moore's Reciprocity Uniqueness Theorem*, see [29], §16. The kernel of the first map is called the *wild kernel* of the number field F , it is a subgroup of the tame kernel since every tame symbol is essentially a Hilbert symbol. The groups $K_0(\mathcal{O}_F)$ and $K_1(\mathcal{O}_F)$ are respectively $\mathbb{Z} \times \mathcal{C}(F)$ and \mathcal{O}_F^* . The last is far from obvious, it is a theorem of Bass, Milnor and Serre [1] and is equivalent to the surjectivity of $(\tau_{\mathfrak{p}})_{\mathfrak{p}}$ in the short exact sequence (16.2).

16.4 Power residue symbols

For the number field \mathbb{Q} we have the Legendre symbol and its generalization, the Jacobi symbol. These notions will be generalized for number fields containing sufficiently many roots of unity.

16.36 Lemma. *Let K be a number field with $\zeta_n \in K$ and let $\mathfrak{p} \in \text{Max}(\mathcal{O}_K)$ such that $\mathfrak{p} \nmid n$. Then the map*

$$\mu_n = \langle \zeta_n \rangle \longrightarrow (\mathcal{O}_K/\mathfrak{p})^*,$$

induced by the canonical map $\mathcal{O}_K \rightarrow \mathcal{O}_K/\mathfrak{p}$, is injective.

PROOF. Divide both sides of $X^n - 1 = \prod_{\zeta \in \mu_n} (X - \zeta)$ by $(X - 1)$ and substitute 1 for X :

$$n = \prod_{\substack{\zeta \in \mu_n \\ \zeta \neq 1}} (1 - \zeta).$$

Since $\mathfrak{p} \nmid n$, We have $\zeta \not\equiv 1 \pmod{\mathfrak{p}}$ for all $\zeta \neq 1$. □

16.37 Definition. Let K be a number field containing μ_n , \mathfrak{p} a finite prime of K and $\alpha \in \mathcal{O}_K$ such that $\mathfrak{p} \nmid n, \alpha$. Then $\bar{\alpha}^{\frac{N(\mathfrak{p})-1}{n}}$ is an n -th root of unity of $\mathcal{O}_K/\mathfrak{p}$. So there is a unique $\zeta \in \mu_n$ such that

$$\alpha^{\frac{N(\mathfrak{p})-1}{n}} \equiv \zeta \pmod{\mathfrak{p}}.$$

This unique ζ is denoted by $\left(\frac{\alpha}{\mathfrak{p}}\right)_n$ and the map

$$\mathcal{O}_K \setminus \mathfrak{p} \longrightarrow \mu_n, \quad \alpha \mapsto \left(\frac{\alpha}{\mathfrak{p}}\right)_n$$

is called the n -the *power residue symbol*.

The power residue symbol is closely connected to a tame Hilbert symbol:

16.38 Lemma. *Let K be a number field containing μ_n , \mathfrak{p} a finite prime of K , $\alpha, \beta \in \mathcal{O}_K$ relatively prime to each other and $\mathfrak{p} \nmid n, \alpha$. Then*

$$\left(\frac{\beta, \alpha}{\mathfrak{p}}\right)_n = \left(\frac{\alpha}{\mathfrak{p}}\right)_n^{v_{\mathfrak{p}}(\beta)}$$

PROOF. By Corollary 16.35:

$$\left(\frac{\beta, \alpha}{\mathfrak{p}}\right)_n \equiv (\beta, \alpha)_{v_{\mathfrak{p}} \frac{N(\mathfrak{p})-1}{n}} \equiv \alpha^{v_{\mathfrak{p}}(\beta) \frac{N(\mathfrak{p})-1}{n}} \equiv \left(\frac{\alpha}{\mathfrak{p}}\right)_n^{v_{\mathfrak{p}}(\beta)} \pmod{\mathfrak{p}} \quad \square$$

The power residue symbol is a generalization of the Legendre symbol.

16.39 Proposition. *In the notations of the definition we have:*

- (i) $\left(\frac{\alpha}{\mathfrak{p}}\right)_n = \left(\frac{\beta}{\mathfrak{p}}\right)_n$ for all $\alpha, \beta \in \mathcal{O}_K \setminus \mathfrak{p}$ with $\alpha \equiv \beta \pmod{\mathfrak{p}}$.
- (ii) $\left(\frac{\alpha\beta}{\mathfrak{p}}\right)_n = \left(\frac{\alpha}{\mathfrak{p}}\right)_n \left(\frac{\beta}{\mathfrak{p}}\right)_n$ for all $\alpha, \beta \in \mathcal{O}_K \setminus \mathfrak{p}$.
- (iii) $\left(\frac{\zeta}{\mathfrak{p}}\right)_n = \zeta^{\frac{N(\mathfrak{p})-1}{n}}$ for all $\zeta \in \mu_n$.
- (iv) $\left(\frac{\alpha}{\mathfrak{p}}\right)_n = 1 \iff \alpha$ is an n -th power modulo \mathfrak{p} .

PROOF. (i), (ii) and (iii) follow directly from the definition of the power residue symbol. For (iv) note that, because the group $(\mathcal{O}_K/\mathfrak{p})^*$ is cyclic of order $q-1$, the n -th powers form a subgroup of order $\frac{N(\mathfrak{p})-1}{n}$ and this subgroup is the kernel of

$$(\mathcal{O}_K/\mathfrak{p})^* \longrightarrow (\mathcal{O}_K/\mathfrak{p})^*, \quad \bar{\alpha} \mapsto \bar{\alpha}^{\frac{N(\mathfrak{p})-1}{n}}. \quad \square$$

We have the following generalization of the Jacobi symbol.

16.40 Definition. Let K be a number field containing μ_n , \mathfrak{b} a nonzero ideal of \mathcal{O}_K relatively prime to n and $\alpha \in \mathcal{O}_K \setminus \{0\}$ relatively prime to \mathfrak{b} . The symbol $\left(\frac{\alpha}{\mathfrak{b}}\right)_n$ is defined as follows

$$\left(\frac{\alpha}{\mathfrak{b}}\right)_n = \prod_{\mathfrak{p}|\mathfrak{b}} \left(\frac{\alpha}{\mathfrak{p}}\right)_n^{v_{\mathfrak{p}}(\mathfrak{b})}.$$

For \mathfrak{b} a principal ideal, say $\mathfrak{b} = (\beta)$, we will write $\left(\frac{\alpha}{\beta}\right)_n$ for $\left(\frac{\alpha}{\mathfrak{b}}\right)_n$.

16.41 Proposition. *In the notation of the definition we have:*

- (i) $\left(\frac{\alpha}{\mathfrak{b}}\right)_n = \left(\frac{\beta}{\mathfrak{b}}\right)_n$ for all $\alpha, \beta \in \mathcal{O}_K$ relatively prime to \mathfrak{b} and $\alpha \equiv \beta \pmod{\mathfrak{b}}$.
- (ii) $\left(\frac{\alpha\beta}{\mathfrak{b}}\right)_n = \left(\frac{\alpha}{\mathfrak{b}}\right)_n \left(\frac{\beta}{\mathfrak{b}}\right)_n$ for all $\alpha, \beta \in \mathcal{O}_K$ relatively prime to \mathfrak{b} .
- (iii) $\left(\frac{\alpha}{\mathfrak{a}\mathfrak{b}}\right)_n = \left(\frac{\alpha}{\mathfrak{a}}\right)_n \left(\frac{\alpha}{\mathfrak{b}}\right)_n$ for all $\mathfrak{a}, \mathfrak{b} \in \mathbb{I}^{n+}(K)$ relatively prime to α .
- (iv) $\left(\frac{\zeta}{\mathfrak{b}}\right)_n = \zeta^{\frac{N(\mathfrak{b})-1}{n}}$ for all $\zeta \in \mu_n$.

PROOF. (i), (ii) and (iii) follow directly from the definition of the symbol. (iv) is easily proved by induction on the number of prime ideal factors of \mathfrak{b} . For the induction step use

$$0 \equiv (N(\mathfrak{a}) - 1)(N(\mathfrak{b}) - 1) = N(\mathfrak{a}\mathfrak{b}) - 1 - N(\mathfrak{a}) + 1 - N(\mathfrak{b}) + 1 \pmod{n^2},$$

which implies

$$\frac{N(\mathfrak{a}\mathfrak{b}) - 1}{n} \equiv \frac{N(\mathfrak{a}) - 1}{n} + \frac{N(\mathfrak{b}) - 1}{n} \pmod{n}. \quad \square$$

Hilbert's reciprocity

The product formula for Hilbert symbols leads to *Hilbert's reciprocity*:

16.42 Hilbert's Reciprocity Theorem. *Let K be a number field containing μ_n and $\alpha, \beta \in \mathcal{O}_K$ prime to each other and to n . Then*

$$\left(\frac{\alpha}{\beta}\right)_n \left(\frac{\beta}{\alpha}\right)_n^{-1} = \prod_{\mathfrak{p}|n_\infty} \left(\frac{\alpha, \beta}{\mathfrak{p}}\right)_n.$$

PROOF. The product formula yields

$$\prod_{\mathfrak{p}|\alpha} \left(\frac{\alpha, \beta}{\mathfrak{p}}\right)_n \cdot \prod_{\mathfrak{p}|\beta} \left(\frac{\alpha, \beta}{\mathfrak{p}}\right)_n \cdot \prod_{\mathfrak{p}|n_\infty} \left(\frac{\alpha, \beta}{\mathfrak{p}}\right)_n = 1.$$

By lemma 16.38

$$\prod_{\mathfrak{p}|\alpha} \left(\frac{\alpha, \beta}{\mathfrak{p}}\right)_n = \prod_{\mathfrak{p}|\alpha} \left(\frac{\beta}{\mathfrak{p}}\right)_n^{v_{\mathfrak{p}}(\alpha)} = \left(\frac{\beta}{\alpha}\right)_n. \quad \square$$

For roots of unity we have:

16.43 First supplement to Hilbert's Reciprocity Theorem. *Let K be a number field containing μ_n , $\zeta \in \mu_n$ and $\beta \in \mathcal{O}_K$ prime to n . Then*

$$\left(\frac{\zeta}{\beta}\right)_n = \prod_{\mathfrak{p}|n\infty} \left(\frac{\zeta, \beta}{\mathfrak{p}}\right)_n = \zeta^{\frac{N(\beta)-1}{n}}.$$

PROOF. In this case the product formula yields

$$\prod_{\mathfrak{p}|\beta} \left(\frac{\zeta, \beta}{\mathfrak{p}}\right)_n \cdot \prod_{\mathfrak{p}|n\infty} \left(\frac{\zeta, \beta}{\mathfrak{p}}\right)_n = 1.$$

Apply Lemma 16.38 and Proposition 16.41(iv). □

For divisors of n :

16.44 Second supplement to Hilbert's Reciprocity Theorem. *Let K be a number field containing μ_n and $\lambda, \beta \in \mathcal{O}_K$ such that $\lambda \mid n$ and $\beta \in \mathcal{O}_K$ prime to n . Then*

$$\left(\frac{\lambda}{\beta}\right)_n = \prod_{\mathfrak{p}|n\infty} \left(\frac{\lambda, \beta}{\mathfrak{p}}\right)_n.$$

PROOF. As for the first supplement the formula follows from the product formula and Lemma 16.38. □

16.5 Some classical reciprocities

The classical reciprocities for power residue symbols follow from Hilbert's Reciprocity Theorem. In this section this is done for quadratic, cubic and quartic reciprocity. Also a reciprocity of Eisenstein for the l -th power residue symbol is derived from Hilbert's theorem. These classical n -th power reciprocities are reciprocities in the cyclotomic field $\mathbb{Q}(\zeta_n)$.

Quadratic reciprocity

We have seen already two proofs: one using extensions of finite fields, the other the splitting behavior of primes in a cyclotomic field. The proof given here indicates how one can proceed in other cases. Hilbert's reciprocity for the field \mathbb{Q} and $n = 2$:

16.45 Proposition.

- (i) $\left(\frac{a}{b}\right)_2 \left(\frac{b}{a}\right)_2 = \left(\frac{a,b}{\infty}\right)_2 \left(\frac{a,b}{2}\right)_2$ for all relatively prime odd $a, b \in \mathbb{Z}$.
- (ii) $\left(\frac{-1}{b}\right)_2 = \left(\frac{-1,b}{2}\right)_2 = (-1)^{\frac{b-1}{2}}$ for all odd $b \in \mathbb{Z}$.
- (iii) $\left(\frac{2}{b}\right)_2 = \left(\frac{2,b}{2}\right)_2$ for all odd $b \in \mathbb{Z}$. □

The subindex 2 will be omitted in this subsection. Note that $\left(\frac{a}{b}\right)$ with $b > 0$ is the Jacobi symbol and that $\left(\frac{a}{b}\right) = \left(\frac{a}{|b|}\right)$. The symbol $\left(\frac{a,b}{\infty}\right)$ is the following symbol on \mathbb{R} :

$$\left(\frac{a,b}{\infty}\right) = -1 \iff a < 0 \text{ and } b < 0.$$

We compute the Hilbert symbol $\left(\frac{a,b}{2}\right)$ for relatively prime nonzero $a, b \in \mathbb{Z}$.

16.46 Lemma. For odd $a \in \mathbb{Z}$ there are unique $j, k \in \{0, 1\}$ such that

$$a \equiv (-1)^j 5^k \equiv (-1)^j (1 + 4k) \pmod{8}$$

and j and k are determined by

$$j \equiv \frac{a-1}{2} \pmod{2} \quad \text{and} \quad k \equiv \frac{a^2-1}{8} \pmod{2}.$$

PROOF. $(-1)^j a \equiv 1 \pmod{4}$ for a unique $j \in \{0, 1\}$ and subsequently $(-1)^j a \equiv 1 + 4k \pmod{8}$ for a unique $k \in \{0, 1\}$. Clearly, $j \equiv \frac{a-1}{2}$ and $a^2 \equiv 1 + 8k \pmod{16}$ implies $\frac{a^2-1}{8} \equiv k \pmod{2}$. □

16.47 Proposition. Let a and b be odd integers. Then

- (i) $\left(\frac{a,b}{2}\right) = (-1)^{\frac{a-1}{2} \frac{b-1}{2}}$.
- (ii) $\left(\frac{-1,b}{2}\right) = (-1)^{\frac{b-1}{2}}$.
- (iii) $\left(\frac{2,b}{2}\right) = (-1)^{\frac{b^2-1}{8}}$.

PROOF. We will use the Proposition 16.45, Lemma 16.46, the inclusion $1 + 8\mathbb{Z}_2 \subset \mathbb{Q}_2^{*2}$ given by Theorem 11.22 and the fact that a Hilbert symbol is a Steinberg symbol. Put $j = \frac{a-1}{2}$, $s = \frac{b-1}{2}$, $k = \frac{a^2-1}{8}$ and $t = \frac{b^2-1}{8}$.

$$(i) \begin{aligned} \left(\frac{a, b}{2}\right) &= \left(\frac{(-1)^j 5^k, (-1)^s 5^t}{2}\right) = \left(\frac{-1, -1}{2}\right)^{js} \left(\frac{-1, 5}{2}\right)^{jt+sk} \left(\frac{5, 5}{2}\right)^{kt}, \\ \left(\frac{5, 5}{2}\right) &= \left(\frac{-1, 5}{2}\right) = \left(\frac{-1, 5}{5}\right) = \left(\frac{-1}{5}\right) = 1 \\ \text{and } \left(\frac{-1, -1}{2}\right) &= \left(\frac{-1, -1}{\infty}\right) = -1. \end{aligned}$$

(ii) This is Proposition 16.45(ii).

$$(iii) \begin{aligned} \left(\frac{2, b}{2}\right) &= \left(\frac{2, (-1)^s 5^t}{2}\right) = \left(\frac{2, -1}{2}\right)^s \left(\frac{2, 5}{2}\right)^t = \left(\frac{2, 5}{2}\right)^t \\ \text{and } \left(\frac{2, 5}{2}\right) &= \left(\frac{2, 5}{5}\right) = \left(\frac{2}{5}\right) = -1. \end{aligned} \quad \square$$

Quadratic reciprocity follows from the Propositions 16.45 and 16.47:

16.48 Theorem.

(i) *The Quadratic Reciprocity Law:*

$$\left(\frac{a}{b}\right) \left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2} \frac{b-1}{2}} \quad \text{for } a, b \in \mathbb{N}^* \text{ odd and relatively prime.}$$

(ii) *The first supplement:* $\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}}$ for odd $b \in \mathbb{N}^*$.

(iii) *The second supplement:* $\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}}$ for odd $b \in \mathbb{N}^*$. □

Cubic reciprocity

Put $\lambda = 1 - \zeta_3$. Then $(3) = (\lambda)^2$ in $\mathbb{Z}[\zeta_3]$. Hilbert’s reciprocity for the field $\mathbb{Q}(\zeta_3)$ and $n = 3$:

16.49 Proposition.

(i) $\left(\frac{\alpha}{\beta}\right)_3 \left(\frac{\beta}{\alpha}\right)_3^{-1} = \left(\frac{\alpha, \beta}{\lambda}\right)_3$ for all relatively prime $\alpha, \beta \in \mathbb{Z}[\zeta_3]$ with $\lambda \nmid \alpha, \beta$.

(ii) $\left(\frac{\zeta_3}{\beta}\right)_3 = \left(\frac{\zeta_3, \beta}{\lambda}\right)_3 = (-1)^{\frac{N(\beta)-1}{3}}$ for all $\beta \in \mathbb{Z}[\zeta_3]$ with $\lambda \nmid \beta$.

(iii) $\left(\frac{\lambda}{\beta}\right)_3 = \left(\frac{\lambda, \beta}{\lambda}\right)_3$ for all $\beta \in \mathbb{Z}[\zeta_3]$ with $\lambda \nmid \beta$. □

For simplicity of notation in this subsection the subindex 3 is often omitted.

16.50 Lemma. *Let $\alpha \in \mathbb{Z}[\zeta]$ such that $\lambda \nmid \alpha$. Then there is a unique root of unity $\xi \in \langle -\zeta \rangle = \mathbb{Z}[\zeta]^*$ such that*

$$\xi\alpha \equiv 1 \pmod{3}.$$

PROOF. The canonical map $\mathbb{Z}[\zeta] \rightarrow \mathbb{Z}[\zeta]/3$ induces an isomorphism

$$\langle -\zeta \rangle \xrightarrow{\sim} (\mathbb{Z}[\zeta]/3)^*. \quad \square$$

16.51 Definition. An $\alpha \in \mathbb{Z}[\zeta]$ is called *primary* if $\alpha \equiv 1 \pmod{3}$.

16.52 Lemma. *For primary $\alpha \in \mathbb{Z}[\zeta]$ there are unique $j, k \in \{-1, 0, 1\}$ such that*

$$\alpha \equiv (1 + 3\zeta)^j(-2 - 3\zeta)^k = (1 + 3j\zeta)(1 + 3k(-1 - \zeta)) \equiv 1 - 3k + 3(j + k)\zeta \pmod{9}.$$

PROOF. The group $(1 + 3\mathbb{Z}[\zeta])/(1 + 9\mathbb{Z}[\zeta]) = \text{Ker}((\mathbb{Z}[\zeta]/9)^* \rightarrow (\mathbb{Z}[\zeta]/3)^*)$ is a 3-elementary abelian group of rank 2. The classes represented by $1 + 3\zeta$ and $-2 - 3\zeta$ form a basis. \square

16.53 Proposition. *Let α and β be primary elements of $\mathbb{Z}[\zeta]$, where in particular $\beta = 1 + 3m + 3n\zeta$ with $m, n \in \mathbb{Z}$. Then*

$$(i) \quad \left(\frac{\alpha, \beta}{\lambda}\right) = 1.$$

$$(ii) \quad \left(\frac{-\zeta, \beta}{\lambda}\right) = \zeta^{\frac{N(\beta)-1}{3}}.$$

$$(iii) \quad \left(\frac{\lambda, \beta}{\lambda}\right) = \zeta^m.$$

PROOF. We use the Proposition 16.49, Lemma 16.52, the inclusion $1 + 9\mathbb{Z}[\zeta]_\lambda \subset \mathbb{Q}(\zeta)_\lambda^{*3}$ given by Theorem 11.22 and Steinberg relations. Let $j, k, s, t \in \mathbb{Z}$ be such that

$$\alpha \equiv (1 + 3\zeta)^j(-2 - 3\zeta)^k \pmod{9} \quad \text{and} \quad \beta \equiv (1 + 3\zeta)^s(-2 - 3\zeta)^t.$$

Then

$$\beta \equiv (1 + 3s\zeta)(1 - 3t(1 + \zeta)) \equiv 1 + 3(-t + (t - s)\zeta) \pmod{9},$$

so $s \equiv n - m \pmod{3}$ and $t \equiv -m \pmod{3}$.

(i) The ideals $(1 + 3\zeta)$ and $(-2 - 3\zeta)$ are the two prime ideals above 7. We have

$$\begin{aligned} \left(\frac{\alpha, \beta}{\lambda}\right) &= \left(\frac{(1 + 3\zeta)^j(-2 - 3\zeta)^k, (1 + 3\zeta)^s(-2 - 3\zeta)^t}{\lambda}\right) \\ &= \left(\frac{1 + 3\zeta, -2 - 3\zeta}{\lambda}\right)^{js-kt} \end{aligned}$$

and

$$\begin{aligned} \left(\frac{1+3\zeta, -2-3\zeta}{\lambda} \right) &= \left(\frac{1+3\zeta}{-2-3\zeta} \right) \left(\frac{-2-3\zeta}{1+3\zeta} \right)^{-1} = \left(\frac{1+3\zeta}{3+\zeta} \right) \left(\frac{-2-3\zeta}{2-\zeta} \right)^{-1} \\ &= \left(\frac{-8}{3+\zeta} \right) \left(\frac{-8}{2-\zeta} \right)^{-1} = 1. \end{aligned}$$

(ii) This is Proposition 16.49(ii).

$$\begin{aligned} \text{(iii)} \quad \left(\frac{\lambda, \beta}{\lambda} \right) &= \left(\frac{\lambda, 1+3\zeta}{\lambda} \right)^s \left(\frac{\lambda, -2-3\zeta}{\lambda} \right)^t = \left(\frac{\lambda}{2-\zeta} \right)^s \left(\frac{\lambda}{3+\zeta} \right)^t \\ &= \left(\frac{-1}{2-\zeta} \right)^s \left(\frac{4}{3+\zeta} \right)^t = \left(\frac{\zeta}{3+\zeta} \right)^t = \zeta^{2t} = \zeta^m. \quad \square \end{aligned}$$

Cubic Reciprocity follows from the Propositions 16.49 and 16.53:

16.54 Theorem.

(i) *The Cubic Reciprocity Law:*

$$\left(\frac{\alpha}{\beta} \right)_3 = \left(\frac{\beta}{\alpha} \right)_3 \quad \text{for all primary } \alpha, \beta \in \mathbb{Z}[\zeta_3] \text{ which are relatively prime.}$$

(ii) *The first supplement:* $\left(\frac{\zeta}{\beta} \right)_3 = \zeta_3^{\frac{N(\beta)-1}{3}}$ for all $\beta \in \mathbb{Z}[\zeta_3]$ with $\lambda \nmid \beta$.

(iii) *The second supplement:* $\left(\frac{\lambda}{\beta} \right)_3 = \zeta_3^m$ for all primary $\beta \in \mathbb{Z}[\zeta_3]$ with m given by $\beta = 1 + 3(m + n\zeta_3)$, $m, n \in \mathbb{Z}$. □

Quartic Reciprocity

Put $\lambda = 1 + i$. Then $(i) = (\lambda)^2$ in the ring $\mathbb{Z}[i]$. Hilbert's Reciprocity for $\mathbb{Q}(i)$ and $n = 4$:

16.55 Proposition.

(i) $\left(\frac{\alpha}{\beta} \right)_4 \left(\frac{\beta}{\alpha} \right)_4^{-1} = \left(\frac{\alpha, \beta}{\lambda} \right)_4$ for all relatively prime $\alpha, \beta \in \mathbb{Z}[i]$ with $\lambda \nmid \alpha, \beta$.

(ii) $\left(\frac{i}{\beta} \right)_4 = \left(\frac{i, \beta}{\lambda} \right)_4 = i^{\frac{N(\beta)-1}{4}}$ for all $\beta \in \mathbb{Z}[i]$ with $\lambda \nmid \beta$.

(iii) $\left(\frac{\lambda}{\beta} \right)_4 = \left(\frac{\lambda, \beta}{\lambda} \right)_4$ for all $\beta \in \mathbb{Z}[i]$ with $\lambda \nmid \beta$. □

In the notation we suppress in this subsection the use of the subindex 4.

16.56 Lemma. *Let $\alpha \in \mathbb{Z}[i]$ such that $\lambda \nmid \alpha$. Then there is a unique root of unity $\zeta \in \langle i \rangle = \mathbb{Z}[i]^*$ such that*

$$\zeta \alpha \equiv 1 \pmod{\lambda^3}.$$

PROOF. The canonical map $\mathbb{Z}[i] \rightarrow \mathbb{Z}[i]/\lambda^3$ induces an isomorphism

$$\langle i \rangle \xrightarrow{\sim} (\mathbb{Z}[i]/\lambda^3)^*. \quad \square$$

16.57 Definition. An $\alpha \in \mathbb{Z}[i]$ is called *primary* if $\alpha \equiv 1 \pmod{\lambda^3}$. So the primary elements of $\mathbb{Z}[i]$ are the elements $1 + 2a + 2bi$ with $a \equiv b \pmod{2}$.

16.58 Lemma. *For primary $\alpha \in \mathbb{Z}[i]$ there are unique $j, k \in \{0, 1, 2, 3\}$ such that*

$$\alpha \equiv (1 + \lambda^3)^j (1 + \lambda^4)^k \pmod{\lambda^7}.$$

PROOF. The abelian group $(1 + \lambda^3\mathbb{Z}[i])/(1 + \lambda^7\mathbb{Z}[i])$ is of order 16. The classes of $1 + \lambda^3$ and $1 + \lambda^4$ are of order 4:

$$\begin{aligned} (1 + \lambda^3)^2 &= 1 + 2\lambda^3 + \lambda^6 = 1 + 2\lambda^4 - \lambda^5 + \lambda^6 = 1 + \lambda^5, \\ (1 + \lambda^4)^2 &\equiv 1 + 2\lambda^4 \equiv 1 + 2\lambda^5 - \lambda^6 \equiv 1 + \lambda^6 \pmod{\lambda^7}, \\ (1 + \lambda^5)^2 &\equiv (1 + \lambda^6)^2 \equiv 1 \pmod{\lambda^7}. \end{aligned} \quad \square$$

By Theorem 11.22, the subgroup $1 + \lambda^7\mathbb{Z}[i]$ of $\mathbb{Q}(i)_\lambda^*$ consists of 4-th powers.

16.59 Proposition. *Let α and β be primary elements of $\mathbb{Z}[i]$, where in particular $\beta = 1 + 2a + 2bi$ with $a, b \in \mathbb{Z}$ and $a \equiv b \pmod{2}$. Then*

- (i) $\left(\frac{\alpha, \beta}{\lambda}\right) = (-1)^{\frac{N(\alpha)-1}{4} \frac{N(\beta)-1}{4}}.$
- (ii) $\left(\frac{i, \beta}{\lambda}\right) = i^{\frac{N(\beta)-1}{4}} = i^{-a}.$
- (iii) $\left(\frac{\lambda, \beta}{\lambda}\right) = i^{\frac{a-b-2b^2}{2}}.$

PROOF.

(i) The maps

$$(1 + \lambda^3\mathbb{Z}[i]) \times (1 + \lambda^3\mathbb{Z}[i]) \longrightarrow \mu_4, \quad (\alpha, \beta) \mapsto \left(\frac{\alpha, \beta}{\lambda}\right)$$

and

$$(1 + \lambda^3\mathbb{Z}[i]) \times (1 + \lambda^3\mathbb{Z}[i]) \longrightarrow \mu_4, \quad (\alpha, \beta) \mapsto (-1)^{\frac{N(\alpha)-1}{4} \frac{N(\beta)-1}{4}}$$

are both bimultiplicative, so by Lemma 16.58 it suffices to verify the formula for $\alpha, \beta \in \{1 + \lambda^3, 1 + \lambda^4\}$. We have by Proposition 16.55(i)

$$\left(\frac{1 + \lambda^3, 1 + \lambda^4}{\lambda}\right) = \left(\frac{-1 + 2i, -3}{\lambda}\right) = \left(\frac{-3}{1 - 2i}\right)^{-1} \left(\frac{-1 + 2i}{3}\right).$$

$N(1 - 2i) = 5$ and $N(3) = 9$, so by definition of the power residue symbol

$$\left(\frac{-3}{1 - 2i}\right) \equiv (-3)^{\frac{5-1}{4}} \equiv -3 \equiv -i \pmod{1 - 2i}$$

and

$$\left(\frac{1 - 2i}{3}\right) \equiv (-1 + 2i)^{\frac{9-1}{4}} \equiv -3 - 4i \equiv -i \pmod{3}.$$

hence

$$\left(\frac{1 + \lambda^3, 1 + \lambda^4}{\lambda}\right) = (-i)^{-1}(-i) = 1 = (-1)^{1 \cdot 2}.$$

By the Steinberg relations and Proposition 16.55(ii)

$$\left(\frac{1 + \lambda^3, 1 + \lambda^3}{\lambda}\right) = \left(\frac{-1, 1 + \lambda^3}{\lambda}\right) = -1$$

and we have $\frac{N(-1+2i)-1}{4} = 1$ and $\frac{N(-1)-1}{4} = 0$. Also

$$\left(\frac{1 + \lambda^4, 1 + \lambda^4}{\lambda}\right) = \left(\frac{-1, 1 + \lambda^4}{\lambda}\right) = (-1)^2 = 1$$

and $\frac{N(-3)-1}{4} = 2$.

(ii) The first identity is Proposition 16.55(ii). For the second note that

$$\frac{N(\beta) - 1}{4} = \frac{(1 + 2a)^2 + 4b^2 - 1}{4} = a + a^2 + b^2 \equiv (a + b)^2 - a \equiv -a \pmod{4}.$$

(iii) First we show that the map

$$1 + \lambda^3 \mathbb{Z}[i] \longrightarrow \mathbb{Z}/4, \quad 1 + 2(a + bi) \mapsto \text{class of } \frac{a - b - 2b^2}{2}$$

is a homomorphism. For $a, b, c, d \in \mathbb{Z}$ with $a \equiv b \pmod{2}$ and $c \equiv d \pmod{2}$ we have

$$(1 + 2(a + bi))(1 + 2(c + di)) = 1 + 2((a + c + 2ac - 2bd) + (b + d + 2ad + 2bc)i)$$

and

$$(a + c + 2ac - 2bd) - (b + d + 2ad + 2bc) - 2(b + d + 2ad + 2bc)^2$$

$$\begin{aligned} &\equiv (a + c + 2ac - 2bd) - (b + d + 2ad + 2bc) - 2b^2 - 4bd - 2d^2 \\ &\equiv (a - b - 2b^2) + (c - d - 2d^2) + 2(a - b)(c - d) \\ &\equiv (a - b - 2b^2) + (c - d - 2d^2) \pmod{8}. \end{aligned}$$

Division by 2 shows that the map is a homomorphism. The subgroup $1 + \lambda^7\mathbb{Z}[i]$ (the case $a \equiv b \equiv 0 \pmod{2}$) is in the kernel. It suffices to verify the formula for $\beta = -1 + 2i$ and $\beta = -3$. By Proposition 16.55(iv)

$$\left(\frac{\lambda, -1 + 2i}{\lambda}\right) = \left(\frac{\lambda}{-1 + 2i}\right) \equiv \lambda \equiv -1 \pmod{-1 + 2i}$$

and

$$\left(\frac{\lambda, -3}{\lambda}\right) = \left(\frac{\lambda}{-3}\right) \equiv \lambda^2 \equiv -i \pmod{3}.$$

Indeed, the images of $-1 + 2i = 1 + 2(-1 + i)$ and $-3 = 1 + 2(-2)$ are the classes of 2 and -1 respectively. \square

Eisenstein's Reciprocity Theorem

Now let l be an odd prime. We will show that a reciprocity theorem of Eisenstein (Theorem 16.62) concerning the l -th power residue symbol on the cyclotomic field $\mathbb{Q}(\zeta_l)$ is a consequence of the product formula for Hilbert symbols as well.

The prime l totally ramifies in $\mathbb{Q}(\zeta_l)$ and the prime ideal above l is principal: $(l) = (1 - \zeta_l)^{l-1}$. Put $\lambda = 1 - \zeta_l$. The prime ideal $\mathfrak{l} = (\lambda)$ is of norm l .

16.60 Lemma. *Let $\alpha \in \mathbb{Z}[\zeta_l]$ such that $\lambda \nmid \alpha$. Then there are unique $\zeta \in \mu_l$ and $a \in \{1, \dots, l-1\}$ such that*

$$\zeta \alpha \equiv a \pmod{\lambda^2}.$$

PROOF. Since $\lambda \nmid \alpha$, the element α is invertible modulo λ^2 , that is $\bar{\alpha} \in (\mathbb{Z}[\zeta_l]/\lambda^2)^*$. The group $(\mathbb{Z}[\zeta_l]/\lambda^2)^*$ is of order $l(l-1)$. The group homomorphism

$$\mu_l \rightarrow (\mathbb{Z}[\zeta_l]/\lambda^2)^*, \quad \zeta \mapsto \bar{\zeta}$$

is injective: $\bar{\zeta}_l \neq 1$. On the other hand, the inclusion $\mathbb{Z} \rightarrow \mathbb{Z}[\zeta_l]$ induces an injection $\mathbb{F}_l^* \rightarrow (\mathbb{Z}[\zeta_l]/\lambda^2)^*$. The images of these injections are of order l and $l-1$ respectively and hence $(\mathbb{Z}[\zeta_l]/\lambda^2)^*$ is the direct product of these two subgroups. \square

16.61 Definition. An $\alpha \in \mathbb{Z}[\zeta_l]$ with $l \nmid \alpha$ is called *primary* if $\alpha \equiv a \pmod{\lambda^2}$ for a (necessarily) unique $a \in \{1, \dots, l-1\}$.

Note that for $l = 3$ we took $a = 1$ in the definition of primary. For $l = 3$ this, however, does not make a big difference.

By Lemma 16.60 for each $\beta \in \mathbb{Z}[\zeta_l]$ with $\lambda \nmid \beta$ there are unique $\zeta \in \mu_l$ and a primary $\alpha \in \mathbb{Z}[\zeta_l]$ such that $\beta = \zeta\alpha$. By Proposition 16.41 we then have

$$\left(\frac{\beta}{\mathfrak{p}}\right)_l = \left(\frac{\zeta}{\mathfrak{p}}\right)_l \left(\frac{\alpha}{\mathfrak{p}}\right)_l = \zeta^{\frac{N(\mathfrak{p})-1}{l}} \left(\frac{\alpha}{\mathfrak{p}}\right)_l.$$

16.62 Eisenstein's Reciprocity Theorem. *Let α be primary in $\mathbb{Z}[\zeta_l]$ and $b \in \mathbb{Z}$ relatively prime to l and α . Then*

$$\left(\frac{\alpha}{b}\right)_l = \left(\frac{b}{\alpha}\right)_l.$$

By Theorem 16.42 the theorem is equivalent to $\left(\frac{\alpha, b}{\lambda}\right)_l = 1$. According to Theorem 11.22 the subgroup $U_\lambda^{l+1} = 1 + \mathfrak{I}^{l+1}$ of $\mathbb{Q}(\zeta_l)^*$ is contained in $\mathbb{Q}(\zeta_l)^*$. A consequence is again that it will suffice to verify the theorem for a finite number of cases.

For the proof of the theorem we use the following lemma.

16.63 Lemma. *Let $\alpha \in \mathbb{Z}[\zeta_l]$ such that $\alpha \equiv 1 \pmod{\lambda^2}$. Then there are unique $a_2, \dots, a_l \in \{0, \dots, l-1\}$ such that*

$$\alpha \equiv (1 - \lambda)^{a_2} (1 - \lambda^3)^{a_3} \dots (1 - \lambda^l)^{a_l} \pmod{\lambda^{l+1}}.$$

PROOF. The multiplicative group $(1 + \lambda^2\mathbb{Z}[\zeta_l]) / (1 + \lambda^{l+1}\mathbb{Z}[\zeta_l])$ is an elementary l -group: for $\alpha = 1 + \lambda^2\beta$ with $\beta \in \mathbb{Z}[\zeta_l]$ we have

$$\alpha^l = 1 + \sum_{k=1}^l \binom{l}{k} \lambda^{2k} \beta^k \equiv 1 \pmod{\lambda^{l+1}},$$

because $v_l(\binom{l}{k} \lambda^{2k}) \geq l-1+2k \geq l+1$ for $1 \leq k < l$ and $v_l(\lambda^{2l}) = 2l \geq l+1$.

The group is of order $l(l-1)$ and the classes of $1 - \lambda^2, \dots, 1 - \lambda^l$ form a basis since they are independent: suppose $(1 - \lambda^k)^{a_k} \dots (1 - \lambda^l)^{a_l} \equiv 1 \pmod{\lambda^{l+1}}$, then $(1 - \lambda^k)^{a_k} \equiv 1 - a_k \lambda^k \equiv 1 \pmod{\lambda^{k+1}}$ and so $a_k \equiv 0 \pmod{l}$. \square

PROOF OF THEOREM 16.62. As mentioned above the theorem will follow from $\left(\frac{\alpha, b}{\lambda}\right)_l = 1$. Since Hilbert symbols are Steinberg symbols, we can use the identities for Steinberg symbols. Raising α and b to the power $l-1$ yields

$$\left(\frac{\alpha^{l-1}, b^{l-1}}{\lambda}\right)_l = \left(\frac{\alpha, b}{\lambda}\right)_l^{(l-1)^2} = \left(\frac{\alpha, b}{\lambda}\right)_l.$$

Since α is primary, $\alpha \equiv a \pmod{\lambda^2}$ for some $a \in \mathbb{Z}$. Because $a^{l-1} \equiv 1 \pmod{l}$ and $(l) = (\lambda)^{l-1}$, we have $\alpha^{l-1} \equiv 1 \pmod{\lambda^2}$. Therefore, we can assume that $\alpha \equiv 1 \pmod{\lambda^2}$ and $b \equiv 1 \pmod{l}$. By Lemma 16.63 there exist $a_2, \dots, a_l, c_{l-1}, c_l \in \mathbb{N}$ and $\beta, \gamma \in \mathbb{Z}[\zeta_l]$ such that $\beta, \gamma \equiv 1 \pmod{\lambda^{l+1}}$,

$$\alpha = (1 - \lambda^2)^{a_2} \cdots (1 - \lambda^l)^{a_l} \gamma \quad \text{and} \quad b = (1 - \lambda^{l-1})^{c_{l-1}} (1 - \lambda^l)^{c_l} \beta.$$

Because β and γ are l -th powers in the l -adic completion, we have

$$\left(\frac{\alpha, b}{\lambda}\right)_l = \prod_{\substack{i=2, \dots, l \\ j=l-1, l}} \left(\frac{1 - \lambda^i, 1 - \lambda^j}{\lambda}\right)_l^{a_i c_j}.$$

So it suffices to prove that $\left(\frac{1 - \lambda^i, 1 - \lambda^j}{\lambda}\right)_l = 1$ for $i \geq 2$ and $j \geq l - 1$. Apply (SS7) using the identity $\lambda^j(1 - \lambda^i) + (1 - \lambda^j) = 1 - \lambda^{i+j}$:

$$\begin{aligned} \left(\frac{\lambda^j(1 - \lambda^i), 1 - \lambda^j}{\lambda}\right)_l &= \left(\frac{\lambda^j(1 - \lambda^i), 1 - \lambda^{i+j}}{\lambda}\right)_l \left(\frac{1 - \lambda^{i+j}, 1 - \lambda^j}{\lambda}\right)_l \left(\frac{1 - \lambda^{i+j}, -1}{\lambda}\right)_l. \end{aligned}$$

Since $i + j \geq l + 1$ each factor of the right hand side equals 1, whereas for the left hand side we have by (SS3):

$$\left(\frac{\lambda^j(1 - \lambda^i), 1 - \lambda^j}{\lambda}\right)_l = \left(\frac{\lambda^j, 1 - \lambda^j}{\lambda}\right)_l \left(\frac{1 - \lambda^i, 1 - \lambda^j}{\lambda}\right)_l = \left(\frac{1 - \lambda^i, 1 - \lambda^j}{\lambda}\right)_l. \quad \square$$

EXERCISES

- Let $E : F$ be an abelian extension of local fields and Z its decomposition group. Prove that for the decomposition field $E' = E^Z$ we have

$$N_F^{E'}(E'^*) = N_F^E(E^*)\mathcal{O}_F^*$$

and that ramification index of $E : F$ is equal to the index of $N_F^E(E^*)$ in $N_F^E(E^*)\mathcal{O}_F^*$.

- Let F be a finite field and a a generator of the cyclic group F^* .
 - Prove that $K_2(F)$ is generated by the element $\{-1, a\}$ of order 1 or 2.
 - Prove that the group $K_2(F)$ is trivial for F of characteristic 2.
 - For F of odd characteristic show that there exist $a, b \in F^*$ such that $a + b = 1$, a a square of F and b a nonsquare of F . (Hint: consider the map $F \setminus \{0, 1\} \rightarrow F \setminus \{0, 1\}$: $a \mapsto 1 - a$.)
 - Show that the group $K_2(F)$ is trivial for F of odd characteristic as well.

3. Let F be a local field containing a primitive n -th root of unity. Show that the n -th Hilbert symbol on F induces a homomorphism

$$K_2(F) \longrightarrow \mu_n,$$

given on generators by $\{\alpha, \beta\} \mapsto (\alpha, \beta)_n$.

4. Prove that $\{-1, 5\} = 1$ in the K_2 of any field.
 5. Prove that $\{1 + 3\zeta_3, -2 - 3\zeta_3\} = 1$ in $K_2(\mathbb{Q}(\zeta_3))$.
 6. Let l be an odd prime number and $\alpha \in \mathbb{Z}[\zeta_l]$.

(i) Let \mathfrak{p} a finite prime of $\mathbb{Z}[\zeta_l]$ such that $\mathfrak{p} \nmid l, \alpha$. Show that

$$\overline{\left(\frac{\alpha}{\mathfrak{p}}\right)_l} = \left(\frac{\bar{\alpha}}{\bar{\mathfrak{p}}}\right)_l.$$

(ii) Assume that $\alpha \in \mathbb{R}$ and that $l \neq 3$. Prove that $\left(\frac{\alpha}{p}\right)_l = 1$ for all prime numbers $\neq l$.

7. Let l be an odd prime and p a prime $\neq l$.

(i) Show that

$$\left(\frac{\zeta_l}{p}\right)_l = \zeta_l^{\frac{l-1}{f} \cdot \frac{p^f-1}{l}},$$

where f is that order of $\bar{p} \in \mathbb{F}_l$.

(ii) Show that $p^{l-1} \equiv 1 \pmod{l^2}$ if $\left(\frac{\zeta_l}{p}\right)_l = 1$.

17 Conductor and Discriminant

The conductor and the discriminant of an abelian number field extension have much in common: their finite prime divisors are the ramifying primes. The *Conductor-Discriminant Formula* describes how they are related for an abelian number field extension $L : K$:

$$\mathfrak{d}_K(L) = \prod_{\chi \in \mathcal{H}(L:K)} \mathfrak{f}_{\chi,0}$$

($\mathfrak{f}_{\chi,0}$ is the finite part of the conductor of χ .) The formula will be proved in the last section. The Classification Theorems of local and global class field theory are used in the proof. A link between the discriminant and the conductor is the different: an ideal of \mathcal{O}_L , the prime divisors of which are the over K ramified primes of L . The different is closely connected to the ramification groups. For an understanding of this connection a detailed study of the ramification groups of a ramifying prime will be necessary.

17.1 Ramification groups of a subextension

In section 7.5 ramification groups were introduced. They were used in chapter 9 for a proof of the Kronecker-Weber Theorem. Here we will study the behavior of the ramification groups of a Galois extension $E : F$ of local fields under restriction to a Galois subextension $E' : F$. It will be shown that by another indexation of the ramification groups the index is not changed when passing from $E : F$ to $E' : F$.

We will fix for this section the following notations:

- $E : F$ a Galois extension of local fields of characteristic 0,
- G the Galois group of $E : F$,
- $n = [E : F] = \#(G)$, the degree of $E : F$,
- p the characteristic of k_F ,
- E' an intermediate field of $E : F$ such that $E : F$ is a Galois extension,
- H the Galois group of $E : E'$, a normal subgroup of G ,
- G' the Galois group of $E' : F$, so $G/H \xrightarrow{\sim} G'$
(not the commutator subgroup),

$$\begin{aligned} V_i & V_{F,i}^{(E)}, \text{ the } i\text{-th ramification group of } E : F, \\ V'_i & V_{F,i}^{(E')}, \text{ the } i\text{-th ramification group of } E' : F, \\ V''_i & V_{E',i}^{(E)}, \text{ the } i\text{-th ramification group of } E : E'. \end{aligned}$$

The ramification groups with index 0 are the inertia groups. Let's write V_{-1} for the Galois group. It coincides with the decomposition group. In G we have a descending chain of ramification groups

$$V_{-1}(= G) \supseteq V_0 \supseteq V_1 \supseteq \cdots \supseteq V_i (= \{1\}).$$

For each $\sigma \neq 1$ in G there is a unique $i \geq -1$ such that $\sigma \in V_i \setminus V_{i+1}$. By definition $\sigma \in V_i$ if and only if $v_E(\sigma(\alpha) - \alpha) \geq i + 1$ for all $\alpha \in \mathcal{O}_E$.

17.1 Notation. If $\sigma \neq 1$, then there is a least $i \in \mathbb{N}$ such that σ does not induce the identity on $\mathcal{O}_E/\mathfrak{p}_E^{i+1}$. This least i is denoted by $i(\sigma)$. For the identity automorphism 1 we put $i(1) = \infty$. So we have

$$V_{j-1} \setminus V_j = \{ \sigma \in G \mid i(\sigma) = j \}.$$

Now we start comparing the ramification groups of $E : F$ and $E' : F$. For this the following proposition fundamental. It tells us for a $\sigma' \in G'$ how the number $i(\sigma')$ is determined by the numbers $i(\sigma)$ for the $\sigma \in G$ with $\sigma|_{E'} = \sigma'$:

17.2 Proposition. *Let $\sigma' \in G'$. Then*

$$i(\sigma') = \frac{1}{e_{F'}^{(E)}} \sum_{\substack{\sigma \in G \\ \sigma|_{E'} = \sigma'}} i(\sigma).$$

PROOF (Tate). For $\sigma' = 1$ we have ∞ on both sides. So we assume that $\sigma' \neq 1$. Choose a fixed $\sigma \in G$ such that $\sigma|_{E'} = \sigma'$. Then the automorphisms in G which restricted to E' are equal to σ' are the $\sigma\tau$ with $\tau \in H$. By Proposition 11.15 there are $\gamma \in \mathcal{O}_E$ and $\gamma' \in \mathcal{O}_{E'}$ such that $\mathcal{O}_E = \mathcal{O}_F[\gamma]$ and $\mathcal{O}_{E'} = \mathcal{O}_F[\gamma']$. The formula to be shown becomes

$$v_E(\sigma(\gamma') - \gamma') = \sum_{\tau \in H} v_E(\sigma\tau(\gamma) - \gamma).$$

Let f be the minimal polynomial of γ over E' . Then

$$f(X) = \prod_{\tau \in H} (X - \tau(\gamma)) \quad \text{and} \quad f^\sigma(X) = \prod_{\tau \in H} (X - \sigma\tau(\gamma)).$$

The polynomial f^σ is the minimal polynomial of $\sigma(\gamma)$ over E' :

$$\prod_{\tau \in H} (X - \sigma\tau(\gamma)) = \prod_{\tau \in H} (X - \sigma\tau\sigma^{-1}\sigma(\gamma)) = \prod_{\tau \in H} (X - \tau\sigma(\gamma)).$$

The coefficients of f are elements of $\mathcal{O}_{E'}$. So $v_{E'}(\sigma'(\alpha) - \alpha) \geq i(\sigma')$ for each coefficient of f . Hence

$$\sigma(\gamma') - \gamma' \mid f^\sigma(\gamma) - f(\gamma) = f^\sigma(\gamma),$$

that is

$$v_E(\sigma(\gamma') - \gamma') \leq v_E(f^\sigma(\gamma)) = \sum_{\tau \in H} v_E(\gamma - \sigma\tau(\gamma)).$$

For the proof of equality put $\gamma' = g(\gamma)$ with $g \in \mathcal{O}_F[X]$. Then γ is a root of the polynomial $g(X) - \gamma' \in \mathcal{O}_{E'}[X]$. Hence $f \mid g(X) - \gamma'$, say $g(X) - \gamma' = f(X)h(X)$ with $h \in E'[X]$. Then $g^\sigma(X) - \sigma(\gamma') = f^\sigma(X)h^\sigma(X)$ and so

$$\gamma' - \sigma(\gamma') = g(\gamma) - \sigma(\gamma') = g^\sigma(\gamma) - \sigma(\gamma') = f^\sigma(\gamma)h^\sigma(\gamma),$$

from which follows $f^\sigma(\gamma) \mid \sigma(\gamma') - \gamma'$. □

We will compare the images $V_i H/H$ of V_i under the isomorphism $G/H \xrightarrow{\sim} G'$ with the groups V'_i . Let's denote $V_i H/H$ by W_i . These subgroups of G' form a descending chain

$$W_{-1}(= G') \supseteq W_0(= V'_0) \supseteq W_1 \supseteq W_2 \supseteq \dots$$

For $\sigma' \in G'$ with $\sigma' \neq 1$ there is a unique $j \in \mathbb{N}$ such that $\sigma' \in W_{j-1} \setminus W_j$, or equivalently, for $\sigma \in G$ with $\sigma|_{E'} = \sigma'$, $\sigma \in V_{j-1}H \setminus V_jH$. This j is also characterized by $\sigma H \cap V_{j-1} \neq \emptyset$ and $H \cap \sigma V_j = \emptyset$.

For $\sigma \notin H$ let $i_G^H(\sigma)$ be the greatest $j \in \mathbb{N}$ for which $\sigma H \cap V_{j-1} \neq \emptyset$. For $\sigma \in H$ we put $i_G^H(\sigma) = \infty$.

We will denote the characteristic function of a subset X of G by δ_X , so for $\sigma \in G$:

$$\delta_X(\sigma) = \begin{cases} 1 & \text{if } \sigma \in X, \\ 0 & \text{if } \sigma \notin X. \end{cases}$$

Then

$$i(\sigma) = \sum_{i=0}^{\infty} \delta_{V_i}(\sigma). \tag{17.1}$$

17.3 Lemma. *Let $\sigma \in G$ and $\sigma' = \sigma|_{E'}$. Then*

$$i(\sigma') = \sum_{i=0}^{i_G^H(\sigma)-1} \frac{1}{(V_0'' : V_i'')}.$$

PROOF. By Lemma 17.2

$$i(\sigma') = \frac{1}{e_{E'}^{(E)}} \sum_{\tau \in H} i(\sigma\tau).$$

By equation (17.1) we have

$$\sum_{\tau \in H} i(\sigma\tau) = \sum_{\tau \in H} \sum_{i=0}^{\infty} \delta_{V_i}(\sigma\tau) = \sum_{i=0}^{\infty} \sum_{\tau \in H} \delta_{V_i}(\sigma\tau) = \sum_{i=0}^{i_G^H(\sigma)-1} \#(\sigma H \cap V_i).$$

Let $\sigma H \cap V_i \neq \emptyset$, say $\tau_0 \in H$ such that $\sigma\tau_0 \in V_i$. Then for $\tau \in H$:

$$\begin{aligned} \sigma\tau \in \sigma H \cap V_i &\iff \sigma\tau_0\tau_0^{-1}\tau \in \sigma H \cap V_i \\ &\iff \tau_0^{-1}\tau \in H \cap V_i \iff \tau \in \tau_0(H \cap V_i). \end{aligned}$$

So multiplication by τ_0 yields a bijection from $H \cap V_i$ to $\sigma H \cap V_i$. In particular we have $\#(\sigma H \cap V_i) = \#(H \cap V_i) = \#(V_i'')$. It follows that

$$\sum_{\tau \in H} i(\sigma\tau) = \sum_{i=0}^{i_G^H(\sigma)-1} \#(V_i'').$$

Finally, divide by $e_{E'}^{(E)} = \#(V_0'')$. □

We extend the indexing set for the ramification groups from integers ≥ -1 to all reals:

17.4 Definition. Let $x \in \mathbb{R}$. Then

$$V_x = \begin{cases} V_{[x]} & \text{if } x > -1, \\ G & \text{if } x \leq -1. \end{cases}$$

($[x]$ is the least integer $\geq x$.)

The indexing set for the groups W_i is extended accordingly: for $x \in \mathbb{R}$ the group W_x is the image of V_x under the restriction $G \rightarrow G'$.

Now for real x we still have the equivalence:

$$\sigma \in V_x \iff i(\sigma) \geq x + 1.$$

The real function

$$x \mapsto \frac{\#(V_x)}{\#(V_0)}$$

is a step function with value $f_F^{(E)}$ for $x \leq -1$. For $m \in \mathbb{N}$ the value on the interval $(m-1, m)$ is $1/(V_0 : V_m)$. It has a jump in m exactly when $V_{m+1} \neq V_m$.

17.5 Definition. The function $\varphi = \varphi_G: \mathbb{R} \rightarrow \mathbb{R}$ is defined by

$$\varphi(x) = \int_0^x \frac{\#(V_y) dy}{\#(V_0)}.$$

The graph of this function connects the points

$$(-1, -1), (0, 0), \left(1, \frac{\#(V_1)}{\#(V_0)}\right), \dots, \left(m, \frac{\sum_{k=1}^m \#(V_k)}{\#(V_0)}\right), \dots$$

with straight lines and for $x < -1$ it has a slope $f_F^{(E)}$. In other words, it is the real function φ with $\varphi(x) = f_F^{(E)} \cdot (x + 1) - 1$ for $x \leq -1$, $\varphi(x) = x$ for $x \in [-1, 0]$ and for $x \in [m, m + 1]$ with $m \in \mathbb{N}$:

$$\varphi(x) = \frac{1}{\#(V_0)} (\#(V_1) + \dots + \#(V_m) + (x - m) \cdot \#(V_{m+1})),$$

where for $m = 0$ this means $\varphi(x) = \frac{\#(V_1)}{\#(V_0)}x$. Obviously it is a continuous function. On the interval $(m, m + 1)$ the derivative is $\frac{\#(V_{m+1})}{\#(V_0)}$. So in $m \in \mathbb{N}$ the left derivative φ'_l takes the value $\frac{\#(V_m)}{\#(V_0)}$ and for the right derivative we have $\varphi'_r(m) = \frac{\#(V_{m+1})}{\#(V_0)}$. The function φ is strictly increasing and piecewise linear with only finitely many breaks: it has a *break* in x if the left derivative $\varphi'_l(x)$ differs from the right derivative $\varphi'_r(x)$. If the function has a break in x , the x is said to be a *break point* of the function. The break points are the $m \in \mathbb{N}$ with $V_{m+1} \neq V_m$. The map φ is a homeomorphism from \mathbb{R} to itself.

Using the function φ Lemma 17.3 can be reformulated as follows:

$$i(\sigma') = \varphi_H(i_G^H(\sigma) - 1) + 1, \text{ for } \sigma \in G \text{ such that } \sigma|_{L'} = \sigma'.$$

By this identity the ramification groups in G' are related to the images of the ramification groups in G :

17.6 Proposition. $W_x = V'_{\varphi_H(x)}$ for all $x \in \mathbb{R}$.

PROOF. Let $\sigma' \in G'$ and $\sigma \in G$ such that $\sigma|_{L'} = \sigma$. Then for all $x \in \mathbb{R}$:

$$\begin{aligned} \sigma' \in V'_{\varphi_H(x)} &\iff i(\sigma') \geq \varphi_H(x) + 1 \iff \varphi_H(i_G^H(\sigma) - 1) \geq \varphi_H(x) \\ &\iff i_G^H(\sigma) - 1 \geq x \iff \sigma \in V_x H \iff \sigma' \in W_x. \quad \square \end{aligned}$$

The inverse of the homeomorphism φ will be frequently used. Therefore, a special notation is introduced:

17.7 Notation. The homeomorphism $\psi = \psi_G: \mathbb{R} \rightarrow \mathbb{R}$ is the inverse of φ_G .

Obviously, the function ψ is continuous, piecewise linear, strictly increasing and convex. For $m \in \mathbb{Z}$ its derivative on the interval $(\varphi(m), \varphi(m+1))$ is $\frac{\#(V_0)}{\#(V_m)}$, which is an integer ≥ 1 for $m \geq -1$. For the left and the right derivative of ψ in $\varphi(m)$ we have

$$\psi'_l(\varphi(m)) = \frac{\#(V_0)}{\#(V_m)} \quad \psi'_r(\varphi(m)) = \frac{\#(V_0)}{\#(V_{m+1})}.$$

Their quotient $\frac{\psi'_r(\varphi(m))}{\psi'_l(\varphi(m))}$ is an integer:

$$\psi'_{r/l}(\varphi(m)) := \frac{\psi'_r(\varphi(m))}{\psi'_l(\varphi(m))} = \frac{\#(V_m)}{\#(V_{m+1})} \in \mathbb{N}^*.$$

The function ψ has a break in x if $\psi'_{r/l}(x) \neq 1$. It has a break in x if and only if φ has a break in $\psi(x)$, that is if $x = \varphi(m)$ for some break point m of φ . So there can only be a break in x if $x \in \varphi(\mathbb{N})$. Moreover, we have:

17.8 Lemma. *Let $v \in \mathbb{N}$. Then $\psi(v) \in \mathbb{N}$.*

PROOF. Take $m = \lfloor \psi(v) \rfloor$. Then $\psi(v) \in [m, m+1]$ and

$$v \cdot \#(V_0) = \varphi(\psi(v)) \cdot \#(V_0) = \#(V_1) + \cdots + \#(V_m) + (\psi(v) - m) \cdot \#(V_{m+1}).$$

Because V_{m+1} is a subgroup of each of the groups V_0, \dots, V_m , it follows that $\#(V_{m+1}) \mid \#(V_i)$ for $i = 0, \dots, m$. So $\psi(v) - m \in \mathbb{Z}$ and therefore, $\psi(v) \in \mathbb{Z}$. \square

Using ψ , Proposition 17.6 can be reformulated as

$$V'_x = W_{\psi_H(x)} \quad \text{for all } x \in \mathbb{R}.$$

17.9 Proposition. *For all $x \in \mathbb{R}$ we have*

$$\varphi_G(x) = \varphi_{G'}(\varphi_H(x)) \quad \text{and} \quad \psi_G(x) = \psi_H(\psi_{G'}(x)).$$

PROOF. The second identity follows from the first. The functions φ_G and $\varphi_{G'} \circ \varphi_H$ both are continuous and piecewise linear. They are not differentiable in only finitely many real numbers. Let $x \in \mathbb{R}$ such that both functions are differentiable. Then

$$\begin{aligned} \frac{d}{dx}(\varphi_{G'} \circ \varphi_H)(x) &= \varphi'_{G'}(\varphi_H(x)) \varphi'_H(x) = \frac{\#(V'_{\varphi_H(x)})}{\#(V'_0)} \cdot \frac{\#(V''_x)}{\#(V''_0)} \\ &= \frac{\#(V_x H)}{\#(V_0 H)} \cdot \frac{\#(V_x \cap H)}{\#(V_0 \cap H)} = \frac{\#(V_x)}{\#(V_0)} = \varphi'_G(x). \end{aligned}$$

Because the functions are continuous at the finitely many points they are not differentiable, they are equal. \square

For the ramification groups we now introduce upper indices:

17.10 Definition. For $x \in \mathbb{R}$:

$$V_F^{(E,x)} = V_{F,\psi_G(x)}^{(E)}$$

These upper indices are compatible with the passage from an extension to a subextension:

17.11 Theorem. *The restriction $G \rightarrow G'$ induces for all $x \in \mathbb{R}$ an isomorphism*

$$V_F^{(E,x)} H/H \xrightarrow{\sim} V_{F'}^{(E',x)}.$$

PROOF. By Proposition 17.9 we have

$$V_{F'}^{(E',x)} = V_{F',\psi_{G'}(x)}^{(E')} = W_{\psi_H(\psi_{G'}(x))} = W_{\psi_G(x)}.$$

Hence $V_F^{(E',x)}$ is the image of $V_{F',\psi_{G'}(x)}^{(E')} = V_F^{(E,x)}$. □

17.12 Example. Let $m \in \mathbb{Z}$ be squarefree and $\equiv 2 \pmod{4}$. Then 2 ramifies in the quadratic number field $\mathbb{Q}(\sqrt{m})$. The local field $E = \mathbb{Q}_2(\sqrt{m})$ is of degree 2 over $F = \mathbb{Q}_2$ and $\mathcal{O}_E = \mathbb{Z}_2[\sqrt{m}]$. Let σ be the generator of $\text{Gal}(E : F)$. Then

$$i(\sigma) = v_E(\sigma(\sqrt{m}) - \sqrt{m}) = v_E(-2\sqrt{m}) = 3.$$

So $\#(V_i) = 2$ for $i \leq 2$ and V_i is trivial for $i \geq 3$. We have

$$\varphi(x) = \begin{cases} x & \text{if } x \leq 2, \\ \frac{1}{2}x + 1 & \text{if } x \geq 2 \end{cases} \quad \text{and} \quad \psi(x) = \begin{cases} x & \text{if } x \leq 2, \\ 2x - 2 & \text{if } x \geq 2. \end{cases}$$

Both functions have a break in $x = 2$. (For $m \equiv 3 \pmod{4}$ the break is in $x = 1$.)

17.13 Example. The prime 2 totally ramifies in $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. See Example 5.24. Put $E = \mathbb{Q}_2(\sqrt{2}, \sqrt{3})$ and $\alpha = \frac{\sqrt{2} + \sqrt{6}}{2}$. Then $\alpha + 1$ is a uniformizer of v_E and $\mathcal{O}_E = \mathbb{Z}_2[\alpha + 1] = \mathbb{Z}_2[\alpha]$. The extension $E : \mathbb{Q}_2$ is biquadratic. The Galois group G is generated by σ and τ given by

$$\begin{aligned} \sigma(\sqrt{2}) &= \sqrt{2}, & \tau(\sqrt{2}) &= -\sqrt{2}, \\ \sigma(\sqrt{3}) &= -\sqrt{3}, & \tau(\sqrt{3}) &= \sqrt{3}. \end{aligned}$$

We have

$$\begin{aligned} i(\sigma) &= v_E(\sigma(\alpha) - \alpha) = v_E(-\sqrt{6}) = 2, \\ i(\tau) &= v_E(\tau(\alpha) - \alpha) = v_E(-2\alpha) = 4, \\ i(\sigma\tau) &= v_E(\sigma\tau(\alpha) - \alpha) = v_E(-\sqrt{2}) = 2. \end{aligned}$$

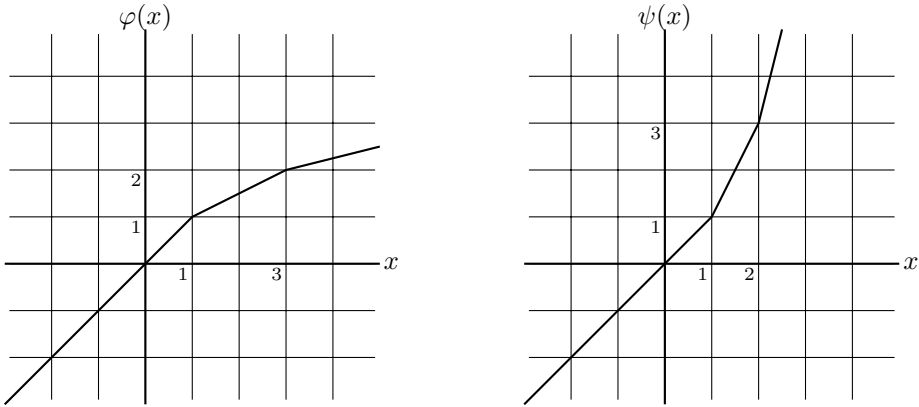


Figure 17.1: Graphs of the functions φ and ψ for the splitting of 2 in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$

So the jumps of $\#(V_x)$ are at 1 and 3. We have

$$V_1 = G \quad \text{and} \quad V_3 = \langle \tau \rangle.$$

The functions φ and ψ are

$$\varphi(x) = \begin{cases} x & \text{if } x \leq 1, \\ \frac{1}{2}x + \frac{1}{2} & \text{if } 1 \leq x \leq 3, \\ \frac{1}{4}x + \frac{5}{4} & \text{if } x \geq 3. \end{cases} \quad \psi(x) = \begin{cases} x & \text{if } x \leq 1, \\ 2x - 1 & \text{if } 1 \leq x \leq 2, \\ 4x - 5 & \text{if } x \geq 2. \end{cases}$$

See Figure 17.1. The break points of φ are 1 and 3. The break points of ψ are 1 and 2. The ramification groups with break points as upper index:

$$V^{(1)} = V_1 = G \quad \text{and} \quad V^{(2)} = V_3 = \langle \tau \rangle.$$

17.14 Example. The same field K as in the previous example, but now we consider the splitting of the prime 3. Put $E = \mathbb{Q}_3(\sqrt{2}, \sqrt{3})$. Then $E^\sigma = \mathbb{Q}_3(\sqrt{2})$, $E^\tau = \mathbb{Q}_3(\sqrt{3})$ and $E^{\sigma\tau} = \mathbb{Q}_3(\sqrt{6})$. The extension $\mathbb{Q}_3(\sqrt{2}) : \mathbb{Q}_3$ is unramified and $E : E^\sigma$ totally ramifies. So $\mathcal{O}_E = \mathcal{O}_{E^\sigma}[\sqrt{3}]$. The extensions $E : E^\tau$ and $E : E^{\sigma\tau}$ are unramified. It follows that $i(\sigma) = v_E(\sigma(\sqrt{3}) - \sqrt{3}) = v_E(-2\sqrt{3}) = 1$ and $i(\tau) = i(\sigma\tau) = 0$. The jumps of $\#(V_x)$ are at -1 and 0 . The functions φ and ψ are

$$\varphi(x) = \begin{cases} 2x + 1 & \text{if } x \leq -1, \\ x & \text{if } -1 \leq x \leq 0, \\ \frac{1}{2}x & \text{if } x \geq 0. \end{cases} \quad \psi(x) = \begin{cases} \frac{1}{2}x - \frac{1}{2} & \text{if } x \leq -1, \\ x & \text{if } -1 \leq x \leq 0, \\ 2x & \text{if } x \geq 0. \end{cases}$$

See Figure 17.2. The functions φ and ψ both have breaks in -1 and 0 . We have

$$V^{(-1)} = V_{-1} = G \quad \text{and} \quad V^{(0)} = V_0 = \langle \sigma \rangle.$$

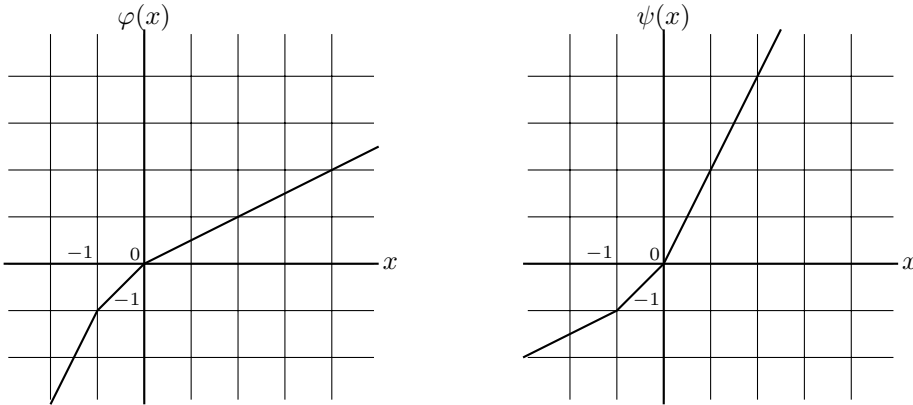


Figure 17.2: Graphs of the functions φ and ψ for the splitting of 3 in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$

17.15 Example. Let $K = \mathbb{Q}(\sqrt[4]{2}, i)$. Put $\alpha = \sqrt[4]{2}$. The extension $K : \mathbb{Q}$ is a Galois extension with $G = \text{Gal}(K : \mathbb{Q}) \cong D_4$, the 4-th dihedral group D_4 . This group is generated by automorphisms σ and τ :

$$\begin{aligned} \sigma(\alpha) &= i\alpha & \tau(\alpha) &= \alpha \\ \sigma(i) &= i & \tau(i) &= i. \end{aligned}$$

The field K has five subfields of degree 4:

$$\begin{aligned} K^{\sigma^2, \tau} &= \mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(\zeta_8), & K^{\sigma\tau} &= \mathbb{Q}((i+1)\alpha) = \mathbb{Q}(\zeta_8\alpha), & K^\tau &= \mathbb{Q}(\alpha), \\ K^{\sigma^3\tau} &= \mathbb{Q}((i-1)\alpha) = \mathbb{Q}(\zeta_8^{-1}\alpha) & \text{and} & & K^{\sigma^2\tau} &= \mathbb{Q}(i\alpha). \end{aligned}$$

The prime 2 totally ramifies in $K = \mathbb{Q}(\sqrt[4]{2}, i)$ since it ramifies in each of these subfields. Let \mathfrak{p} be the unique prime ideal of \mathcal{O}_K above 2. Both the numerator and the denominator of $\beta = \frac{\zeta_8+1}{\alpha}$ generate the ideal \mathfrak{p}^2 . A simple elementary calculation shows that $f(X) = X^8 - 4X^6 + 8X^4 - 4X^2 + 1$ is the minimal polynomial of β over \mathbb{Q} . From $f(1) = 2$ follows that $\mathfrak{p} = (\beta - 1)$. Completion at \mathfrak{p} yields the extension $\mathbb{Q}_2(\alpha, i) : \mathbb{Q}_2$ of local fields. Put $E = \mathbb{Q}_2(\alpha, i)$. The element $\beta - 1$ is a uniformizer of v_E . Since 2 totally ramifies, we have $\mathcal{O}_E = \mathbb{Z}_2[\beta - 1] = \mathbb{Z}_2[\beta]$. Hence for generators of the cyclic subgroups of G we have:

$$\begin{aligned} i(\sigma) &= v_E\left(\frac{-\zeta_8+1}{i\alpha} - \frac{\zeta_8+1}{\alpha}\right) = v_E\left(\frac{(1-i\zeta_8)(1-i)}{i\alpha}\right) = 2 + 4 - 2 = 4, \\ i(\sigma^2) &= v_E\left(\frac{\zeta_8+1}{-\alpha} - \frac{\zeta_8+1}{\alpha}\right) = v_E(-2\frac{\zeta_8+1}{\alpha}) = 8 + 2 - 2 = 8, \\ i(\tau) &= v_E\left(\frac{\zeta_8^{-1}+1}{\alpha} - \frac{\zeta_8+1}{\alpha}\right) = v_E(\zeta_8^{-1}\frac{1-i}{\alpha}) = 4 - 2 = 2, \\ i(\sigma^2\tau) &= v_E\left(\frac{\zeta_8^{-1}+1}{-\alpha} - \frac{\zeta_8+1}{\alpha}\right) = v_E(-\alpha(1 + \sqrt{2})) = 2, \end{aligned}$$

$$i(\sigma\tau) = v_E\left(\frac{-\zeta_8^{-1}+1}{i\alpha} - \frac{\zeta_8+1}{\alpha}\right) = v_E\left(\frac{1-i}{i\alpha}\right) = 4 - 2 = 2,$$

$$i(\sigma^3\tau) = v_E\left(\frac{-\zeta_8^{-1}+1}{\alpha} \frac{\zeta_8+1}{-\alpha} - \frac{\zeta_8+1}{\alpha}\right) = v_E(-(i+2)\alpha) = 2.$$

So $\#(V_x)$ jumps at 1, 3 and 7. The ramification groups with lower index at these values:

$$V_1 = G, \quad V_3 = \langle \sigma \rangle \quad \text{and} \quad V_7 = \langle \sigma^2 \rangle.$$

The functions φ and ψ :

$$\varphi(x) = \begin{cases} x & \text{if } x \leq 1, \\ \frac{1}{2}x + \frac{1}{2} & \text{if } 1 \leq x \leq 3, \\ \frac{1}{4}x + \frac{5}{4} & \text{if } 3 \leq x \leq 7, \\ \frac{1}{8}x + \frac{17}{8} & \text{if } x \geq 7. \end{cases} \quad \psi(x) = \begin{cases} x & \text{if } x \leq 1, \\ 2x - 1 & \text{if } 1 \leq x \leq 2, \\ 4x - 5 & \text{if } 2 \leq x \leq 3, \\ 8x - 17 & \text{if } x \geq 3. \end{cases}$$

The function ψ has breaks in 1, 2 and 3. The ramification groups with these values as upper index:

$$V^{(1)} = V_1 = G, \quad V^{(2)} = V_3 = \langle \sigma \rangle \quad \text{and} \quad V^{(3)} = V_7 = \langle \sigma^2 \rangle.$$

For any Galois extension of local fields the break points of φ are integers by construction. In the examples given above the break points of ψ are integers as well. Later we will see that this is the case for any abelian extension (Theorem 17.46, the Hasse-Arf Theorem). In the last example the Galois group is nonabelian, but nevertheless the break points of ψ are integral. In the next example the Galois group is the smallest nonabelian group S_3 and the function ψ has a nonintegral break point.

17.16 Example. Let $K = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$. Put $\alpha = \sqrt[3]{2}$. Many computations in this field have been done in Example 7.17. We use the same notations. The prime 3 totally ramifies in K . The prime ideal \mathfrak{p} of \mathcal{O}_K above 3 is a principal ideal: $\mathfrak{p} = (\delta)$, where $\delta = \frac{1+2\zeta_3}{\alpha+1}$. Completion at \mathfrak{p} yields the extension $\mathbb{Q}_3(\alpha, \zeta_3) : \mathbb{Q}_3$ of local fields. Put $E = \mathbb{Q}_3(\alpha, \zeta_3)$. The element δ is a uniformizer of v_E . We have $\mathcal{O}_E = \mathbb{Z}_3[\delta]$. For generators of cyclic subgroups of $G = \text{Gal}(E : \mathbb{Q}_3)$ we have:

$$i(\sigma) = v_E\left(\frac{1+2\zeta_3}{\zeta_3\alpha+1} - \frac{1+2\zeta_3}{\alpha+1}\right) = v_E\left(\frac{(1+2\zeta_3)\alpha(1-\zeta_3)}{(\zeta_3\alpha+1)(\alpha+1)}\right) = 3 + 3 - 2 - 2 = 2,$$

$$i(\tau) = v_E\left(\frac{1+2\zeta_3^2}{\alpha+1} - \frac{1+2\zeta_3}{\alpha+1}\right) = v_E\left(\frac{2\zeta_3(\zeta_3-1)}{\alpha+1}\right) = 3 - 2 = 1,$$

$$i(\sigma\tau) = v_E\left(\frac{1+2\zeta_3^2}{\zeta_3\alpha+1} - \frac{1+2\zeta_3}{\alpha+1}\right) = v_E\left(\frac{(1-\zeta_3)(\alpha-2\zeta_3)}{(\alpha+1)(\zeta_3\alpha+1)}\right) = 3 + 2 - 2 - 2 = 1,$$

$$i(\sigma^2\tau) = v_E\left(\frac{1+2\zeta_3^2}{\zeta_3^2\alpha+1} - \frac{1+2\zeta_3}{\alpha+1}\right) = v_E\left(\frac{(1-\zeta_3)(\alpha-2\zeta_3)}{(\alpha+1)(\zeta_3^2\alpha+1)}\right) = 3 + 2 - 2 - 2 = 1.$$

The last three outcomes just verify what we already know: in a quadratic extension the prime tamely ramifies. So $\#(V_x)$ jumps at 0 and 1. We have $V_0 = G$ and

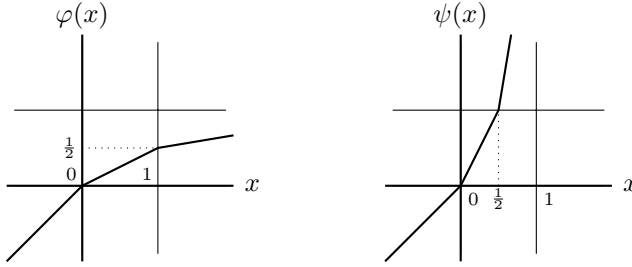


Figure 17.3: The graphs of the functions φ and ψ for the splitting of 3 in $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$

$V_1 = \langle \sigma \rangle$. The functions φ and ψ :

$$\varphi(x) = \begin{cases} x & \text{if } x \leq 0, \\ \frac{1}{2}x & \text{if } 0 < x < 1, \\ \frac{1}{6}x + \frac{1}{3} & \text{if } x \geq 1. \end{cases} \quad \psi(x) = \begin{cases} x & \text{if } x \leq 0, \\ 2x & \text{if } 0 < x < \frac{1}{2}, \\ 6x - 2 & \text{if } x \geq \frac{1}{2}. \end{cases}$$

See Figure 17.3. The function ψ breaks at 0 and $\frac{1}{2}$. The ramification groups with these values as upper index:

$$V^{(0)} = V_0 = G \quad \text{and} \quad V^{(\frac{1}{2})} = V_1 = \langle \sigma \rangle.$$

17.17 Example. Let p be an odd prime and $r \in \mathbb{N}^*$. In Example 7.64 the ramification groups of the prime p in $\mathbb{Q}(\zeta_{p^r})$ have been computed:

$$V_j = \text{Gal}(\mathbb{Q}(\zeta_{p^r}) : \mathbb{Q}(\zeta_{p^m})) \quad \text{if} \quad p^{m-1} \leq j \leq p^m - 1.$$

The jumps in the descending chain of ramification groups are at $p^m - 1$ for $m = 0, \dots, r - 1$. These groups coincide with the ramification groups of $\mathbb{Q}_p(\zeta_{p^r}) : \mathbb{Q}_p$. For $m \geq 1$ the slope of φ on $[p^{m-1} - 1, p^m - 1]$ is equal to

$$\frac{\#(V_{p^{m-1}})}{\#(V_0)} = \frac{p^{r-m}}{p^{r-1}(p-1)} = \frac{1}{p^{m-1}(p-1)}.$$

So

$$\varphi(p^m - 1) - \varphi(p^{m-1} - 1) = \frac{(p^m - 1) - (p^{m-1} - 1)}{p^{m-1}(p-1)} = 1.$$

This implies that the function ψ breaks at $0, \dots, r - 1$:

$$V^{(0)} = V_0 = G \quad \text{and} \quad V^{(i)} = V_{p^i - 1} = \text{Gal}(\mathbb{Q}(\zeta_{p^r}) : \mathbb{Q}(\zeta_{p^i})) \quad \text{for } i = 1, \dots, r.$$

17.2 The different

In this section the different of a field extension is introduced and for Galois extensions its relation to the ramification groups is studied. The following notations are used in this section:

R	a Dedekind domain,
K	the field of fractions of R ,
$L : K$	a finite separable field extension,
n	the degree of $L : K$,
S	the integral closure of R in L .

In this section both localization and completion occur. In case of localization at a single maximal ideal \mathfrak{p} the following notations are used:

$R_{\{\mathfrak{p}\}}$	the localization of R at the maximal ideal \mathfrak{p} ,
$K_{\mathfrak{p}}$	the completion of K with respect to the discrete valuation $v_{\mathfrak{p}}$,
$R_{\mathfrak{p}}$	the valuation ring of $K_{\mathfrak{p}}$

and in case of a number field K

$K_{\{\mathfrak{p}\}}$	the localization of \mathcal{O}_K at the maximal ideal \mathfrak{p} , so $K_{\{\mathfrak{p}\}} = (\mathcal{O}_K)_{\{\mathfrak{p}\}}$.
------------------------	--

All residue fields R/\mathfrak{p} , where $\mathfrak{p} \in \text{Max}(\mathcal{O}_R)$ are assumed to be finite. In section 1.5 we considered the nondegenerate symmetric bilinear map

$$L \times L \rightarrow K, \quad (\alpha, \beta) \mapsto \text{Tr}_K^L(\alpha\beta).$$

17.18 Definition. Let $\mathfrak{a} \in \mathbb{I}(L)$. Then

$$*\mathfrak{a} = \{ \beta \in L \mid \text{Tr}_K^L(\beta\mathfrak{a}) \subseteq R \}$$

is called the *dual* of \mathfrak{a} with respect to R .

17.19 Lemma. *The dual of a fractional ideal is a fractional ideal.*

PROOF. Let $\mathfrak{a} \in \mathbb{I}(L)$. Clearly, $*\mathfrak{a}$ is an S -submodule of L . So it suffices to show that there is an $\alpha \in L^*$ such that $\alpha \cdot *\mathfrak{a} \subseteq S$. Let $\alpha_1, \dots, \alpha_n \in S$ be a K -basis of L and $d = \text{disc}(\alpha_1, \dots, \alpha_n) = \det(\text{Tr}_K^L(\alpha_i\alpha_j))$. Let $\beta \in *\mathfrak{a}$, say $\beta = b_1\alpha_1 + \dots + b_n\alpha_n$ with $b_1, \dots, b_n \in K$. Take a nonzero $a \in \mathfrak{a} \cap R$. Let β_1, \dots, β_n be the dual basis of $\alpha_1, \dots, \alpha_n$. For $a\beta$ we have

$$a\beta = \text{Tr}_K^L(a\beta\alpha_1)\beta_1 + \dots + \text{Tr}_K^L(a\beta\alpha_n)\beta_n$$

and for $j = 1, \dots, n$

$$\mathrm{Tr}_K^L(a\beta\alpha_j) = \sum_{i=1}^n \mathrm{Tr}_K^L(ab_i\alpha_i\alpha_j).$$

In matrix notation:

$$(\mathrm{Tr}_K^L(\alpha_i\alpha_j)) \begin{pmatrix} ab_1 \\ \vdots \\ ab_n \end{pmatrix} = \begin{pmatrix} \mathrm{Tr}_K^L(a\beta\alpha_1) \\ \vdots \\ \mathrm{Tr}_K^L(a\beta\alpha_n) \end{pmatrix}.$$

Because $a\beta, \alpha_j \in S$, we have $\mathrm{Tr}_K^L(a\beta\alpha_j) \in R$ and so $dab_j \in R$ for $j = 1, \dots, n$. It follows that $da\beta \in S$. Hence $da \cdot {}^* \mathfrak{a} \subseteq S$. \square

17.20 Definition. The dual of S with respect to R is called the *complementary fractional ideal* of S over K . Note that the ring S is determined by R and L . This is reflected in the notation for the complementary fractional ideal:

$$\mathfrak{c}_R(L) = {}^* S.$$

Its inverse in the group $\mathbb{I}(L)$ is called the *different* of L over R . Notation:

$$\partial_R(L) = (\mathfrak{c}_R(L))^{-1}.$$

For a number field extension $L : K$ we define the *different* of L over K to be the different of L over \mathcal{O}_K :

$$\partial_K(L) = \partial_{\mathcal{O}_K}(L).$$

Note that, since $\mathfrak{c}_R(L)$ is a fractional ideal of S , we have $\mathrm{Tr}_K^L(\mathfrak{c}_R(L)) = \mathrm{Tr}_K^L(\mathfrak{c}_R(L)S) \subseteq R$.

17.21 Lemma. *The different of L over R is an ideal of S .*

PROOF. Clearly $S \subseteq \mathfrak{c}_R(L)$: for all $\alpha \in S$ we have $\alpha S \subseteq S$ and so $\mathrm{Tr}_K^L(\alpha S) \subseteq R$. Hence, $\partial_R(L) \subseteq S^{-1} = S$. \square

The different under localization:

17.22 Proposition. *Let P be a collection of maximal ideals of R and Q the collection of maximal ideals of S above P . Then*

$$\partial_{R_P}(L) = \partial_R(L)S_Q.$$

PROOF. We prove that $\mathfrak{c}_{R_P}(L) = \mathfrak{c}_R(L)S_Q$.

\supseteq : Let $\alpha \in \mathfrak{c}_R(L)$, $\mathfrak{p} \in P$ and $\beta \in S_Q$. Choose $t \in R$ such that $v_{\mathfrak{p}}(t) = 0$ and $t\beta \in S$. Then $t\mathrm{Tr}_K^L(\alpha\beta) = \mathrm{Tr}_K^L(\alpha t\beta) \subseteq R$ and $v_{\mathfrak{p}}(\mathrm{Tr}_K^L(\alpha\beta)) = v_{\mathfrak{p}}(\mathrm{Tr}(\alpha t\beta))$. Hence, $\mathrm{Tr}_K^L(\alpha S_Q) \subseteq R_{\{\mathfrak{p}\}}$. It follows that

$$\mathrm{Tr}_K^L(\alpha S_Q) \subseteq \bigcap_{\mathfrak{p} \in P} R_{\{\mathfrak{p}\}} = R_P$$

and so $\mathfrak{c}_R(L) \subseteq \mathfrak{c}_{R_P}(L)S_Q$ and for the fractional S_Q -ideal $\mathfrak{c}_R(L)S_Q$ we have $\mathfrak{c}_{R_P}(L) \subseteq \mathfrak{c}_R(L)S_Q$.

\subseteq : Let $\alpha \in \mathfrak{c}_{R_P}(L)$. By Proposition 6.25

$$\alpha \in \mathfrak{c}_R(L)S_Q \iff v_{\mathfrak{q}}(\alpha) \geq v_{\mathfrak{q}}(\mathfrak{c}_R(L)) \text{ for all } \mathfrak{q} \in Q.$$

Let $\mathfrak{q} \in Q$ and $\mathfrak{q} \cap K = \mathfrak{p}$. Choose $t \in R$ such that $v_{\mathfrak{p}}(t) = 0$ and $t\alpha \in S$. Then $\mathrm{Tr}_K^L(t\alpha S) \subseteq \mathrm{Tr}_K^L(S) \subseteq R$. So $t\alpha \in \mathfrak{c}_R(L)$ and, therefore, $v_{\mathfrak{q}}(t\alpha) \geq v_{\mathfrak{q}}(\mathfrak{c}_R(L))$. Because $t \notin \mathfrak{q}$, we have $v_{\mathfrak{q}}(\alpha) \geq v_{\mathfrak{q}}(\mathfrak{c}_R(L))$. \square

The different is an ideal of S . Its norm in K is the discriminant. More precisely:

17.23 Theorem. $\mathfrak{d}_R(L) = N_K^L(\partial_R(L))$.

PROOF. The Propositions 7.23 and 17.22 allow us to localize: let $\mathfrak{p} \in \mathrm{Max}(R)$ and $Q = \{\mathfrak{q} \in \mathrm{Max}(S) \mid v_{\mathfrak{q}}(\mathfrak{p}S) > 0\}$. Set $\mathfrak{p}' = \mathfrak{p}R_{\{\mathfrak{p}\}}$ and $\mathfrak{q}' = \mathfrak{q}S_Q$. Then

$$v_{\mathfrak{p}}(\mathfrak{d}_R(L)) = v_{\mathfrak{p}'}(\mathfrak{d}_{R_{\{\mathfrak{p}\}}}(L)) \quad \text{and} \quad v_{\mathfrak{q}}(\partial_R(L)) = v_{\mathfrak{q}'}(\partial_{R_{\{\mathfrak{p}\}}}(L)).$$

We may assume that R is a discrete valuation ring. Then S is a free R -module of rank n , say $S = R\alpha_1 + \cdots + R\alpha_n$. Thus $\mathfrak{d}_R(L) = \mathrm{disc}_K(\alpha_1, \dots, \alpha_n)R$. Let $(\beta_1, \dots, \beta_n)$ be the dual basis of the basis $(\alpha_1, \dots, \alpha_n)$. We have for $\gamma \in L$:

$$\begin{aligned} \gamma \in \mathfrak{c}_R(L) &\iff \mathrm{Tr}_R^S(\gamma S) \subseteq R \\ &\iff \mathrm{Tr}(\gamma\alpha_i) \in R \text{ for } i = 1, \dots, n \\ &\iff \gamma \in R\beta_1 + \cdots + R\beta_n. \end{aligned}$$

So $\mathfrak{c}_R(L) = R\beta_1 + \cdots + R\beta_n$. The R -module $\mathfrak{c}_R(L)$ is a fractional ideal of S . By Proposition 2.21 the ring S is a principal ideal domain, so there is a $\gamma \in L^*$ such that $\mathfrak{c}_R(L) = S\gamma$. We have

$$\begin{aligned} \mathrm{disc}_K(\beta_1, \dots, \beta_n)R &= \mathrm{disc}_K(\gamma\alpha_1, \dots, \gamma\alpha_n)R = N_K^L(\gamma)^2 \mathrm{disc}_K(\alpha_1, \dots, \alpha_n)R \\ &= N_K^L(\gamma)^2 \mathfrak{d}_R(L) = N_K^L(\mathfrak{c}_R(L))^2 \mathfrak{d}_R(L). \end{aligned}$$

The different $\partial_R(L)$ is the inverse of $\mathfrak{c}_R(L)$, so

$$\mathrm{disc}_R(\beta_1, \dots, \beta_n)N_K^L(\partial_R(L))^2 = \mathfrak{d}_R(L).$$

By Proposition 1.32 we have $\mathrm{disc}_K(\beta_1, \dots, \beta_n) = \mathrm{disc}_K(\alpha_1, \dots, \alpha_n)^{-1}$. Hence

$$N_K^L(\partial_R(L))^2 = \mathfrak{d}_R(L) \mathrm{disc}_K(\alpha_1, \dots, \alpha_n) = \mathfrak{d}_R(L)^2. \quad \square$$

So the prime ideals of S which divide the different $\partial_R(L)$ all lie above ramifying prime ideals of K . They are in fact all over K ramified prime ideals (Theorem 17.26).

The different under completion:

17.24 Proposition. *Let $\mathfrak{q} \in \text{Max}(S)$ and $\mathfrak{p} = \mathfrak{q} \cap K$. Then*

$$\partial_{R_{\mathfrak{p}}}(L_{\mathfrak{q}}) = \partial_R(L)S_{\mathfrak{q}}.$$

PROOF. We will prove that $\mathfrak{c}_{R_{\mathfrak{p}}}(L_{\mathfrak{q}}) = \mathfrak{c}_R(L)S_{\mathfrak{q}}$. By Proposition 17.22 we may assume that R is a discrete valuation ring.

\supseteq : Let $\alpha \in \mathfrak{c}_R(L)$, $\beta \in S_{\mathfrak{q}}$ and Q the set of prime ideals of S above \mathfrak{p} . Put $n_{\mathfrak{q}'} = \max(-v_{\mathfrak{q}'}(\alpha), 0)$ for all $\mathfrak{q}' \in Q$. Choose $\gamma \in S$ such that

$$\gamma \equiv \begin{cases} \beta \pmod{\hat{\mathfrak{q}}^{n_{\mathfrak{q}}}} \\ 0 \pmod{(\mathfrak{q}')^{n_{\mathfrak{q}'}}} \text{ for } \mathfrak{q}' \in Q \setminus \{\mathfrak{q}\}. \end{cases}$$

By Corollary 10.47

$$\text{Tr}_K^L(\alpha\gamma) = \text{Tr}_{\mathfrak{p}}^{\mathfrak{q}}(\alpha\gamma) + \sum_{\mathfrak{q}' \in Q \setminus \{\mathfrak{q}\}} \text{Tr}_{\mathfrak{p}}^{\mathfrak{q}'}(\alpha\gamma).$$

From $\gamma \in S$ and $\alpha \in \mathfrak{c}_R(L)$ follows that $\text{Tr}_K^L(\alpha\gamma) \in R \subseteq R_{\mathfrak{p}}$. For $\mathfrak{q}' \in Q \setminus \{\mathfrak{q}\}$ we have $v_{\mathfrak{q}'}(\alpha\gamma) = v_{\mathfrak{q}'}(\alpha) + v_{\mathfrak{q}'}(\gamma) \geq 0$. So $\gamma\alpha \in S_{\mathfrak{q}'}$ and therefore, $\text{Tr}_{\mathfrak{p}}^{\mathfrak{q}'}(\alpha\gamma) \in R_{\mathfrak{p}}$. By the above formula for the traces we have $\text{Tr}_{\mathfrak{p}}^{\mathfrak{q}}(\alpha\gamma) \in R_{\mathfrak{p}}$. From $v_{\mathfrak{q}}(\beta - \gamma) \geq n_{\mathfrak{q}}$ follows that $v_{\mathfrak{q}}(\alpha\beta - \alpha\gamma) \geq n_{\mathfrak{q}} + v_{\mathfrak{q}}(\alpha) \geq 0$. So

$$\text{Tr}_{\mathfrak{p}}^{\mathfrak{q}}(\alpha\beta) = \text{Tr}_{\mathfrak{p}}^{\mathfrak{q}}(\alpha\gamma) + \text{Tr}_{\mathfrak{p}}^{\mathfrak{q}}(\alpha\beta - \alpha\gamma) \in R_{\mathfrak{p}}.$$

It follows that $\text{Tr}_{\mathfrak{p}}^{\mathfrak{q}}(\alpha S_{\mathfrak{q}}) \subseteq R_{\mathfrak{p}}$, that is $\alpha \in \mathfrak{c}_{R_{\mathfrak{p}}}(L_{\mathfrak{q}})$.

\subseteq : Let $\alpha \in \mathfrak{c}_{R_{\mathfrak{p}}}(L_{\mathfrak{q}})$. Put $m = \max(0, v_{\mathfrak{q}}(\mathfrak{c}_R(L)))$. Choose $\beta \in L$ such that

$$v_{\mathfrak{q}}(\beta - \alpha) \geq m \quad \text{and} \quad v_{\mathfrak{q}'} \geq 0 \text{ for all } \mathfrak{q}' \in Q \setminus \{\mathfrak{q}\}.$$

Let $\gamma \in S$. Then $\text{Tr}_{\mathfrak{p}}^{\mathfrak{q}}(\beta\gamma) = \text{Tr}_{\mathfrak{p}}^{\mathfrak{q}}(\beta\gamma - \alpha\gamma) + \text{Tr}_{\mathfrak{p}}^{\mathfrak{q}}(\alpha\gamma) \in R_{\mathfrak{p}}$ and $\text{Tr}_{\mathfrak{p}}^{\mathfrak{q}'}(\beta\gamma) \in R_{\mathfrak{p}}$ for $\mathfrak{q}' \in Q \setminus \{\mathfrak{q}\}$. So again by the formula in Corollary 10.47: $\text{Tr}_K^L(\beta\gamma) \in R_{\mathfrak{p}} \cap K = R$. Hence $\beta \in \mathfrak{c}_R(L)$. Because $v_{\mathfrak{q}}(\beta - \alpha) \geq v_{\mathfrak{q}}(\mathfrak{c}_R(L))$, we have $\alpha \in \mathfrak{c}_R(L)S_{\mathfrak{q}}$. \square

So the different is the product of the local different, more precisely:

17.25 Corollary. $\partial_R(L) = \prod_{\mathfrak{q} \in \text{Max}(S)} \partial_{R_{\mathfrak{q} \cap K}}(L_{\mathfrak{q}}) \cap S.$

PROOF. For $\mathfrak{q} \in \text{Max}(S)$, put $v_{\mathfrak{q}}(\partial_R(L)) = k_{\mathfrak{q}}$ and $\mathfrak{p} = \mathfrak{q} \cap K$. Then by Proposition 17.24 $\partial_{R_{\mathfrak{p}}}(L_{\mathfrak{q}}) = \hat{\mathfrak{q}}^{k_{\mathfrak{q}}}$ and $\partial_{R_{\mathfrak{p}}}(L_{\mathfrak{q}}) \cap S = \mathfrak{q}^{k_{\mathfrak{q}}}$. \square

17.26 Theorem. For all $\mathfrak{q} \in \text{Max}(\mathcal{O}_L)$ we have

$$\mathfrak{q} \text{ is ramified over } K \iff \mathfrak{q} \mid \partial_R(L).$$

PROOF. Let $\mathfrak{q} \in \text{Max}(\mathcal{O}_L)$ and $\mathfrak{q} \cap K = \mathfrak{p}$. Then by Propositions 17.24 and Theorem 17.23:

$$\begin{aligned} v_{\mathfrak{p}}(\partial_{R_{\mathfrak{p}}}(L_{\mathfrak{q}})) &= v_{\mathfrak{p}}(N_{K_{\mathfrak{p}}}^{L_{\mathfrak{q}}}(\partial_{R_{\mathfrak{p}}}(L_{\mathfrak{q}}))) = f_{K_{\mathfrak{p}}}(\mathfrak{q}S_{\mathfrak{q}}) \cdot v_{\mathfrak{q}}(\partial_{R_{\mathfrak{p}}}(L_{\mathfrak{q}})) \\ &= f_{K_{\mathfrak{p}}}(\mathfrak{q}S_{\mathfrak{q}}) \cdot v_{\mathfrak{q}}(\partial_R(L)). \end{aligned} \quad \square$$

As far as the prime divisors of the different and of the discriminant are concerned, the discriminant contains less information than the different. The different tells us which prime ideals are ramified over the base field, whereas the discriminant only tells us over which prime ideals of the base field they lie.

For a tower of extensions:

17.27 Proposition. Let $M : L$ be a separable field extension and T the integral closure of R in M . Then

$$\partial_R(M) = \partial_S(M)\partial_R(L).$$

PROOF. We prove that $\mathfrak{c}_R(M) = \mathfrak{c}_S(M)\mathfrak{c}_R(L)$.

\supseteq :

$$\begin{aligned} \text{Tr}_K^M(\mathfrak{c}_S(M)\mathfrak{c}_R(L)) &= \text{Tr}_L^M \text{Tr}_K^L(\mathfrak{c}_S(M)\mathfrak{c}_R(L)) = \text{Tr}_K^L(\mathfrak{c}_R(L)\text{Tr}_L^M(\mathfrak{c}_S(M))) \\ &\subseteq \text{Tr}_K^L(\mathfrak{c}_R(L)S) \subseteq R. \end{aligned}$$

Hence, $\mathfrak{c}_S(M)\mathfrak{c}_R(L) \subseteq \mathfrak{c}_R(M)$.

\subseteq : From $\text{Tr}_K^L \text{Tr}_L^M(\mathfrak{c}_R(M)) = \text{Tr}_K^M(\mathfrak{c}_R(M)) \subseteq R$ follows that $\text{Tr}_L^M(\mathfrak{c}_R(M)) \subseteq \mathfrak{c}_R(L)$. So

$$\text{Tr}_L^M((\mathfrak{c}_R(L))^{-1}\mathfrak{c}_R(M)) = (\mathfrak{c}_R(L))^{-1}\text{Tr}_L^M(\mathfrak{c}_R(M)) \subseteq S.$$

Therefore, $(\mathfrak{c}_R(L))^{-1}\mathfrak{c}_R(M) \subseteq \mathfrak{c}_S(M)$, that is $\mathfrak{c}_R(M) \subseteq \mathfrak{c}_S(M)\mathfrak{c}_R(L)$. \square

For number field extensions this formula reads as

$$\partial_K(M) = \partial_L(M)\partial_K(L).$$

As a consequence we obtain a formula for the discriminant for a tower of extensions.

17.28 Theorem. *Let $M : L$ be a finite separable field extension and T the integral closure of R in M . Then*

$$\mathfrak{d}_R(M) = (\mathfrak{d}_R(L))^{[M:L]} \cdot \mathbb{N}_K^L(\mathfrak{d}_S(M)).$$

PROOF. By Proposition 17.25 $\partial_R(M) = \partial_S(M)\partial_R(L) = \partial_S(M) \cdot \partial_R(M)T$. Application of \mathbb{N}_K^M yields by Theorem 17.23:

$$\begin{aligned} \mathfrak{d}_R(M) &= \mathbb{N}_K^M(\partial_R(M)) = \mathbb{N}_K^L \mathbb{N}_L^M(\partial_S(M)) \cdot \mathbb{N}_K^L \mathbb{N}_L^M(\partial_R(L)T) \\ &= \mathbb{N}_K^L(\mathfrak{d}_S(M)) \cdot \mathbb{N}_K^L((\partial_R(L))^{[M:L]}) = \mathbb{N}_K^L(\mathfrak{d}_S(M)) \cdot (\mathfrak{d}_R(L))^{[M:L]}. \quad \square \end{aligned}$$

For number field extensions:

$$\mathfrak{d}_K(M) = (\mathfrak{d}_K(L))^{[M:L]} \cdot \mathbb{N}_K^L(\mathfrak{d}_L(M)).$$

For discriminants of extensions $L : K$ the discriminants of K -bases of L are of importance. Likewise, for differentials we have differentials of elements.

17.29 Definition. Let $\alpha \in L$ and let f be the characteristic polynomial of α over K . The *different* $\partial_K^L(\alpha)$ of α over K is defined by

$$\partial_K^L(\alpha) = f'(\alpha).$$

If α is not a primitive element of the extension, say $[L : K(\alpha)] = m > 1$, then the roots of f have multiplicity m and, therefore, $f'(\alpha) = 0$. Furthermore, if $\alpha \in S$, then $f \in R[X]$ and $f'(\alpha) \in S$.

A special case, particularly interesting in case of extensions of local fields:

17.30 Proposition. *If there is an $\alpha \in L$ such that $S = R[\alpha]$, then $\partial_K(S) = (\partial_K^L(\alpha))$.*

PROOF. Let $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ be the characteristic polynomial of α over K . Put

$$\frac{f(X)}{X - \alpha} = \beta_{n-1}X^{n-1} + \beta_{n-2}X^{n-2} + \cdots + \beta_0 = g(X) \in S[X].$$

Let $\alpha_1, \dots, \alpha_n$ be the roots of f in a splitting field of f over L . Let's assume $\alpha = \alpha_1$. For each $0 \leq i \leq n-1$ there is a unique polynomial h (over the splitting field of f over L) of degree $\leq n-1$ such that $h(\alpha_j) = \alpha_j^i$ for $j = 0, \dots, n-1$. It obviously is the polynomial X^i and Lagrange's interpolation formula yields

$$\sum_{j=1}^n \frac{\alpha_j^i f(X)}{f'(\alpha_j)(X - \alpha_j)} = X^i.$$

Since $\beta_0, \dots, \beta_{n-1} \in L$, we can rewrite this as

$$\sum_{j=1}^{n-1} \operatorname{Tr}_K^L \left(\alpha^i \frac{\beta_j}{f'(\alpha)} \right) X^j = X^i.$$

Hence

$$\operatorname{Tr}_K^L \left(\alpha^i \frac{\beta_j}{f'(\alpha)} \right) = \delta_{ij}$$

and this means that

$$\frac{\beta_0}{f'(\alpha)}, \dots, \frac{\beta_{n-1}}{f'(\alpha)}$$

is the dual basis of $1, \alpha, \dots, \alpha^{n-1}$. Let $\gamma \in L$. Then

$$\gamma = \operatorname{Tr}_K^L(\gamma) \frac{\beta_0}{f'(\alpha)} + \dots + \operatorname{Tr}_K^L(\gamma \alpha^{n-1}) \frac{\beta_{n-1}}{f'(\alpha)},$$

Because $S = R[\alpha]$, we have $\gamma \in \mathfrak{c}_R(L)$ if and only if $\operatorname{Tr}_K^L(\gamma \alpha^i) \in R$ for $i = 0, \dots, n-1$. This means that

$$\mathfrak{c}_R(L) = R \frac{\beta_0}{f'(\alpha)} + \dots + R \frac{\beta_{n-1}}{f'(\alpha)}.$$

From $f(X) = (X - \alpha)g(X)$ follows

$$\begin{aligned} \beta_{n-1} &= 1 \\ \beta_{n-2} - \alpha \beta_{n-1} &= a_{n-1} \\ &\vdots \\ \beta_0 - \alpha \beta_1 &= a_1 \end{aligned}$$

and this leads to

$$\begin{aligned} \beta_{n-1} &= 1 \\ \beta_{n-2} &= \alpha + a_{n-1} \\ \beta_{n-3} &= \alpha^2 + a_{n-1}\alpha \\ &\vdots \\ \beta_0 &= \alpha^{n-1} + a_{n-1}\alpha^{n-2} + \dots + a_1. \end{aligned}$$

It follows that $R[\alpha] = R\beta_0 + \dots + R\beta_{n-1}$. Hence $\mathfrak{c}_R(L) = \frac{1}{f'(\alpha)}S$, and thus $\partial_R(L) = f'(\alpha)S$. \square

Since the different is the product of the local differentials and our main interest is the case of a number field extension, we will now consider local field extensions. It turns out that the different is completely determined by the ramification groups of the extension (Theorem 17.34).

17.31 Definition and notation. Let $E : F$ be an extension of local fields. The *different* $\partial_F(E)$ of E over F is defined to be the different of \mathcal{O}_E over F :

$$\partial_F(E) = \partial_{\mathcal{O}_F}(E).$$

It is, as an ideal of \mathcal{O}_E , a power of the maximal ideal \mathfrak{p}_E .

17.32 Proposition. Let $E : F$ be an extension of local fields. There exists a $\gamma \in \mathcal{O}_E$ such that $\mathcal{O}_E = \mathcal{O}_F[\gamma]$. Let f be the minimal polynomial of γ over F . Then $\partial_F(E) = (f'(\gamma))$.

PROOF. The existence of γ is Proposition 11.15 and the formula $\partial_F(E) = (f'(\gamma))$ follows from Proposition 17.30. \square

17.33 Definition and notation. Let $E : F$ be a Galois extension of local fields. The i -th *ramification group* of $E : F$ is the i -th ramification group of \mathfrak{p}_F in E and is denoted by $V_{F,i}(E)$, that is

$$V_{F,i}(E) = V_{F,i}(\mathfrak{p}_E).$$

17.34 Theorem. Let $E : F$ be a Galois extension of local fields and V_i the i -th ramification group of E over F : $V_i = V_{F,i}(E)$. Then

$$v_E(\partial_F(E)) = \sum_{i=0}^{\infty} (\#(V_i) - 1).$$

PROOF. Let γ and f be as in Proposition 17.32 and put $G = \text{Gal}(E : F)$. Then by Proposition 17.32 we have $\partial_F(E) = (f'(\gamma))$. Choose $t \in \mathbb{N}$ such that $V_t = \{1\}$. From

$$f'(\gamma) = \prod_{\substack{\sigma \in G \\ \sigma \neq 1}} (\sigma(\gamma) - \gamma)$$

and

$$\sigma \in V_i \setminus V_{i+1} \iff v_E(\sigma(\gamma) - \gamma) = i + 1$$

then follows

$$\begin{aligned} v_E(\partial_F(E)) &= v_E(f'(\gamma)) = \sum_{\sigma \neq 1} v_E(\sigma(\gamma) - \gamma) = \sum_{i=0}^{\infty} \sum_{\sigma \in V_i \setminus V_{i+1}} v_E(\sigma(\gamma) - \gamma) \\ &= \sum_{i=0}^{\infty} \sum_{\sigma \in V_i \setminus V_{i+1}} (i + 1) = \sum_{i=0}^{\infty} (i + 1)(\#(V_i) - \#(V_{i+1})) \\ &= \sum_{i=0}^t (i + 1)\#(V_i) - \sum_{i=0}^t (i + 1)\#(V_{i+1}) = \sum_{i=0}^t (i + 1)\#(V_i) - \sum_{i=1}^{t+1} i\#(V_i) \end{aligned}$$

$$\begin{aligned}
 &= \#(V_0) - (t+1)\#(V_{t+1}) + \sum_{i=1}^t \#(V_i) = \#(V_0) - 1 - t + \sum_{i=1}^t \#(V_i) \\
 &= \sum_{i=0}^t (\#(V_i) - 1). \quad \square
 \end{aligned}$$

For a number field extension we obtain:

17.35 Corollary. *Let $L : K$ be a Galois extension of number fields and $\mathfrak{q} \in \text{Max}(\mathcal{O}_L)$. Then*

$$v_{\mathfrak{q}}(\partial_K(L)) = \sum_{i=0}^{\infty} (\#(V_{K,i}(\mathfrak{q})) - 1).$$

PROOF. Let $\mathfrak{p} = \mathfrak{q} \cap K$ and choose $K_{\mathfrak{p}}$ to be a subfield of $L_{\mathfrak{q}}$. Then restriction of automorphisms yields an isomorphism

$$\text{Gal}(L_{\mathfrak{q}} : K_{\mathfrak{p}}) \xrightarrow{\sim} Z_K(\mathfrak{q})$$

and for each $i \in \mathbb{N}$ an isomorphism

$$V_{K_{\mathfrak{p}},i}(\hat{\mathfrak{q}}) \xrightarrow{\sim} V_{K,i}(\mathfrak{q}).$$

So

$$v_{\mathfrak{q}}(\partial_K(L)) = v_{\mathfrak{q}}(\partial_{K_{\mathfrak{p}},i}(L_{\mathfrak{q}})) = \sum_{i=0}^{\infty} (\#(V_{K_{\mathfrak{p}},i}(\hat{\mathfrak{q}})) - 1) = \sum_{i=0}^{\infty} (\#(V_{K,i}(\mathfrak{q})) - 1). \quad \square$$

17.36 Example. Let's verify the formula of the last theorem for (the completion of) the extension $\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}$ considered in Example 17.15. We will use the same notations. The minimal polynomial of $\beta \in \mathcal{O}_L$ over \mathbb{Q} is $f(X) = X^8 - 4X^6 + 8X^4 - 4X^2 + 1$ and $\beta - 1$ generates the prime ideal \mathfrak{p} above 2. Since only 2 ramifies in K , the discriminant of $K : \mathbb{Q}$ is a power of 2. Moreover, since 2 totally ramifies, one has $\mathcal{O}_K = \mathbb{Z}[\beta - 1] = \mathbb{Z}[\beta]$. So

$$\begin{aligned}
 \text{disc}(K) &= N_{\mathbb{Q}}^K(f'(\beta)) = N_{\mathbb{Q}}^K(8\beta^7 - 24\beta^5 + 32\beta^3 - 8\beta) \\
 &= 2^{24} N_{\mathbb{Q}}^K(\beta^6 - 3\beta^4 + 4\beta^2 - 1) = 2^{24}u,
 \end{aligned}$$

where u is odd, since $\beta^6 - 3\beta^4 + 4\beta^2 - 1 \notin \mathfrak{p} = (\beta - 1)$. In fact, $u = 1$ as remarked before. From Theorem 17.34 it follows that the \mathfrak{p} -valuation of $\partial_{\mathbb{Z}}(K)$ is equal to $2(8 - 1) + 2(4 - 1) + 4(2 - 1) = 24$ and this is the 2-valuation of $\text{disc}(K)$ as well.

Theorem 17.34 relates the different to the orders of the ramification groups given by lower indices. In case the function ψ has only breaks at integral arguments we obtain by grouping lower indices a formula in terms of orders of ramification groups given by upper indices.

17.37 Theorem. *Let $E : F$ be a Galois extension of local fields with Galois group G . Suppose that the function ψ_G has only breaks at integral arguments. Then*

$$v_E(\partial_F(E)) = e_F^{(E)} \sum_{i=0}^{\infty} \left(1 - \frac{1}{\#(V_F^{(i)}(E))} \right).$$

PROOF. Put $V_i = V_{F,i}(E)$ and $V^{(i)} = V_F^{(i)}(E)$. By assumption the function $\psi = \psi_G$ has no breaks between integers $i - 1$ and i . This means the function $\varphi = \varphi_G$ has no breaks between $\psi(i - 1)$ and $\psi(i)$. Start with the formula of Theorem 17.34:

$$\begin{aligned} v_E(\partial_F(E)) &= \sum_{i=0}^{\infty} (\#(V_i) - 1) = \sum_{i=0}^{\infty} \sum_{j=\psi(i-1)+1}^{\psi(i)} (\#(V_j) - 1) \\ &= \sum_{i=0}^{\infty} \sum_{j=\psi(i-1)+1}^{\psi(i)} (\#(V_{\psi(i)}) - 1) \\ &= \sum_{i=0}^{\infty} (\psi(i) - \psi(i-1)) (\#(V_{\psi(i)}) - 1) \\ &= \sum_{i=0}^{\infty} \psi'_i(i) (\#(V_{\psi(i)}) - 1) = \sum_{i=0}^{\infty} \frac{1}{\varphi'_i(\psi(i))} (\#(V_{\psi(i)}) - 1) \\ &= \sum_{i=0}^{\infty} \frac{\#(V_0)}{\#(V_{\psi(i)})} (\#(V_{\psi(i)}) - 1) = e_F^{(E)} \sum_{i=0}^{\infty} \left(1 - \frac{1}{\#(V^{(i)})} \right). \quad \square \end{aligned}$$

17.3 Local Artin maps and ramification groups

Let $E : F$ be an abelian extension of local fields of characteristic 0, $G = \text{Gal}(E : F)$ and $n = [E : F]$. By local Artin reciprocity the local Artin map $\vartheta_F^{(E)} : F^* \rightarrow G$ induces an isomorphism

$$\vartheta_F^{(E)} : F^* / N_F^E(E^*) \xrightarrow{\sim} G.$$

17.38 Notation. In 16.16 the notation $U_F^{(i)}$ was introduced for F a local field and $i \in \mathbb{N}$. Now we also allow $i = -1$ in this notation by putting

$$U_F^{(-1)} = F^*.$$

The groups $U_F^{(i)}$ form a descending chain of subgroups of F^* :

$$\begin{array}{ccccccc} U_F^{(-1)} & \supseteq & U_F^{(0)} & \supseteq & \cdots & \supseteq & U_F^{(i)} & \supseteq & \cdots \\ & & \parallel & & & & & & \\ & & F^* & & & & & & \end{array}$$

Taking products with the subgroup $N_F^E(E^*)$ yields the descending chain

$$\begin{array}{ccccccc} N_F^E(E^*)U_F^{(-1)} & \supseteq & N_F^E(E^*)U_F^{(0)} & \supseteq & \cdots & \supseteq & N_F^E(E^*)U_F^{(i)} & \supseteq & \cdots \\ & & \parallel & & & & & & \\ & & F^* & & & & & & \end{array}$$

Let j be the least integer such that $U_F^{(j)} \subseteq N_F^E(E^*)$. Then the conductor $\mathfrak{f}_F(E)$ of $E : F$ equals \mathfrak{p}_F^j . So $N_F^E(E^*)U_F^{(i)} = N_F^E(E^*)$ if and only if $i \geq j$. By setting $W_F^{(i)}(E) = \vartheta_F^{(E)}(N_F^E(E^*)U_F^{(i)}) = \vartheta_F^{(E)}(U_F^{(i)})$, we obtain a corresponding descending chain of subgroups of the Galois group:

$$\begin{array}{ccccccc} W_F^{(-1)}(E) & \supseteq & W_F^{(0)}(E) & \supseteq & \cdots & \supseteq & W_F^{(i)}(E) & \supseteq & \cdots \\ & & \parallel & & & & & & \\ & & G & & & & & & \end{array}$$

and we have $W_F^{(i)}(E) = \{1\}$ if and only if $i \geq j$.

17.39 Example. Let p be an odd prime and $r \in \mathbb{N}^*$. The cyclotomic field $\mathbb{Q}(\zeta_{p^r})$ is as an abelian field the class field of \mathcal{D}_{p^r} and in the general class field theory it is the class field of $\mathcal{H}_{(p)^r\infty}(\mathbb{Q})$. In the first sense its conductor is p^r and in the second it is $(p)^r\infty$. Its local conductor at the prime p is the ideal $(p)^r$ of \mathbb{Z} . This implies that the conductor of $\mathbb{Q}_p(\zeta_{p^r}) : \mathbb{Q}_p$ is the ideal $(p)^r$ of \mathbb{Z}_p . Put $E = \mathbb{Q}_p(\zeta_{p^r})$. Since p is the norm of $1 - \zeta_{p^r}$ we have

$$N_{\mathbb{Q}_p}^E(E^*) = U_{\mathbb{Q}_p}^{(p^r)} \cdot \langle p \rangle = (1 + (p)^r) \cdot \langle p \rangle.$$

It follows with Example 17.17 that $W_{\mathbb{Q}_p}^{(i)}(E) = V_{\mathbb{Q}_p}^{(i)}(E)$ for $i = 0, \dots, r$.

The main result in this section is that in general $W_F^{(i)}(E) = V_F^{(i)}(E)$ for all $i \geq -1$. This is Theorem 17.48. For its proof a detailed study of the function ψ is needed, to start with cyclic extensions of prime degree. This is done in a series of lemmas.

17.40 Lemma. *Let $E : F$ be cyclic of prime degree l , $s \in \mathbb{N}^*$ and $\gamma \in E$ such that $v_E(\gamma) \geq s$. Then*

$$N_F^E(1 + \gamma) \equiv 1 + \text{Tr}_F^E(\gamma) + N_F^E(\gamma) \pmod{\text{Tr}_F^E(\mathfrak{p}_E^{2s})}.$$

PROOF. The norm of $1 + \gamma$ is the product over its conjugates and we expand this product:

$$N_F^E(1 + \gamma) = \prod_{\tau \in G} (1 + \tau(\gamma)) = \sum_I \prod_{\tau \in I} \tau(\gamma) = \sum_I \left(\sum_{\tau \in I} \tau \right) \cdot \gamma = \sum_I \beta_I,$$

where the sum is taken over all subsets I of G and $\beta_I = \left(\sum_{\tau \in I} \tau \right) \cdot \gamma$. The group G operates on the set of subsets of G by $\sigma I = \{ \sigma \tau \mid \tau \in I \}$. Only \emptyset and G are fixed under this operation: $\beta_\emptyset = \gamma$ and $\beta_G = N_G \cdot \gamma = N_F^E(\gamma)$. The other subsets are in orbits of length l . For a proper nonempty subset I we have

$$\begin{aligned} \sum_{\sigma \in G} \beta_{\sigma I} &= \sum_{\sigma \in G} \beta_{\sigma I} = \sum_{\sigma \in G} \left(\sum_{\tau \in I} \sigma \tau \right) \cdot \gamma = \sum_{\sigma \in G} \prod_{\tau \in I} \sigma \tau(\gamma) \\ &= \sum_{\sigma \in G} \sigma \left(\prod_{\tau \in I} \tau(\gamma) \right) = \text{Tr}_F^E \left(\prod_{\tau \in I} \tau(\gamma) \right). \end{aligned}$$

In particular for the orbit of one element sets we have

$$\sum_{\sigma \in G} \beta_\sigma = \text{Tr}_F^E(\gamma).$$

For $1 < \#(I) < l$:

$$v_E \left(\text{Tr}_F^E \left(\prod_{\tau \in I} \tau(\gamma) \right) \right) \geq v_E \left(\text{Tr}_F^E(\mathfrak{p}_E^{2s}) \right).$$

Hence

$$N_F^E(1 + \gamma) \equiv 1 + \text{Tr}_F^E(\gamma) + N_F^E(\gamma) \pmod{\text{Tr}_F^E(\mathfrak{p}_E^{2s})}. \quad \square$$

17.41 Lemma. *Let $E : F$ be ramified and cyclic of prime degree l , $s \in \mathbb{N}^*$ and $m = v_E(\partial_F(E))$. Then*

$$v_F(\text{Tr}_F^E(\mathfrak{p}_E^s)) = \left\lfloor \frac{m+s}{l} \right\rfloor.$$

PROOF. For $t \in \mathbb{N}$ we have

$$\begin{aligned} \text{Tr}_F^E(\mathfrak{p}_E^s) \subseteq \mathfrak{p}_F^t &\iff \mathfrak{p}_F^{-t} \text{Tr}_F^E(\mathfrak{p}_E^s) \subseteq \mathcal{O}_F \iff \text{Tr}(\mathfrak{p}_F^{-t} \mathfrak{p}_E^s) \subseteq \mathcal{O}_F \\ &\iff \mathfrak{p}_E^{-lt+s} \subseteq \mathfrak{c}_F(E) \iff \partial_F(E) \subseteq \mathfrak{p}_E^{lt-s} \iff m \geq lt - s \\ &\iff t \leq \frac{m+s}{l}. \end{aligned}$$

This proves the lemma. \square

For $E : F$ a cyclic extension of prime degree l and Galois group G , let t be the unique jump in the chain of ramification groups:

$$G = V_{F,-1}(E) = V_{F,0}(E) = \cdots = V_{F,t}(E)$$

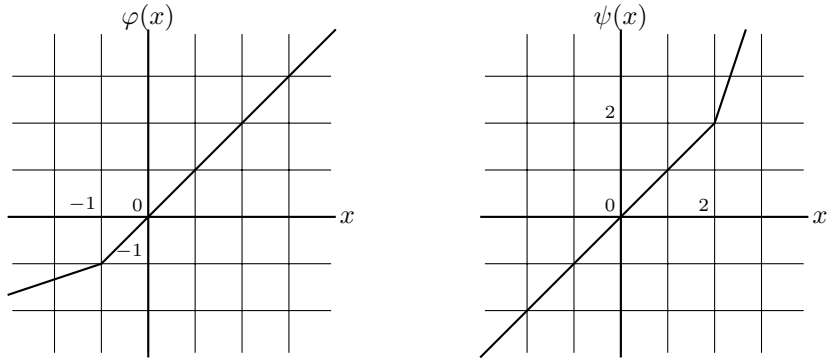


Figure 17.4: The functions φ and ψ for a cyclic extension of degree 3 with breaks respectively -1 and 2

$$\{1\} = V_{F,t+1}(E) = V_{F,t+2}(E) = \dots$$

Then by Theorem 17.34 $v_E(\partial_F(E)) = \sum_{i=0}^t (l-1) = (t+1)(l-1)$.

17.42 Lemma. *Let $E : F$ be cyclic of prime degree l with Galois group G . If $t = -1$, that is $E : F$ is unramified, then*

$$\psi(x) = \begin{cases} \frac{1}{l}(x+1) - 1 & \text{if } x \leq -1, \\ x & \text{if } x \geq -1. \end{cases}$$

If $t \geq 0$, then

$$\psi(x) = \begin{cases} x & \text{if } x \leq t, \\ l(x-t) + t & \text{if } x \geq t. \end{cases}$$

PROOF. Put $V_i = V_{F,i}(E)$. By Definition 17.5 we have for $t = -1$

$$\varphi(x) = \begin{cases} l(x+1) - 1 & \text{if } x \leq -1, \\ x & \text{if } x \geq -1. \end{cases}$$

and for $t \geq 0$

$$\varphi(x) = \begin{cases} x & \text{if } x \leq t, \\ \frac{1}{l}(x-t) + t & \text{if } x \geq t. \end{cases}$$

See Figure 17.4. The function ψ is the inverse function of φ . □

The function ψ has one break, namely for $x = t$:

$$\psi_{r/l}(t) = \frac{\#(V_t)}{\#(V_{t+1})} = l.$$

17.43 Lemma. *Let $E : F$ be cyclic of prime degree l . Then for each integer $i \geq -1$:*

$$\mathbf{N}_F^E(U_E^{(\psi(i))}) \subseteq U_F^{(i)} \quad \text{and} \quad \mathbf{N}_F^E(U_E^{(\psi(i)+1)}) \subseteq U_F^{(i+1)},$$

and

$$(U_F^{(i)} : U_F^{(i+1)} \mathbf{N}_F^E(U_E^{(\psi(i))})) \leq \psi'_{r/l}(i) = \begin{cases} 1 & \text{if } i \neq t, \\ l & \text{if } i = t. \end{cases}$$

PROOF. The proof is by distinction of cases.

$i = -1$: We have $\psi(-1) = -1$, $U_F^{(-1)} = F^*$, $U_F^{(0)} = \mathcal{O}_F^*$. Obviously, $\mathbf{N}_F^E(E^*) \subseteq F^*$ and $\mathbf{N}_F^E(\mathcal{O}_E^*) \subseteq \mathcal{O}_F^*$. Furthermore, by Theorem 12.22

$$(\mathcal{O}_F^* : \mathbf{N}_F^E(E^*)) = e_F^{(E)} = \begin{cases} 1 & \text{if } t = -1, \\ l & \text{if } t \neq -1. \end{cases}$$

By Lemma 15.50

$$\mathcal{O}_F^* \subseteq \mathbf{N}_F^E(E^*) \iff t = -1$$

and, therefore,

$$(U_F^{(-1)} : U_F^{(0)} \mathbf{N}_F^E(U_E^{(0)})) = (F^* : \mathcal{O}_F^* \mathbf{N}_F^E(E^*)) = \begin{cases} 1 & \text{if } t \neq -1, \\ l & \text{if } t = -1. \end{cases}$$

$i = 0$: We have $\psi(0) = 0$, $U_F^{(0)} = \mathcal{O}_F^*$ and $U_F^{(1)} = 1 + \mathfrak{p}_F$. From $\mathfrak{p}_E \cap F = \mathfrak{p}_F$ follows that for $\alpha \in \mathfrak{p}_E$ we have $\mathbf{N}_F^E(1 + \alpha) = \prod_{\sigma \in G} \sigma(1 + \alpha) = \prod_{\sigma \in G} (1 + \sigma(\alpha)) \in (1 + \mathfrak{p}_E) \cap F = 1 + \mathfrak{p}_F$ and so $\mathbf{N}_F^E(1 + \mathfrak{p}_E) \subseteq 1 + \mathfrak{p}_F$.

For the computation of the index $(\mathcal{O}_F^* : (1 + \mathfrak{p}_F) \mathbf{N}_F^E(\mathcal{O}_E^*))$ use:

$$(\mathcal{O}_F^* : (1 + \mathfrak{p}_F) \mathbf{N}_F^E(\mathcal{O}_E^*)) \mid (\mathcal{O}_F^* : (1 + \mathfrak{p}_F)) = \#(k_F^*)$$

$$(\mathcal{O}_F^* : (1 + \mathfrak{p}_F) \mathbf{N}_F^E(\mathcal{O}_E^*)) \mid (\mathcal{O}_F^* : \mathbf{N}_F^E(\mathcal{O}_E^*)) = e_F^{(E)}$$

$$\text{If } t = -1, \text{ then } e_F^{(E)} = 1.$$

$$\text{If } t \geq 0, \text{ then } e_F^{(E)} = l.$$

$$\text{If } t > 0, \text{ then } \text{char}(k_F) = l \text{ and so } l \nmid \#(k_F^*).$$

$i > 0$:

$t = -1$: Then $\psi(i) = i$ and $\partial_F(E) = \mathcal{O}_E$. For all $j \in \mathbb{N}$

$$\text{Tr}_F^E(\mathfrak{p}_E^i) \subseteq \mathfrak{p}_F^j \iff \text{Tr}_F^E(\mathfrak{p}_E^{i-j}) \subseteq \mathfrak{c}_F(E) \iff \mathcal{O}_E \subseteq \mathfrak{p}_E^{j-i} \iff j \leq i$$

and so $\text{Tr}_F^E(\mathfrak{p}_E^i) = \mathfrak{p}_F^i$. Replacing i by $i + 1$ and $2i$ respectively yields $\text{Tr}_F^E(\mathfrak{p}_E^{i+1}) = \mathfrak{p}_F^{i+1}$ and $\text{Tr}_F^E(\mathfrak{p}_E^{2i}) = \mathfrak{p}_F^{2i} \subseteq \mathfrak{p}_F^{i+1}$. Moreover, $N_F^E(\mathfrak{p}_E^i) = \mathfrak{p}_F^{li} \subseteq \mathfrak{p}_F^{i+1}$. By Lemma 17.40 we have for all $\gamma \in \mathfrak{p}_E^i$:

$$N_F^E(1 + \gamma) \equiv 1 + \text{Tr}_F^E(\gamma) \pmod{\mathfrak{p}_F^{i+1}}.$$

So $U_F^{(i)} N_F^E(U_E^{(i)}) \subseteq U_F^{(i+1)}$. On the other hand let $\beta \in \mathfrak{p}_F^{(i+1)}$ and choose a $\gamma \in \mathfrak{p}_E^{(i+1)}$ such that $\text{Tr}_F^E(\gamma) = \beta$. Then

$$N_F^E(1 + \gamma) \equiv 1 + \beta \pmod{\mathfrak{p}_F^{i+1}},$$

that is

$$\frac{1 + \beta}{N_F^E(1 + \gamma)} \in U_F^{(i+1)}.$$

It follows that $1 + \beta \in U_F^{(i+1)} N_F^E(U_E^{(i)})$.

$t > i$: By Lemma 17.42 $\psi(i) = i$. For $\gamma \in \mathfrak{p}_E^i$ we have by Lemma 17.40

$$N_F^E(1 + \gamma) \equiv 1 + \text{Tr}_F^E(\gamma) + N_F^E(\gamma) \pmod{\text{Tr}_F^E(\mathfrak{p}_E^{2i})}.$$

By Lemma 17.41 $v_F(\text{Tr}_F^E(\mathfrak{p}_E^t)) = t$ and we have $(t + 1)(l - 1) + i > (i + 1)(l - 1) + i = il + l - 1$, that is $(t + 1)(l - 1) + i \geq il + l$. Therefore, also by Lemma 17.41, $v_F(\text{Tr}_F^E(\mathfrak{p}_E^i)) \geq i + 1$ and, moreover, $v_F(\text{Tr}_F^E(\mathfrak{p}_E^{2i})) \geq v_F(\text{Tr}_F^E(\mathfrak{p}_E^i)) \geq i + 1$. Hence for $\gamma \in \mathfrak{p}_E^i$

$$N_F^E(1 + \gamma) \equiv 1 + N_F^E(\gamma) \pmod{\mathfrak{p}_F^{i+1}}$$

and, in particular for $\gamma \in \mathfrak{p}_E^i$, respectively $\gamma \in \mathfrak{p}_E^{i+1}$:

$$N_F^E(1 + \gamma) \equiv 1 \pmod{\mathfrak{p}_F^i}, \quad \text{respectively } N_F^E(1 + \gamma) \equiv 1 \pmod{\mathfrak{p}_F^{i+1}}.$$

So $N_F^E(U_E^{(i)}) \subseteq U_F^{(i)}$, $N_F^E(U_E^{(i+1)}) \subseteq U_F^{(i+1)}$ and $U_F^{(i+1)} N_F^E(U_E^{(i)}) \subseteq U_F^{(i)}$. Now let $\beta \in \mathfrak{p}_F^i$ and choose a $\gamma \in \mathfrak{p}_E^i$ such that $N_F^E(\gamma) = \beta$. Then as in the previous case it follows that $1 + \beta \in U_F^{(i+1)} N_F^E(U_E^{(i)})$.

$t = i$: By Lemma 17.42 we have $\psi(t) = t$. Since $(t + 1)(l - 1) + t = lt + l - 1$ and $\lfloor \frac{lt+l-1}{l} \rfloor = t$, we have by Lemma 17.41

$$\text{Tr}_F^E(\mathfrak{p}_E^t) = \mathfrak{p}_F^t.$$

Similarly $\text{Tr}_F^E(\mathfrak{p}_E^{t+1}) = \mathfrak{p}_F^{t+1}$ and $\text{Tr}_F^E(\mathfrak{p}_E^{2t}) = \mathfrak{p}_F^{2t} \subseteq \mathfrak{p}_F^{t+1}$. By Lemma 17.40 for all $\gamma \in \mathfrak{p}_E^t$:

$$N_F^E(1 + \gamma) \equiv 1 + \text{Tr}_F^E(\gamma) + N_F^E(\gamma) \pmod{\mathfrak{p}_F^{t+1}}$$

and

$$N_F^E(1 + \gamma) \equiv 1 \pmod{\mathfrak{p}_F^t}.$$

Moreover, if $\gamma \in \mathfrak{p}_E^{(t+1)}$, then $N_F^E(1 + \gamma) \equiv 1 \pmod{\mathfrak{p}_F^{t+1}}$. So N_F^E induces a group homomorphism

$$\bar{N}: U_E^{(t)}/U_E^{(t+1)} \rightarrow U_F^{(t)}/U_F^{(t+1)}.$$

The cokernel of \bar{N} is $U_F^{(t)}/U_F^{(t+1)}N_F^E(U_E^{(t)})$. Choose uniformizers π_E and π_F of E and F respectively. Then $\text{Tr}_F^E(\pi_E^t) = a\pi_F^t$ and $N_F^E(\pi_E^t) = b\pi_F^t$, where $a, b \in \mathcal{O}_F^*$. The residue class field k_E is equal to the residue class field k_F . We have isomorphisms

$$k_E = k_F \xrightarrow{\sim} U_E^{(t)}/U_E^{(t+1)}, \quad x \mapsto \overline{1 + x\pi_E^t}$$

and

$$k_F \xrightarrow{\sim} U_F^{(t)}/U_F^{(t+1)}, \quad x \mapsto \overline{1 + x\pi_F^t},$$

their domain being the additive group of the residue field. Via these isomorphisms the homomorphism \bar{N} translates into a homomorphism $\tilde{N}: k_F \rightarrow k_F$. For $x \in \mathcal{O}_F$ we have

$$\begin{aligned} N_F^E(1 + x\pi_E^t) &\equiv 1 + x\text{Tr}_F^E(\pi_E) + x^l N_F^E(\pi_E) \pmod{\mathfrak{p}_F^{t+1}} \\ &\equiv 1 + bx\pi_F^t + ax^l \pi_F^t \pmod{\mathfrak{p}_F^{t+1}} \\ &\equiv 1 + (bx + ax^l)\pi_F^t \pmod{\mathfrak{p}_F^{t+1}}. \end{aligned}$$

So the corresponding homomorphism $k_F \rightarrow k_F$ is the map

$$\tilde{N}: k_F \rightarrow k_F, \quad y \mapsto \bar{b}y + \bar{a}y^l.$$

The order of the kernel of \tilde{N} is at most l . So the order of the cokernel is at most l as well. This proves that

$$(U_F^{(t)} : U_F^{(t+1)}N_F^E(U_E^{(t)})) \leq l.$$

$t < i$: By Lemma 17.42 we have $\psi(i) = t + l(i - t)$. Since $(t + 1)(l - 1) + \psi(i) = (t + 1)(l - 1) + t + l(i - t) = li + l - 1$ and $\lfloor \frac{li + l - 1}{l} \rfloor = i$, we have by Lemma 17.41

$$\text{Tr}_F^E(\mathfrak{p}_E^{\psi(i)}) = \mathfrak{p}_F^i.$$

Also by Lemma 17.41

$$\text{Tr}_F^E(\mathfrak{p}_E^{\psi(i)+1}) = \mathfrak{p}_F^{i+1}.$$

From $\psi(i) = t + l(i - t) > t + (i - t) = i$ follows that $N_F^E(\mathfrak{p}_E^{\psi(i)}) \subseteq N_F^E(\mathfrak{p}_E^{i+1}) = \mathfrak{p}_F^{i+1}$. Hence by Lemma 17.40 for $\gamma \in \mathfrak{p}_E^{\psi(i)}$:

$$N_F^E(1 + \gamma) \equiv 1 + \text{Tr}_F^E(\gamma) \pmod{\mathfrak{p}_F^{i+1}} \quad \text{and} \quad N_F^E(1 + \gamma) \equiv 1 \pmod{\mathfrak{p}_F^i}.$$

So $N_F^E(U_E^{(\psi^{(i)})}) \subseteq U_F^{(i)}$ and $U_F^{(i+1)}N_F^E(U_E^{(\psi^{(i)})}) \subseteq U_F^{(i)}$. For the opposite inclusion let $\beta \in \mathfrak{p}_F^i$. There is a $\gamma \in \mathfrak{p}_E^{\psi^{(i)}}$ such that $\text{Tr}_F^E(\gamma) = \beta$. Then

$$N_F^E(1 + \gamma) \equiv 1 + \beta \pmod{\mathfrak{p}_F^{i+1}}$$

and it follows that $1 + \beta \in U_F^{(i+1)}N_F^E(U_E^{(\psi^{(i)})})$. \square

We generalize the lemma to the case of a Galois extension of local fields.

17.44 Lemma. *Let $E : F$ be a Galois extension of local fields. Then for each integer $i \geq -1$:*

$$N_F^E(U_E^{(\psi^{(i)})}) \subseteq U_F^{(i)} \quad \text{and} \quad N_F^E(U_E^{(\psi^{(i+1)})}) \subseteq U_F^{(i+1)},$$

and

$$(U_F^{(i)} : U_F^{(i+1)}N_F^E(U_E^{(\psi^{(i)})})) \leq \psi'_{r/l}(i).$$

PROOF. The proof is by induction on the degree of the extension. For degree 1 it is trivially true and for prime degree it is the previous lemma. Since Galois groups of local field extensions are solvable, for composite degree there exists an intermediate field E' such that $E' : F$ is a Galois extension and $E \neq E' \neq F$. By induction we assume the statements in the theorem to be true for the Galois extensions $E : E'$ and $E' : F$.

Put $G = \text{Gal}(E : F)$, $H = \text{Gal}(E : E')$ and $G' = \text{Gal}(E' : F)$. We will use

$$N_F^E = N_F^{E'}N_{E'}^E \quad \text{and} \quad \psi_G = \psi_H\psi_{G'} \text{ (Proposition 17.9).}$$

The verification of the inclusion statements is straightforward:

$$\begin{aligned} N_F^E(U_E^{(\psi_G^{(i)})}) &= N_{E'}^E N_F^{E'}(U_E^{(\psi_H\psi_{G'}^{(i)})}) \subseteq N_{E'}^E(U_{E'}^{(\psi_{G'}^{(i)})}) \subseteq U_F^{(i)}, \\ N_F^E(U_E^{(\psi_G^{(i+1)})}) &= N_{E'}^E N_F^{E'}(U_E^{(\psi_H\psi_{G'}^{(i+1)})}) \subseteq N_{E'}^E(U_{E'}^{(\psi_{G'}^{(i+1)})}) \subseteq U_F^{(i+1)}. \end{aligned}$$

For the last statement use the inclusions

$$N_{E'}^E(U_E^{(\psi_H\psi_{G'}^{(i)})}) \subseteq U_{E'}^{\psi_{G'}^{(i)}} \quad \text{and} \quad N_F^{E'}(U_{E'}^{(\psi_{G'}^{(i+1)})}) \subseteq U_F^{(i+1)} :$$

$$\begin{aligned} &(U_F^{(i)} : U_F^{(i+1)}N_F^E(U_E^{(\psi_G^{(i)})})) \\ &= (U_F^{(i)} : U_F^{(i+1)}N_F^{E'}(U_{E'}^{\psi_{G'}^{(i)}})) \cdot (U_F^{(i+1)}N_F^{E'}(U_{E'}^{\psi_{G'}^{(i)}}) : U_F^{(i+1)}N_F^E(U_E^{(\psi_G^{(i)})})) \\ &\leq \psi'_{G',r/l}(i) \cdot (U_F^{(i+1)}N_F^{E'}(U_{E'}^{\psi_{G'}^{(i)}}) : U_F^{(i+1)}N_F^{E'}N_{E'}^E(U_E^{(\psi_H\psi_{G'}^{(i)})})) \\ &\leq \psi'_{G',r/l}(i) \cdot (U_F^{(i+1)}N_F^{E'}(U_{E'}^{\psi_{G'}^{(i)}}) : U_F^{(i+1)}N_F^{E'}(U_{E'}^{(\psi_{G'}^{(i+1)})})N_{E'}^E(U_E^{(\psi_H\psi_{G'}^{(i)})})) \\ &\leq \psi'_{G',r/l}(i) \cdot (U_{E'}^{\psi_{G'}^{(i)}} : U_{E'}^{(\psi_{G'}^{(i+1)})})N_{E'}^E(U_E^{(\psi_H\psi_{G'}^{(i)})}) \end{aligned}$$

$$\leq \psi'_{G',r/l}(i) \cdot \psi'_{H,r/l}(\psi_{G'(i)}) = \frac{\psi'_{G',r}(i)}{\psi'_{G',l}(i)} \cdot \frac{\psi'_{H,r}(\psi_{G'(i)})}{\psi'_{H,l}(\psi_{G'(i)})} = \frac{\psi'_{G,r}(i)}{\psi'_{G,l}(i)} = \psi'_{G,r/l}(i).$$

The ψ -functions have only finitely many breaks, so the chain rule for the left and right derivatives applies. \square

17.45 Lemma. *Let $E : F$ be an abelian extension of local fields. Then for each integer $i \geq -1$:*

$$(U_F^{(i)} N_F^E(E^*) : U_F^{(i+1)} N_F^E(E^*)) = (U_F^{(i)} : U_F^{(i+1)} N_F^E(U_E^{(\psi(i))})) = \psi'_{r/l}(i).$$

PROOF. There is an integer t such that $U_F^{(t)} \subseteq N_F^E(E^*)$ and ψ has no break for all $x \geq t$. Consider the chain

$$\begin{array}{ccccccc} U_F^{(-1)} N_F^E(E^*) & \supseteq & U_F^{(0)} N_F^E(E^*) & \supseteq & \cdots & \supseteq & U_F^{(t)} N_F^E(E^*) \\ \parallel & & & & & & \parallel \\ F^* & & & & & & N_F^E(E^*) \end{array}$$

By Lemma 17.44

$$(U_F^{(i)} N_F^E(E^*) : U_F^{(i+1)} N_F^E(E^*)) \leq (U_F^{(i)} : U_F^{(i+1)} N_F^E(U_E^{(\psi(i))})) \leq \psi'_{r/l}(i). \quad (17.2)$$

So we have

$$\begin{aligned} [E : F] &= (F^* : N_F^E(E^*)) = \prod_{i=-1}^{t-1} (U_F^{(i)} N_F^E(E^*) : U_F^{(i+1)} N_F^E(E^*)) \\ &\leq \prod_{i=-1}^{t-1} \psi'_{r/l}(i) = \prod_{i=-1}^{t-1} \frac{\psi'_r(i)}{\psi'_l(i)} = \frac{1}{\psi'_l(-1)} \cdot \prod_{i=0}^{t-1} \frac{\psi'_r(i-1)}{\psi'_l(i)} \cdot \psi'_r(t-1) \\ &\leq f_F^{(E)} e_F^{(E)} = [E : F], \end{aligned}$$

where $\frac{\psi'_r(i-1)}{\psi'_l(i)} \leq 1$ because of the function ψ being concave. It follows that the inequalities in (17.2) are actually equalities. \square

The proof also shows that $\psi'_r(i-1) = \psi'_l(i)$ for all integers i . This proves:

17.46 Theorem (Hasse-Arf). *Let $E : F$ an abelian extension of local fields. Then the function $\psi = \psi_G$ has only breaks at integral arguments.* \square

17.47 Lemma. *Let $E : F$ be an abelian extension of local fields. Then for each integer $t \geq -1$:*

$$W_F^{(t)} = \{1\} \iff V_F^{(t)} = \{1\}.$$

PROOF. We have:

$$\begin{aligned}
 W_F^{(t)} = \{1\} &\iff U_F^{(t)} N_F^E(E^*) = N_F^E(E^*) \iff (F^* : U_F^{(t)} N_F^E(E^*)) = [E : F] \\
 &\iff \prod_{i=-1}^{t-1} (U_F^{(i)} N_F^E(E^*) : U_F^{(i+1)} N_F^E N_F^E(E^*)) = [E : F] \\
 &\iff \prod_{i=-1}^{t-1} \psi'_{r/l}(i) = [E : F] \quad (\text{Lemma 17.45}) \\
 &\iff \prod_{i=t}^{\infty} \psi'_{r/l}(i) = 1 \iff \psi'_{r/l}(i) = 1 \text{ for all integers } i \geq t \\
 &\iff \psi'_{r/l}(x) = 1 \text{ for all } x \in [t, \infty) \\
 &\iff \psi'_r(t) = \psi'_l(t) = \#(V_{F,0}(E)) \iff V_{F,\psi(t)}(E) = \{1\} \\
 &\iff V_F^{(t)}(E) = \{1\}. \quad \square
 \end{aligned}$$

17.48 Theorem. Let $E : F$ be an abelian extension of local fields. Then $W_F^{(i)}(E) = V_F^{(i)}(E)$ for all $i \geq -1$.

PROOF. Let i be an integer ≥ -1 . For each subgroup H of $\text{Gal}(E : F)$:

$$\begin{aligned}
 W_F^{(i)}(E) \subseteq H &\iff \vartheta_F^{(E)}(U_F^{(i)}) \subseteq H \\
 &\iff \vartheta_F^{(E^H)}(U_F^{(i)}) = \{1\} \\
 &\iff W_F^{(i)}(E^H) = \{1\} \\
 &\iff V_F^{(i)}(E^H) = \{1\} \quad (\text{Lemma 17.47}) \\
 &\iff V_F^{(i)}(E) \subseteq H.
 \end{aligned}$$

Therefore, $W_F^{(i)}(E) = V_F^{(i)}(E)$. □

17.4 The Conductor-Discriminant Formula

17.49 Notations. Let $E : F$ be an abelian extension of local fields and $\chi \in \text{Gal}(E : F)^\vee$. Then the field F_χ is the intermediate field of $E : F$ corresponding to the subgroup $\text{Ker}(\chi)$ of $\text{Gal}(E : F)$:

$$F_\chi = E^{\text{Ker}(\chi)}.$$

The conductor of $F_\chi : F$ is denoted by \mathfrak{f}_χ .

17.50 Theorem (Local Conductor-Discriminant Formula). *Let $E : F$ be an abelian extension of local fields and $G = \text{Gal}(E : F)$. Then*

$$v_F(\mathfrak{d}_F(E)) = \sum_{\chi \in G^\vee} v_F(\mathfrak{f}_\chi).$$

PROOF. Let $\chi \in G^\vee$. Then for $i \in \mathbb{N}$:

$$\begin{aligned} v_F(\mathfrak{f}_\chi) \leq i &\iff U_F^{(i)} \subseteq N_{F^\chi}^{F_\chi}(F_\chi) \\ &\iff W_F^{(i)}(F_\chi) = \{1\} \\ &\iff V_F^{(i)}(F_\chi) = \{1\} && \text{(Lemma 17.47)} \\ &\iff V_F^{(i)}(E) \subseteq \text{Gal}(E : F_\chi) && \text{(Theorem 17.11)} \\ &\iff V_F^{(i)} \subseteq \text{Ker}(\chi). \end{aligned}$$

We have for each i

$$\sum_{\sigma \in V_F^{(i)}(E)} \chi(\sigma) = \begin{cases} 0 & \text{if } V_F^{(i)}(F_\chi) \neq \{1\}, \\ \#(V_F^{(i)}(E)) & \text{if } V_F^{(i)}(F_\chi) = \{1\}. \end{cases}$$

So

$$v_F(\mathfrak{f}_\chi) = \sum_{i=0}^{v_F(\mathfrak{f}_\chi)-1} 1 = \sum_{i=0}^{\infty} \frac{\#(V_F^{(i)}(E)) - \sum_{\sigma \in V_F^{(i)}(E)} \chi(\sigma)}{\#(V_F^{(i)}(E))}.$$

Summation over all χ gives:

$$\begin{aligned} \sum_{\chi \in G^\vee} v_F(\mathfrak{f}_\chi) &= \sum_{i=0}^{\infty} \frac{n\#(V_F^{(i)}(E)) - \sum_{\chi \in G^\vee} \sum_{\sigma \in V_F^{(i)}(E)} \chi(\sigma)}{\#(V_F^{(i)}(E))} \\ &= \sum_{i=0}^{\infty} \frac{n\#(V_F^{(i)}(E)) - \sum_{\sigma \in V_F^{(i)}(E)} \sum_{\chi \in G^\vee} \chi(\sigma)}{\#(V_F^{(i)}(E))} \\ &= \sum_{i=0}^{\infty} \frac{n\#(V_F^{(i)}(E)) - n}{\#(V_F^{(i)}(E))} = n \sum_{i=0}^{\infty} \left(1 - \frac{1}{\#(V_F^{(i)}(E))}\right). \end{aligned}$$

By Theorem 17.37

$$v_F(\mathfrak{d}_F(E)) = f_F^{(E)} \cdot v_E(\mathfrak{d}_F(E)) = f_F^{(E)} e_F^{(E)} \sum_{i=0}^{\infty} \left(1 - \frac{1}{\#(V_F^{(i)}(E))}\right). \quad \square$$

So for an abelian extension $E : F$ of local fields with Galois group G we obtain

$$\mathfrak{d}_F(E) = \prod_{\chi \in G^\vee} \mathfrak{f}_\chi.$$

The discriminant of a number field extension is the product of its local discriminants. As a consequence we obtain a global formula:

17.51 Theorem (Global Conductor-Discriminant Formula). *Let $L : K$ be an abelian extension of number fields. Then*

$$\mathfrak{d}_K(L) = \prod_{\chi \in \mathcal{H}(L:K)} \mathfrak{f}_{\chi,0}.$$

where $\mathfrak{f}'_{\chi,0}$ denotes the finite part of the modulus \mathfrak{f}_{χ} .

PROOF. The identity can be interpreted as an identity of ideals of \mathcal{O}_K . Let $\mathfrak{p} \in \text{Max}(\mathcal{O}_K)$. We will show that

$$v_{\mathfrak{p}}(\mathfrak{d}_K(L)) = \sum_{\chi \in \mathcal{H}(L:K)} v_{\mathfrak{p}}(\mathfrak{f}_{\chi}).$$

Fix a $\mathfrak{q} \in \text{Max}(\mathcal{O}_L)$ above \mathfrak{p} . Put $G = \text{Gal}(L : K)$ and $Z = Z_{\mathfrak{p}}^{(L)}$. By Theorem 17.28

$$\mathfrak{d}_K(L) = (\mathfrak{d}_K(L^Z))^{\#(Z)} \cdot N_K^{L^Z}(\mathfrak{d}_{L^Z}(L)) = N_K^{L^Z}(\mathfrak{d}_{L^Z}(L)).$$

So $v_{\mathfrak{p}}(\mathfrak{d}_K(L)) = (G : Z) \cdot v_{\mathfrak{q}^z}(\mathfrak{d}_{L^Z}(L))$. From Theorem 17.50 follows via the dual Artin isomorphism

$$v_{\mathfrak{q}^z}(\mathfrak{d}_{L^Z}(L)) = \sum_{\chi \in Z^{\vee}} v_{\mathfrak{q}^z}(\mathfrak{f}_{\chi}).$$

The number of characters of G which coincide on Z is $(G : Z)$. Hence

$$\sum_{\chi \in G^{\vee}} v_{\mathfrak{p}}(\mathfrak{f}_{\chi}) = (G : Z) \sum_{\chi \in Z^{\vee}} v_{\mathfrak{q}^z}(\mathfrak{f}_{\chi}) = (G : Z) v_{\mathfrak{q}^z}(\mathfrak{d}_{L^Z}(L)) = v_{\mathfrak{p}}(\mathfrak{d}_K(L)). \quad \square$$

This theorem leads to connections between the discriminant of a noncyclic abelian extension of number fields and the discriminant of its subextensions. In full generality this connection is explained in section 18.3. Here is a special case:

17.52 Corollary. *Let p be a prime number and $L : K$ an abelian extension of number fields with an elementary p -group of rank 2 as Galois group. Then*

$$\mathfrak{d}_K(L) = \prod_{i=1}^{p+1} \mathfrak{d}_K(L_i),$$

where L_1, \dots, L_{p+1} are the intermediate fields of degree p over K .

PROOF. The group $\mathcal{H}(L : K)$ is an elementary p -group of rank 2. The intermediate fields of degree p over K correspond subgroups of $\mathcal{H}(L : K)$ of order p . The

subsets $\mathcal{H}(L : K_i) \setminus \{1\}$ form a partition of $\mathcal{H}(L : K) \setminus \{1\}$. Hence, by Theorem 17.51 and since $\mathfrak{f}_{1,0} = (1)$,

$$\mathfrak{d}_K(L) = \prod_{i=1}^{p+1} \prod_{\chi \in \mathcal{H}(L_i:K)} \mathfrak{f}_{\chi,0} = \prod_{i=1}^{p+1} \mathfrak{d}_K(L_i). \quad \square$$

This generalizes the formula obtained in exercise 9 of chapter 1.

EXERCISES

1. Verify Theorem 17.11 for the three quadratic subfields of the biquadratic field in Example 17.13
2. In Example 17.17 the ramification groups $V^{(i)}$ for an odd prime p in $\mathbb{Q}(\zeta_{p^r})$ have been computed. Compute the different of the extension $\mathbb{Q}_p(\zeta_{p^r}) : \mathbb{Q}_p$ using Theorem 17.37. Compare the answer with the formula of Proposition 1.54.
3. Show that Theorem 7.28 follows from Theorem 17.23 and Theorem 17.26.
4. Show that Proposition 9.91 follows from Theorem 17.51.
5. Show that Proposition 7.30 follows from Theorem 17.23 and Theorem 17.25.
6. Let $E : F$ be an abelian extension of local fields. Prove that $E : F$ is tamely ramified if and only if $\mathfrak{f}_F(E) \mid \mathfrak{p}_F$. (Hint: use Theorem 17.48.)
7. Let $L : K$ be a tamely ramified abelian extension of number fields. Prove that $\mathfrak{f}_K(L)$ is squarefree, i.e. not divisible by the square of a finite prime of K .

18 Zeta Function Relations

In algebraic number theory various structures associated to a number field come up: ideal class group, unit group, ray class group, zeta function and many more. In this chapter we study for a Galois extension of number fields relations between these structures for the intermediate fields of the extension. This is done by studying norm relations, relations of norm elements in the group ring of the Galois group. In section 18.1 norm relations of a finite group are introduced and it is shown how they are related to the noncyclic subgroups of the group. For a finite abelian group a special norm relation is obtained using the characters of the group. For modules A over a finite abelian group G group having the property that multiplication by $\#(G)$ is an isomorphism, a norm relation leads to a relation between the submodules A^U for subgroups U of G . This is shown in section 18.2. In section 18.3 it is shown that a norm relation leads to a relation between the zeta functions of intermediate fields as well as for the discriminants of these fields.

The relations are especially interesting if in the group ring the element 1 is a combination of norm elements of nontrivial subgroups. If such a norm relation does not exist the group is called strongly exceptional. In the last section it is shown that a group is strongly exceptional if and only if all subgroups of order pq with p and q not necessarily distinct prime numbers, are cyclic. Modules over noncyclic groups of order pq with p and q prime have been studied in the sections 12.5 and 12.6.

18.1 Norm relations

The argument used in Example 5.37 is based on the following relation for the elements N_G, N_σ, N_τ and $N_{\sigma\tau}$ in $\mathbb{Z}[G]$, where $G = \langle \sigma, \tau \rangle \cong C_2 \times C_2$:

$$2 = N_\sigma + N_\tau + N_{\sigma\tau} - N_G.$$

For example for $\nu \in \mathcal{O}_K^*$ this implies

$$\nu^2 \in (\mathcal{O}_K^*)^\sigma (\mathcal{O}_K^*)^\tau (\mathcal{O}_K^*)^{\sigma\tau} (\mathcal{O}_K^*)^G = \langle -1, 2 + \sqrt{3} \rangle.$$

In this section this kind of relations will be studied. The following notations will be used for various collections of subgroups.

18.1 Notations. Collections of subgroups of a finite group G :

$\Omega(G)$: the collection of cyclic subgroups of G ,

$\Omega_0(G)$: the collection of nontrivial cyclic subgroups of G ,

$\Omega'(G)$: the collection of noncyclic subgroups of G ,

$\Sigma(G)$: the collection of subgroups of G ,

$\Sigma_0(G)$: the collection of nontrivial subgroups of G ,

$\Upsilon(G)$: the collection of normal subgroups H of G such that G/H is a finite cyclic group,

$\Upsilon_0(G)$: the collection of H in $\Upsilon(G)$ with $H \neq G$.

The free abelian group on a set X will be denoted by $\mathbb{Z}X$ or occasionally, for reasons of clarity, by $\mathbb{Z} \cdot X$. For a group G the abelian group $\mathbb{Z}G$ has in a natural way the structure of a ring. With this ring structure it is the group ring $\mathbb{Z}[G]$.

18.2 Definition. Let G be a finite group. A *norm relation* of G is an element of the kernel of the homomorphism

$$\pi_G: \mathbb{Z}\Sigma(G) \rightarrow \mathbb{Z}[G], \quad \sum_{U \in \Sigma(G)} n_U U \mapsto \sum_{U \in \Sigma(G)} n_U N_U$$

The kernel of π_G is the *group of norm relations* of G and is denoted by $\text{NR}(G)$. So $\sum_{U \in \Sigma(G)} n_U U$ is a norm relation of G if and only if $\sum_{U \in \Sigma(G)} n_U N_U = 0$.

18.3 Lemma. Let G be a finite group and let the homomorphism $\pi'_G: \mathbb{Z}\Sigma(G) \rightarrow \mathbb{Z}\Omega(G)$ be defined by $\pi'_G(U) = \sum_{H \in \Omega(U)} H$ on basis elements $U \in \Sigma(G)$. Then $\text{Ker}(\pi'_G) = \text{NR}(G)$.

PROOF. For $H \in \Omega(G)$ put

$$[H] = \{ \sigma \in G \mid \langle \sigma \rangle = H \}.$$

It is an equivalence class of the equivalence relation in G defined by

$$\sigma \sim \tau \iff \langle \sigma \rangle = \langle \tau \rangle.$$

For $H \in \Omega(G)$ put

$$S_H = \sum_{\sigma \in [H]} \sigma.$$

Then

$$N_U = \sum_{H \in \Omega(U)} S_U.$$

Let the homomorphism $\gamma_G: \mathbb{Z}\Omega(G) \rightarrow \mathbb{Z}[G]$ be defined by $\gamma_G(H) = S_H$ on basis elements $H \in \Omega(G)$. Then for each $U \in \Sigma(G)$:

$$\gamma_G \pi'_G(U) = \gamma_G\left(\sum_{H \in \Omega(U)} H\right) = \sum_{H \in \Omega(U)} S_H = N_U.$$

So $\gamma_G \pi'_G = \pi_G$. Since γ_G is injective, it follows that $\text{Ker}(\pi'_G) = \text{Ker}(\gamma_G \pi'_G) = \text{Ker}(\pi_G) = \text{NR}(G)$. \square

18.4 Lemma. *Let G be a finite group and let the homomorphism $\psi_G: \mathbb{Z}\Omega(G) \rightarrow \mathbb{Z}\Sigma(G)$ be defined by $\psi_G(H) = \sum_{H^* \in \Omega(H)} \mu(H : H^*)H^*$ on basis elements $H \in \Omega(G)$. Then $\pi'_G \psi_G$ is the identity on $\mathbb{Z}\Omega(G)$.*

The coefficient $\mu(H : H^*)$ is the Möbius function applied to the index $(H : H^*)$, so $\mu(H : H^*) = \mu((H : H^*))$.

PROOF. Let $H \in \Omega(G)$ and $n = \#(H)$. For each $d \mid n$ there is a unique subgroup H_d of H with $\#(H_d) = d$. We have

$$\begin{aligned} \psi_G \pi'_G(H) &= \psi_G\left(\sum_{d \mid n} H_d\right) = \sum_{d \mid n} \psi_G(H_d) \\ &= \sum_{d \mid n} \sum_{s \mid d} \mu\left(\frac{d}{s}\right) H_s = \sum_{s \mid n} \sum_{t \mid \frac{n}{s}} \mu(t) H_s = H_n = H. \end{aligned} \quad \square$$

As a consequence a \mathbb{Z} -basis of $\text{NR}(G)$ is formed by the elements

$$\begin{aligned} U - \psi_G \pi'_G(U) &= U - \sum_{H \in \Omega(U)} \psi_G(H) = U - \sum_{H \in \Omega(U)} \sum_{H^* \in \Omega(H)} \mu(H : H^*)H^* \\ &= U - \sum_{H^* \in \Omega(U)} \sum_{\substack{H \in \Omega(U) \\ H \supseteq H^*}} \mu(H : H^*)H^*, \end{aligned}$$

where $U \in \Omega'(G)$. This leads to the following definition.

18.5 Definition. Let G be a finite group. For each $H \in \Omega(G)$ the *norm coefficient* $d_G(H)$ of H in G is the integer defined as follows:

$$d_G(H) = \sum_{\substack{H^* \in \Omega(G) \\ H^* \supseteq H}} \mu(H^* : H).$$

We have shown:

18.6 Theorem. *Let G be a finite group. Then the abelian group $\text{NR}(G)$ is freely generated by the elements*

$$U - \sum_{H \in \Omega(U)} d_U(H)H,$$

where $U \in \Omega'(G)$. □

18.7 Definition. Let G be a finite group. The element $G - \sum_{H \in \Omega(G)} d_G(H)H \in \text{NR}(G)$ is called the *principal norm relation* of G .

Nontrivial norm relations of a group G may have consequences for the structure of G -modules.

18.8 Notation. Let G be a nontrivial finite group and A a G -module. The submodule of A generated by all A^U for $U \in \Sigma_0(G)$ is denoted by A_0 . So

$$A_0 = \sum_{U \in \Sigma_0(G)} A^U.$$

18.9 Lemma. *Let G be a nontrivial finite group, A a G -module and $\sum_U n_U U$ a norm relation of G . Then*

$$n_{\{1\}}A \subseteq A_0.$$

PROOF. The identity $n_{\{1\}} = -\sum_{U \in \Sigma_0(G)} n_U N_U$ implies

$$n_{\{1\}}A \subseteq \sum_{U \in \Sigma_0(G)} n_U N_U A \subseteq \sum_{U \in \Sigma_0(G)} n_U A^U \subseteq A_0. \quad \square$$

18.10 Definition. Let G be a finite group. The coefficient $d_G(\{1\})$ is called the *trivial norm coefficient* of G .

18.11 Example. Let p be a prime number and G an elementary abelian p -group of rank $r \geq 2$. There are $\frac{p^r-1}{p-1}$ nontrivial cyclic subgroups, each of order p . In this case $d_G(H) = 1$ for each $H \in \Omega_0(G)$ and $d_G(\{1\}) = 1 - \frac{p^r-1}{p-1} = -\frac{p^r-p}{p-1}$. So we have the identity

$$N_G = -\frac{p^r-p}{p-1} + \sum_{H \in \Omega_0(G)} N_H.$$

For $r = 2$ we get

$$N_G = -p + \sum_{H \in \Omega_0(G)} N_H.$$

In section 12.5 this identity was easily obtained by direct computation. The trivial norm coefficient of this group is $-p$. For $r > 2$ there are more noncyclic subgroups and, therefore, more norm relations.

18.12 Example. Let G be the group considered in section 12.6. We use the notation of that section. Let's for simplicity assume that q is prime. Then G is the unique nonabelian group of order pq . The group G has exactly p subgroups of order q : the groups $\langle \sigma^i \tau \rangle$ for $i = 0, \dots, p-1$. By Theorem 18.6

$$N_G = -p + N_\sigma + \sum_{i=0}^{p-1} N_{\sigma^i \tau}.$$

The same identity was obtained in section 12.6 by direct computation. The trivial norm coefficient is $-p$.

18.13 Example. The group $G = A_4$ of even permutations of four elements has two noncyclic subgroups: A_4 itself and a subgroup V of order 4. There are three subgroups B_1, B_2 and B_3 of order 2 and four subgroups C_1, C_2, C_3 and C_4 of order 3. The group $\text{NR}(G)$ is of rank 2 and is generated by

$$\begin{aligned} R_G &= G - B_1 - B_2 - B_3 - C_1 - C_2 - C_3 - C_4 + 6\{1\}, \\ R_V &= V - B_1 - B_2 - B_3 + 2\{1\}. \end{aligned}$$

The norm relation $R_G - R_V = G - V - C_1 - C_2 - C_3 - C_4 + 4\{1\}$ shows that a finite G -module A is up to 2-torsion generated by the submodules A^V and A^{C_i} ($i = 1, \dots, 4$).

18.14 Example. Let G be the symmetric group S_n with $n \geq 4$. Then G has a subgroup isomorphic to $C_2 \times C_2$ and also a subgroup isomorphic to S_3 . The norm coefficients of these groups are -2 and -3 respectively. So a finite G -module is the sum of submodules A^H with H nontrivial.

A norm relation of a group induces a norm relation of each of its subgroups:

18.15 Proposition. Let G be a finite group, V a subgroup of G and $\sum_{U \in \Sigma(G)} n_U U$ a norm relation of G . Then

$$\sum_{U \in \Sigma(G)} n_U (U \cap V) \in \text{NR}(V).$$

PROOF. Let $\pi_V: \mathbb{Z}[G] \rightarrow \mathbb{Z}[V]$ be the homomorphism determined by

$$\pi_V(\sigma) = \begin{cases} \sigma & \text{if } \sigma \in V, \\ 0 & \text{if } \sigma \in G \setminus V. \end{cases}$$

Then for each $U \in \Sigma(G)$:

$$\pi_V(N_U) = \pi_V\left(\sum_{\sigma \in U} \sigma\right) = \sum_{\sigma \in U} \pi_V(\sigma) = \sum_{\sigma \in U \cap V} \sigma = N_{U \cap V}.$$

Application of π_V to $\sum_{U \in \Sigma(G)} n_U N_U = 0$ yields

$$\sum_{U \in \Sigma(G)} n_U N_{U \cap V} = 0. \quad \square$$

18.16 Proposition. *Let G be a finite group and $\sum_{U \in \Sigma(U)} n_U U$ a norm relation of G . Then*

$$\sum_{U \in \Sigma(G)} n_U \#(U) = 0 \quad \text{and} \quad \sum_{U \in \Sigma(G)} n_U = 0.$$

PROOF. For the first identity apply the augmentation to $\sum_{U \in \Sigma(G)} n_U N_U = 0$. For the second take $V = \{1\}$ in Proposition 18.15. \square

We conclude this section with functorial properties of the group of norm relations. A group homomorphism $f: G_1 \rightarrow G_2$ determines a ring homomorphism $f_*: \mathbb{Z}[G_1] \rightarrow \mathbb{Z}[G_2]$ by $f_*(\sigma) = f(\sigma)$ on basis elements. For U a subgroup of G_1 we have $f_*(N_U) = \#(U \cap \text{Ker}(f)) \cdot N_{f(U)}$. Define $f_*: \mathbb{Z}\Sigma(G_1) \rightarrow \mathbb{Z}\Sigma(G_2)$ by

$$f_*(U) = \#(U \cap \text{Ker}(f)) \cdot f(U)$$

on basis elements $U \in \Sigma(G_1)$. Then the following square of abelian groups commutes:

$$\begin{array}{ccc} \mathbb{Z}\Sigma(G_1) & \xrightarrow{\pi_{G_1}} & \mathbb{Z}[G_1] \\ f_* \downarrow & & \downarrow f_* \\ \mathbb{Z}\Sigma(G_2) & \xrightarrow{\pi_{G_2}} & \mathbb{Z}[G_2] \end{array}$$

So $f: G_1 \rightarrow G_2$ induces by restriction of $f_*: \mathbb{Z}\Sigma(G_1) \rightarrow \mathbb{Z}\Sigma(G_2)$ a homomorphism $f_* = \text{NR}(f): \text{NR}(G_1) \rightarrow \text{NR}(G_2)$:

$$\begin{aligned} f_* \left(\sum_{U \in \Sigma(G_1)} n_U U \right) &= \sum_{U \in \Sigma(G_1)} n_U \#(U \cap \text{Ker}(f)) \cdot f(U) \\ &= \sum_{U' \in \Sigma(G_2)} \left(\sum_{\substack{U \in \Sigma(G_1) \\ f(U)=U'}} n_U \#(U \cap \text{Ker}(f)) \right) U'. \end{aligned}$$

18.17 Proposition. *NR is a functor from finite groups to abelian groups.*

PROOF. Clearly $\text{NR}(1_G) = 1_{\text{NR}(G)}$. Let $f: G_1 \rightarrow G_2$ and $g: G_2 \rightarrow G_3$ be homomorphisms of finite groups. It suffices to show that for $U \in \Sigma(G_1)$ we have $(gf)_*(U) = g_*(f_*(U))$. For this consider the following commutative triangle of surjective group homomorphisms:

$$\begin{array}{ccc}
 U & \xrightarrow{f|_U} & f(U) \\
 & \searrow gf|_U & \swarrow g|_{f(U)} \\
 & & gf(U)
 \end{array}$$

The kernels form a short exact sequence:

$$0 \longrightarrow U \cap \text{Ker}(f) \longrightarrow U \cap \text{Ker}(f'f) \longrightarrow f(U) \cap \text{Ker}(f') \longrightarrow 0.$$

Therefore, $\#(U \cap \text{Ker}(gf)) = \#(U \cap \text{Ker}(f)) \cdot \#(f(U) \cap \text{Ker}(g))$. □

18.2 Norm relations for abelian groups

In this section G is a finite abelian group of order n and R a commutative ring in which n is a unit: $n \in R^*$. We will derive for a finite abelian group G an orthogonal system of idempotents of the group algebra $\mathbb{Z}[\frac{1}{n}][G]$ and consider its consequences for the structure of $R[G]$ -modules. The idempotents will correspond to subgroups $H \in \Upsilon(G)$. It leads to both a norm relation for these subgroups and a relation for the submodules A^H of an $R[G]$ -module A . Note that there is a unique ring homomorphism $\mathbb{Z}[\frac{1}{n}] \rightarrow R$.

18.18 Definition and notation. Let $\chi \in G^\vee$. Then an element ε_χ of the group algebra of G over $\mathbb{Z}[\frac{1}{n}, \zeta_n]$ is defined as follows:

$$\varepsilon_\chi = \frac{1}{n} \sum_{\sigma \in G} \chi(\sigma) \sigma^{-1} \in \mathbb{Z}[\frac{1}{n}, \zeta_n][G].$$

18.19 Lemma. *The collection $(\varepsilon_\chi)_{\chi \in G^\vee}$ is a collection of orthogonal idempotents of the group algebra $\mathbb{Z}[\frac{1}{n}, \zeta_n][G]$.*

PROOF. Let $\chi, \eta \in G^\vee$. Then

$$\begin{aligned} n^2 \varepsilon_\chi \varepsilon_\eta &= \left(\sum_{\sigma \in G} \chi(\sigma) \sigma^{-1} \right) \left(\sum_{\tau \in G} \eta(\tau) \tau^{-1} \right) = \sum_{\sigma, \tau \in G} \chi(\sigma) \eta(\tau) \sigma^{-1} \tau^{-1} \\ &= \sum_{\sigma, \rho \in G} \chi(\sigma) \eta(\sigma^{-1} \rho) \rho^{-1} = \sum_{\sigma, \rho \in G} \chi \eta^{-1}(\sigma) \eta(\rho) \rho^{-1} \\ &= \left(\sum_{\sigma \in G} \chi \eta^{-1}(\sigma) \right) \left(\sum_{\rho \in G} \eta(\rho) \rho^{-1} \right) = \left(\sum_{\sigma \in G} \chi \eta^{-1}(\sigma) \right) \cdot n \varepsilon_\eta. \end{aligned}$$

For $\chi \neq \eta$ the first factor equals 0 and for $\chi = \eta$ it equals n . □

18.20 Lemma. *The ε_χ form a basis of the free $\mathbb{Z}[\frac{1}{n}, \zeta_n]$ -module $\mathbb{Z}[\frac{1}{n}, \zeta_n][G]$.*

PROOF. For $\chi \in G^\vee$ and $\sigma \in G$ we have

$$\varepsilon_\chi \sigma = \frac{1}{n} \sum_{\tau \in G} \chi(\tau) \tau^{-1} \sigma = \frac{1}{n} \sum_{\rho \in G} \chi(\sigma \rho) \rho^{-1} = \frac{1}{n} \chi(\sigma) \sum_{\rho \in G} \chi(\rho) \rho^{-1} = \chi(\sigma) \varepsilon_\chi.$$

So for $\alpha = \sum_{\sigma \in G} a_\sigma \sigma \in \mathbb{Z}[\frac{1}{n}, \zeta_n][G]$

$$\alpha = \left(\sum_{\chi \in G^\vee} \varepsilon_\chi \right) \left(\sum_{\sigma \in G} a_\sigma \sigma \right) = \sum_{\chi \in G^\vee} \left(\sum_{\sigma \in G} a_\sigma \chi(\sigma) \right) \varepsilon_\chi.$$

If $\sum_{\chi \in G^\vee} a_\chi \varepsilon_\chi = 0$ with $a_\chi \in \mathbb{Z}[\frac{1}{n}, \zeta_n]$, then for all $\eta \in G^\vee$

$$0 = \varepsilon_\eta \sum_{\chi \in G^\vee} a_\chi \varepsilon_\chi = a_\eta \varepsilon_\eta$$

and so $a_\chi = 0$ for all $\chi \in G^\vee$. So the ε_χ generate the group algebra as $\mathbb{Z}[\frac{1}{n}, \zeta_n]$ -module and, moreover, they are independent. □

18.21 Notations. Subgroups $V \in \Sigma(G^\vee)$ correspond to subgroups $U \in \Sigma(G)$ as follows:

$$V^\perp = \{ \sigma \in G \mid \chi(\sigma) = 1 \text{ for all } \chi \in V \}$$

and

$$U^\perp = \{ \chi \in G^\vee \mid \chi(\sigma) = 1 \text{ for all } \sigma \in U \}.$$

The collection of subgroups H of a finite abelian group G with G/H cyclic is denoted by $\Upsilon(G)$. Groups in $\Upsilon(G)$ correspond to groups in $\Omega(G^\vee)$.

Summation over the characters vanishing on a subgroup $U \in \Sigma(G)$ yields the obvious idempotent:

18.22 Lemma. *Let $U \in \Sigma(G)$. Then*

$$\sum_{\chi \in U^\perp} \varepsilon_\chi = \frac{N_U}{\#(U)} \in \mathbb{Z}[\frac{1}{n}][G].$$

PROOF. Characters vanishing on U correspond to characters of G/U , so

$$\sum_{\chi \in U^\perp} \chi(\sigma) = \begin{cases} 0 & \text{if } \sigma \notin U \\ (G : U) & \text{if } \sigma \in U. \end{cases}$$

Using this identity:

$$\begin{aligned} \sum_{\chi \in U^\perp} \varepsilon_\chi &= \frac{1}{n} \sum_{\chi \in U^\perp} \sum_{\sigma \in G} \chi(\sigma) \sigma^{-1} = \frac{1}{n} \sum_{\sigma \in G} \left(\sum_{\chi \in U^\perp} \chi(\sigma) \right) \sigma^{-1} \\ &= \frac{1}{n} \sum_{\sigma \in U} (G : U) \sigma^{-1} = \frac{1}{n} (G : U) N_U = \frac{N_U}{\#(U)}. \end{aligned} \quad \square$$

18.23 Definition. For $H \in \Upsilon(G)$ the idempotent ε_H is defined by

$$\varepsilon_H = \sum_{\substack{\chi \in G^\vee \\ \langle \chi \rangle^\perp = H}} \varepsilon_\chi.$$

18.24 Proposition. *Let $H \in \Upsilon(G)$. Then*

$$\varepsilon_H = \sum_{\substack{H^* \in \Upsilon(G) \\ H^* \subseteq H}} \mu(H^* : H) \frac{N_{H^*}}{\#(H^*)}$$

In particular $\varepsilon_H \in \mathbb{Z}[\frac{1}{n}][G]$.

PROOF. For each $d \mid (G : H)$ let $H_d \in \Upsilon(G)$ be the unique group H_d satisfying $H \leq H_d \leq G$ and $(H_d : H) = d$. By Lemma 18.22 we have

$$\frac{N_H}{\#(H)} = \sum_{d \mid (G:H)} \varepsilon_{H_d}$$

and by Möbius inversion

$$\varepsilon_H = \sum_{d \mid (G:H)} \mu(d) \frac{N_{H_d}}{\#(H_d)}. \quad \square$$

Since the ε_H are actually elements of $\mathbb{Z}[\frac{1}{n}][G]$ we have:

18.25 Theorem. *The system $(\varepsilon_H)_{H \in \Upsilon(G)}$ is a system of orthogonal idempotents of the group algebra $\mathbb{Z}[\frac{1}{n}][G]$. □*

Norm relations

In order to avoid confusion let's denote the standard basis elements of the group algebra $\mathbb{Z}[\zeta_n, \frac{1}{n}][G^\vee]$ by $[\chi]$. From Lemma 18.20 it follows that we have an isomorphism

$$\mathbb{Z}[\zeta_n, \frac{1}{n}][G^\vee] \longrightarrow \mathbb{Z}[\zeta_n, \frac{1}{n}][G], \quad [\chi] \mapsto \varepsilon_\chi \quad (18.1)$$

of $\mathbb{Z}[\zeta_n, \frac{1}{n}]$ -modules. This isomorphism induces a bijection $\text{NR}(G^\vee) \xrightarrow{\sim} \text{NR}(G)$:

18.26 Theorem.

$$\sum_{V \in \Sigma(G^\vee)} n_V V \in \text{NR}(G^\vee) \iff \sum_{U \in \Sigma(G)} (G : U) n_{U^\perp} U \in \text{NR}(G).$$

PROOF. The isomorphism (18.1) maps

$$\sum_{V \in \Sigma(G^\vee)} n_V N_V$$

to

$$\sum_{V \in \Sigma(G^\vee)} n_V \sum_{\chi \in V} \varepsilon_\chi = \sum_{V \in \Sigma(G^\vee)} n_V \frac{N_{V^\perp}}{\#(V^\perp)} = \sum_{U \in \Sigma(G)} n_{U^\perp} \frac{N_U}{\#(U)} = 0.$$

Hence,

$$\sum_{V \in \Sigma(G^\vee)} n_V N_V = 0 \iff \sum_{U \in \Sigma(G)} (G : U) n_{U^\perp} N_U = 0. \quad \square$$

In particular, the principal norm relation for G^\vee ,

$$G^\vee - \sum_{Z \in \Omega(G^\vee)} d_{G^\vee}(Z) Z,$$

leads to a norm relation for G . For its formulation we use the following notation.

18.27 Notation. For $H \in \Upsilon(G)$ put $d_G^\vee(H) = d_{G^\vee}(H^\perp) \in \mathbb{Z}$. So

$$d_G^\vee(H) = \sum_{\substack{H^* \in \Upsilon(G) \\ H^* \subseteq H}} \mu(H^{*\perp} : H^\perp) = \sum_{\substack{H^* \in \Upsilon(G) \\ H^* \subseteq H}} \mu(H : H^*).$$

18.28 Corollary.

$$\#(G) = \sum_{H \in \Upsilon(G)} (G : H) d_G^\vee(H) N_H. \quad \square$$

18.29 Example. Let p be a prime number and, as in Example 18.11, G an elementary abelian p -group of rank $r > 1$. The collection $\Upsilon_0(G)$ consists of the $\frac{p^r-1}{p-1}$ subgroups of order p^{r-1} . For each $H \in \Upsilon_0(G)$ we have $d_G^\vee(H) = 1$. The formula of Corollary 18.28 gives, after division by p :

$$p^{r-1} = \sum_{H \in \Upsilon_0(G)} N_H - \frac{p^{r-1} - 1}{p - 1} N_G.$$

For $r = 2$ the group $\text{NR}(G)$ is free of rank 1 and, indeed, this identity is essentially the same as the one in Example 18.11.

Module structures

Since the ε_H for $H \in \Upsilon(G)$ form an orthogonal system of idempotents of the group algebra $\mathbb{Z}[\frac{1}{n}][G]$ (Theorem 18.25), we obtain a decomposition for each $R[G]$ -module:

18.30 Theorem. *Let G be a finite abelian group of order n and A an $R[G]$ -module. Then*

$$A = \bigoplus_{H \in \Upsilon(G)} \varepsilon_H A \quad \text{and} \quad A^H = \bigoplus_{\substack{H^* \in \Upsilon(G) \\ H^* \supseteq H}} \varepsilon_{H^*} A$$

as R -modules.

This tells us how the R -module A is determined by its R -submodules A^H for $H \in \Upsilon(G)$:

18.31 Theorem. *Let G be a finite abelian group of order n and A an $R[G]$ -module. Then*

$$A = \varinjlim_{H \in \Upsilon(G)} A^H,$$

where the direct limit is over the groups $H \in \Upsilon(G)$ ordered by \supseteq . □

This \varinjlim is the direct limit in the categorical sense. The limit above can be constructed as the direct sum of the R -modules A^H modulo the relation which identifies the summand A^{H_2} with the R -submodule A^{H_2} of the summand A^{H_1} if $H_1 \supseteq H_2$. In terms of generators and relations it is the R -module with

generators:	$[a, H]$	with $H \in \Upsilon(G)$ and $a \in A^H$,
relations:	$[a, H_1] = [a, H_2]$	if $H_1 \supseteq H_2$ and $a \in A^{H_1}$,
	$r \cdot [a, H] = [ra, H]$	if $a \in A^H$,
	$[a_1, H] + [a_2, H] = [a_1 + a_2, H]$	if $a_1, a_2 \in A^H$.

For abelian G we have the following proposition, due to Nehr Korn [30], and rediscovered by Fröhlich [11].

Proposition. *Let G be an abelian group and A an abelian l -group with $l \nmid \#(G)$. Then $A = \sum A^H$, where H ranges over all subgroups of G such that G/H is cyclic.*

Cornell and Rosen [10] gave a simplified version of Fröhlich's proof. By Theorem 18.31 the group structure of A is determined in terms of the subgroups A^H . This is not the case for Nehr Korn's proposition. Note that in the theorem the direct limit is over $H \in \Upsilon(G)$ ordered by \supseteq , which is stronger than the direct limit over the subgroups A^H ordered by \subseteq , in which case we only have

$$A = \sum_{H \in \Upsilon(G)} A^H.$$

For A an abelian l -group this is Nehr Korn's proposition.

In particular, we have the following generalization of Proposition 12.40.

18.32 Corollary. *Let p be a prime number and G an elementary abelian p -group of rank r . Then for $\mathbb{Z}[\frac{1}{p}][G]$ -modules A we have*

$$A/A^G = \bigoplus_{\substack{H \in \Upsilon(G) \\ H \neq G}} A^H/A^G.$$

PROOF. $\Upsilon(G)$ consists of G and $\frac{p^r-1}{p-1}$ subgroups of order p^{r-1} . By Theorem 18.30

$$A = \varepsilon_G A \oplus \bigoplus_{\substack{H \in \Upsilon(G) \\ H \neq G}} \varepsilon_H A,$$

$A^G = \varepsilon_G A$ and $A^H = \varepsilon_G A \oplus \varepsilon_H A$ for each H of index p . □

For A an $R[G]$ -module each norm relation for G leads to a relation for the R -submodules A^U with $U \in \Sigma(G)$. The following lemma will be used:

18.33 Lemma. *Let G be a finite group, $H \in \Upsilon(G)$ and $\sum_{U \in \Sigma(G)} n_U U \in \text{NR}(G)$. Then for each $d \mid (G : H)$*

$$\sum_{\substack{U \in \Sigma(G) \\ (U : U \cap H) = d}} n_U \#(U) = 0.$$

In particular, for $d = 1$

$$\sum_{U \in \Sigma(H)} n_U \#(U) = 0.$$

PROOF. Let $f: G \rightarrow G/H$ be the canonical homomorphism. For each $d \mid (G : H)$ let H_d be the unique subgroup of G which contains H such that $(H_d : H) = d$. The homomorphism $\text{NR}(f)$ maps the norm relation $\sum_{U \in \Sigma(G)} n_U U$ to:

$$\sum_{d \mid (G:H)} \left(\sum_{\substack{U \in \Sigma(G) \\ (UH:H)=d}} n_U \#(U \cap H) \right) (H_d/H) \in \text{NR}(G/H).$$

The cyclic group has no nontrivial norm relations, so for each $d \mid (G : H)$ we have

$$\sum_{\substack{U \in \Sigma(G) \\ (UH:H)=d}} n_U \#(U \cap H) = 0.$$

The groups UH/H and $U/(U \cap H)$ are isomorphic, so if $(UH : H) = d$, then $(U : U \cap H) = d$ and $\#(U \cap H) = \#(U)/d$. \square

18.34 Theorem. *Let A be an R -module and $\sum_{U \in \Sigma(G)} n_U U \in \text{NR}(G)$. For each $U \in \Sigma(G)$ write $n_U = k_U - l_U$ with $k_U, l_U \in \mathbb{N}$. Then*

$$\bigoplus_{U \in \Sigma(G)} (A^U)^{k_U \#(U)} \cong \bigoplus_{U \in \Sigma(G)} (A^U)^{l_U \#(U)} \tag{18.2}$$

as R -modules.

PROOF. On both sides we have $R[G]$ -modules. They are isomorphic if they have isomorphic components in the decompositions given by the system $(\varepsilon_H)_{H \in \Upsilon(G)}$ of orthogonal idempotents of $R[G]$. For $H \in \Upsilon(G)$, $U \in \Sigma(G)$ and $\eta \in G^\vee$ such that $\langle \eta \rangle = H^\perp$ we have

$$\varepsilon_\eta \sum_{\chi \in U^\perp} \varepsilon_\chi = \sum_{\chi \in U^\perp} \varepsilon_\eta \varepsilon_\chi = \begin{cases} \varepsilon_\eta & \text{if } \eta \in U^\perp, \\ 0 & \text{otherwise} \end{cases}$$

and so

$$\varepsilon_H \frac{N_U}{\#(U)} = \sum_{\substack{\eta \in G^\vee \\ \langle \eta \rangle = H^\perp}} \varepsilon_\eta \sum_{\chi \in U^\perp} \varepsilon_\chi = \begin{cases} \varepsilon_H & \text{if } H \supseteq U, \\ 0 & \text{otherwise.} \end{cases}$$

The number of components $\varepsilon_H A$ on the left hand and the right hand sides of (18.2) is respectively

$$\sum_{U \in \Sigma(H)} k_U \#(U) \quad \text{and} \quad \sum_{U \in \Sigma(H)} l_U \#(U).$$

These numbers are equal by Lemma 18.33. \square

A sharper result is easily obtained by taking $k_U = n_U$ for $n_U \geq 0$ and $l_U = -n_U$ for $n_U < 0$. Let $d = \gcd_{U \in \Sigma(G)}(n_U \#(U))$. Then the above proof shows that

$$\bigoplus_{U \in \Sigma(G)} (A^U)^{\frac{k_U \#(U)}{d}} \cong \bigoplus_{U \in \Sigma(G)} (A^U)^{\frac{l_U \#(U)}{d}}.$$

In particular for the norm relation of Corollary 18.28:

18.35 Corollary. *Let A be an R -module and let for each $H \in \Upsilon(G)$ the numbers $k_H, l_H \in \mathbb{N}$ be such that $d_G^\vee(H) = k_H - l_H$. Then*

$$A \oplus \bigoplus_{H \in \Upsilon(G)} (A^H)^{k_H} \cong \bigoplus_{H \in \Upsilon(G)} (A^H)^{l_H}$$

as R -modules. □

18.36 Example. For G an elementary abelian p -group of rank $r \geq 1$ and A a $\mathbb{Z}[\frac{1}{p}][G]$ -module we obtain the relation for submodules described in Corollary 18.32:

$$A \oplus (A^G)^{\frac{p^r - p}{p - 1}} \cong \bigoplus_{H \in \Upsilon_0(G)} A^H.$$

18.3 Relations for Dedekind zeta functions

A norm relation of the Galois group of a Galois extension of number fields determines a relation for the zeta functions of the intermediate fields (Theorem 18.38). As a result it also determines a relation for their residues at the pole $s = 1$. This is even more interesting since the same relation holds for the discriminants (Theorem 18.45).

We will use the Euler product of the Dedekind zeta function. The relation for the zeta functions will follow from the same relation for each of the Euler factors. For this we need the splitting behavior of a prime in an intermediate field. It has been described in section 7.4. We will use the following lemma.

18.37 Lemma. *Let G be a finite group, $Z \in \Sigma(G)$, $T \in \Upsilon(Z)$ and $\sum_{U \in \Sigma(G)} n_U U \in \text{NR}(G)$. Then for each $d \mid (Z : T)$*

$$\sum_{\substack{U \in \Sigma(G) \\ (Z \cap U : T \cap U) = d}} n_U \#(Z \cap U) = 0.$$

PROOF. By Proposition 18.15

$$\sum_{U \in \Sigma(G)} n_U(Z \cap U) \in \text{NR}(Z).$$

Application of Lemma 18.33 yields the required formula. □

18.38 Theorem. *Let $L : K$ be a Galois extension of number fields, G the Galois group of $L : K$ and $\sum_{U \in \Sigma(G)} n_U U$ a norm relation for G . Then*

$$\prod_{U \in \Sigma(G)} \zeta_{L^U}(s)^{n_U \#(U)} = 1.$$

PROOF. For $U \in \Sigma(G)$ let \mathfrak{p}_U stand for maximal ideals of \mathcal{O}_{L^U} . We have the Euler product

$$\zeta_{L^U}(s) = \prod_{\mathfrak{p}_U} \frac{1}{1 - \frac{1}{N(\mathfrak{p}_U)^s}} = \prod_{\mathfrak{p}} \prod_{\mathfrak{p}_U | \mathfrak{p}} \frac{1}{1 - \frac{1}{N(\mathfrak{p}_U)^s}} = \prod_{\mathfrak{p}} \prod_{\mathfrak{p}_U | \mathfrak{p}} \frac{1}{1 - \frac{1}{N(\mathfrak{p})^{f_K(\mathfrak{p}_U)^s}}},$$

where the product is over all $\mathfrak{p} \in \text{Max}(\mathcal{O}_K)$. It suffices to show that for each \mathfrak{p}

$$\prod_{U \in \Sigma(G)} \prod_{\mathfrak{p}_U | \mathfrak{p}} \left(\frac{1}{1 - \frac{1}{N(\mathfrak{p})^{f_K(\mathfrak{p}_U)^s}} \right)^{n_U \#(U)} = 1.$$

This will be done by showing that for each given d the net number of factors with $f_K(\mathfrak{p}_U) = d$ vanishes. In other words we will prove that

$$\sum_{U \in \Sigma(G)} \sum_{\substack{\mathfrak{p}_U | \mathfrak{p} \\ f_K(\mathfrak{p}_U) = d}} n_U \#(U) = 0. \tag{18.3}$$

We use the description in section 7.4 of the splitting of a prime in a subextension of a Galois extension. Let \mathfrak{q} be a fixed maximal ideal of \mathcal{O}_L above \mathfrak{p} , $Z = Z_K(\mathfrak{q})$, $T = T_K(\mathfrak{q})$ and $f = f_K(\mathfrak{q})$. The group Z acts from the right on the collection $U \setminus G$ of left cosets of U in G . The collection of orbits of the action of Z on $U \setminus G$ is denoted by $(U \setminus G)_Z$. Thus we have a partition of G into orbits of cosets. By Theorem 7.53 and Lemma 7.52 the map

$$G \longrightarrow \text{Max}(\mathcal{O}_{L^U}), \quad \sigma \mapsto \sigma(\mathfrak{q}) \cap L^U$$

induces a bijection from the collection of orbits to the set of maximal ideals \mathfrak{p}_U above \mathfrak{p} :

$$(U \setminus G)_Z \xrightarrow{\sim} \{ \mathfrak{p}_U \in \text{Max}(\mathcal{O}_{L^U}) \mid \mathfrak{p}_U \cap K = \mathfrak{p} \}.$$

The length of an orbit is equal to

$$e_K(\sigma(\mathfrak{q}) \cap L^U) f_K(\sigma(\mathfrak{q}) \cap L^U) = (Z : (Z \cap \sigma^{-1} U \sigma)),$$

where σ is an element of one of the cosets in the orbit. Furthermore,

$$e_K(\sigma(\mathfrak{q}) \cap L^U) = (T : (T \cap \sigma^{-1}U\sigma))$$

and so

$$f_K(\sigma(\mathfrak{q}) \cap L^U) = \frac{(Z : (Z \cap \sigma^{-1}U\sigma))}{(T : (T \cap \sigma^{-1}U\sigma))} = \frac{f}{((Z \cap \sigma^{-1}U\sigma) : (T \cap \sigma^{-1}U\sigma))}.$$

In each coset $C \in U \setminus G$ choose a σ_C and for each orbit X choose a σ_X in one of its cosets. The number in equation (18.3) multiplied by $\#(Z)$ is equal to

$$\begin{aligned} & \sum_{U \in \Sigma(G)} \sum_{\substack{X \in (U \setminus G)_Z \\ ((Z \cap \sigma_X^{-1}U\sigma_X) : (T \cap \sigma_X^{-1}U\sigma_X)) = f/d}} n_U \#(U) \#(Z) \\ &= \sum_{U \in \Sigma(G)} \sum_{\substack{C \in (U \setminus G) \\ ((Z \cap \sigma_C^{-1}U\sigma_C) : (T \cap \sigma_C^{-1}U\sigma_C)) = f/d}} n_U \#(U) \#(Z \cap \sigma_C^{-1}U\sigma_C) \\ &= \sum_{U \in \Sigma(G)} \sum_{\substack{\sigma \in G \\ ((Z \cap \sigma^{-1}U\sigma) : (T \cap \sigma^{-1}U\sigma)) = f/d}} n_U \#(Z \cap \sigma^{-1}U\sigma) \\ &= \sum_{\sigma \in G} \sum_{\substack{U \in \Sigma(G) \\ ((\sigma Z \sigma^{-1} \cap U) : (\sigma T \sigma^{-1} \cap U)) = f/d}} n_U \#(\sigma Z \sigma^{-1} \cap U) \end{aligned}$$

and by Lemma 18.37 this equals 0. □

For the splitting of a prime \mathfrak{p} in L the group $T_{\mathfrak{p}}^{(L)}$ is a normal subgroup of $Z_{\mathfrak{p}}^{(L)}$ and the quotient group is cyclic. Only this has been used in the proof. No use is made of the special structure of the group $Z_{\mathfrak{p}}^{(L)}$.

For the principal norm relation of the Galois group we get ([4],[24]):

18.39 Corollary (Brauer-Kuroda). *Let $L : K$ be a Galois extension of number fields with Galois group G . Then*

$$\zeta_K(s)^{\#(G)} = \prod_{H \in \Omega(G)} \zeta_{L^H}(s)^{d_G(H) \#(H)}. \quad \square$$

In particular for a metacyclic Galois group as described in section 12.6 we get:

18.40 Corollary. *Let $L : K$ be a Galois extension with $G = \text{Gal}(L : K) \cong C_p \rtimes C_q$, where p and q are prime numbers, C the subgroup of G of order p and D one of the subgroups of order q . Then*

$$\frac{\zeta_L(s)}{\zeta_K(s)} = \frac{\zeta_{L^C}(s)}{\zeta_K(s)} \left(\frac{\zeta_{L^D}(s)}{\zeta_K(s)} \right)^q.$$

PROOF. Note that conjugate subgroups determine isomorphic subfields. The principal norm relation yields

$$\zeta_K(s)^{pq} = \zeta_L(s)^{-p} \zeta_{L^C}(s)^p \prod_{\substack{H \in \Omega(G) \\ \#(H)=q}} \zeta_{L^H}(s)^q = \zeta_L(s)^{-p} \zeta_{L^C}(s)^p \zeta_{L^D}(s)^{pq}.$$

Dedekind zeta functions have real values in real arguments. So in the field of meromorphic functions we get

$$\zeta_K(s)^p = \zeta_L(s)^{-1} \zeta_{L^C}(s) \zeta_{L^D}(s)^q. \quad \square$$

For an elementary abelian p -group of rank 2:

18.41 Corollary. *Let $L : K$ be a Galois extension with $G = \text{Gal}(L : K) \cong C_p \times C_p$, where p is a prime number. Then*

$$\frac{\zeta_L(s)}{\zeta_K(s)} = \prod_{H \in \Omega_0} \frac{\zeta_{L^H}(s)}{\zeta_K(s)}.$$

PROOF. The principal norm relation yields

$$\zeta_K(s)^{p^2} = \zeta_L(s)^{-p} \prod_{H \in \Omega_0} \zeta_{L^H}(s). \quad \square$$

For an abelian extension:

18.42 Corollary. *Let $L : K$ be an abelian extension of number fields with Galois group G . Then*

$$\zeta_L(s) = \prod_{H \in \Upsilon(G)} \zeta_{L^H}(s)^{d_G^\vee(H)}. \quad \square$$

Division by $\zeta_K(s)$ in the formulas of the Corollaries 18.39 and 18.42 yields

$$\prod_{H \in \Omega(G)} \left(\frac{\zeta_{L^H}(s)}{\zeta_K(s)} \right)^{d_G(H)\#(H)} = 1$$

and

$$\frac{\zeta_L(s)}{\zeta_K(s)} = \prod_{H \in \Upsilon(G)} \left(\frac{\zeta_{L^H}(s)}{\zeta_K(s)} \right)^{d_G^\vee(H)}.$$

The formula for the zeta functions implies a similar formula for their residues at $s = 1$:

$$\prod_{U \in \Sigma(G)} \left(\frac{2^{r(L^U)} (2\pi)^{s(L^U)} h(L^U) \text{Reg}(L^U)}{w(L^U) \sqrt{|\text{disc}(L^U)|}} \right)^{n_U \#(U)} = 1. \quad (18.4)$$

We will consider some of the factors in this formula. First the numbers of real and complex infinite primes.

18.43 Proposition. *Let $L : K$ be a Galois extension of number fields, G the Galois group of $L : K$ and $\sum_{U \in \Sigma(G)} n_U U$ a norm relation for G . For $U \leq G$ let r_U be the number of real infinite primes of L^U and s_U the number of complex infinite primes of L^U . Then*

$$\sum_{U \in \Sigma(G)} n_U \#(U) r_U = \sum_{U \in \Sigma(G)} n_U \#(U) s_U = 0.$$

PROOF. Set $[L : K] = n$. For $U \in \Sigma(G)$ put $n_U = k_U - l_U$, where $k_U, l_U \in \mathbb{N}$. The additive group of L is a $K[G]$ -module. So by Theorem 18.34

$$\bigoplus_{U \in \Sigma(G)} (L^U)^{k_U \#(U)} \cong \bigoplus_{U \in \Sigma(G)} (L^U)^{l_U \#(U)}$$

as K -vector spaces. Taking dimensions over K yields:

$$\sum_{U \in \Sigma(G)} k_U \#(U) (r_U + 2s_U) = \sum_{U \in \Sigma(G)} l_U \#(U) (r_U + 2s_U)$$

and so

$$\sum_{U \in \Sigma(G)} n_U \#(U) (r_U + 2s_U) = 0.$$

Similarly for the $\mathbb{R}[G]$ -module with the set $\mathcal{P}_0(L)$ of finite primes of L as an \mathbb{R} -basis (the ‘logarithmic space’ of L):

$$\sum_{U \in \Sigma(G)} n_U \#(U) (r_U + s_U) = 0. \quad \square$$

Next the discriminants $\text{disc}(L^U)$ in formula (18.4). For this we will use the following relation for the differentials over the intermediate fields:

18.44 Proposition. *Let $L : K$ be a Galois extension of number fields, G the Galois group of $L : K$ and $\sum_{U \in \Sigma(G)} n_U U$ a norm relation for G . Then*

$$\prod_{U \in \Sigma(G)} \partial_{L^U}(L)^{n_U} = \mathcal{O}_L.$$

PROOF. Let $\mathfrak{q} \in \text{Max}(\mathcal{O}_L)$. We will prove that

$$v_{\mathfrak{q}} \left(\prod_{U \in \Sigma(G)} \partial_{L^U}(L)^{n_U} \right) = 0.$$

Let $N \in \mathbb{N}$ be large enough such that $V_{K,i}(\mathfrak{q}) = \{1\}$. Use Corollary 17.35 and Proposition 7.5:

$$v_{\mathfrak{q}} \left(\prod_{U \in \Sigma(G)} \partial_{L^U}(L)^{n_U} \right) = \sum_{U \in \Sigma(G)} (\#(\partial_{L^U}(L))) n_U$$

$$\begin{aligned}
 &= \sum_{U \in \Sigma(G)} \sum_{i=0}^{\infty} \left(\#(V_{L^U, i}(\mathfrak{q})) - 1 \right) n_U \\
 &= \sum_{U \in \Sigma(G)} \sum_{i=0}^{\infty} \left(\#(V_{K, i}(\mathfrak{q}) \cap U) - 1 \right) n_U \\
 &= \sum_{i=0}^N \sum_{U \in \Sigma(G)} \left(\#(V_{K, i}(\mathfrak{q}) \cap U) - 1 \right) n_U \\
 &= \sum_{i=0}^N \sum_{U \in \Sigma(G)} \left(\#(V_{K, i}(\mathfrak{q}) \cap U) \right) n_U - (N+1) \sum_{U \in \Sigma(G)} n_U = 0. \quad \square
 \end{aligned}$$

18.45 Theorem. *Let $L : K$ be a Galois extension of number fields, G the Galois group of $L : K$ and $\sum_{U \in \Sigma(G)} n_U U$ a norm relation for G . Then*

$$\prod_{U \in \Sigma(G)} \mathfrak{d}_K(L^U)^{n_U \#(U)} = \mathcal{O}_K.$$

PROOF. Using Theorem 17.23, Theorem 17.28, Proposition 18.16 and Proposition 18.44:

$$\begin{aligned}
 \prod_{U \in \Sigma(G)} \mathfrak{d}_K(L^U)^{n_U \#(U)} &= \prod_{U \in \Sigma(G)} \mathfrak{d}_K(L)^{n_U} N_K^{L^U}(L)^{-n_U} \\
 &= \mathfrak{d}_K(L)^{\sum_{U \in \Sigma(G)} n_U} \prod_{U \in \Sigma(G)} N_N^{L^U}(N_{L^U}^L(\partial_{L^U}(L)))^{-n_U} \\
 &= \prod_{U \in \Sigma(G)} N_K^L(\partial_{L^U}(L))^{-n_U} = N_K^L \left(\prod_{U \in \Sigma(G)} \partial_{L^U}(L)^{-n_U} \right) \\
 &= N_K^L(\mathcal{O}_L)^{-1} = \mathcal{O}_K. \quad \square
 \end{aligned}$$

For the absolute discriminants this implies:

18.46 Theorem. *Let $L : K$ be a Galois extension of number fields, G the Galois group of $L : K$ and $\sum_{U \in \Sigma(G)} n_U U$ a norm relation for G . Then*

$$\prod_{U \in \Sigma(G)} |\text{disc}(L^U)|^{n_U \#(U)} = 1.$$

PROOF. By Theorem 17.28

$$\mathfrak{d}_{\mathbb{Q}}(L) = \mathfrak{d}_{\mathbb{Q}}(K)^{\#(G)} \cdot N_{\mathbb{Q}}^K(\mathfrak{d}_K(L))$$

and so for the generators in \mathbb{N}^* of these ideals of \mathbb{Z} :

$$|\text{disc}(L)| = |\text{disc}(K)|^{\#(G)} \cdot N(\mathfrak{d}_K(L)).$$

Also for each subgroup U of G :

$$|\text{disc}(L^U)| = |\text{disc}(K)|^{(G:U)} \cdot N(\mathfrak{d}_K(L^U)).$$

Apply Theorem 18.45 and Proposition 18.16:

$$\begin{aligned} & \prod_{U \in \Sigma(G)} |\text{disc}(L^U)|^{n_U \#(U)} \\ &= \prod_{U \in \Sigma(G)} |\text{disc}(K)|^{(G:U)n_U \#(U)} \cdot \prod_{U \in \Sigma(G)} N(\mathfrak{d}_K(L^U))^{n_U \#(U)} \\ &= |\text{disc}(K)|^{\#(G) \sum_{U \in \Sigma(G)} n_U} \cdot N\left(\prod_{U \in \Sigma(G)} \mathfrak{d}_K(L^U)^{n_U \#(U)}\right) = 1. \quad \square \end{aligned}$$

Combining equation (18.4), Theorem 18.46 and Proposition 18.43:

18.47 Theorem. *Let $L : K$ be a Galois extension of number fields, G the Galois group of $L : K$ and $\sum_{U \in \Sigma(G)} n_U U$ a norm relation for G . Then*

$$\prod_{U \in \Sigma(G)} \left(\frac{h(L^U) \text{Reg}(L^U)}{w(L^U)} \right)^{n_U \#(U)} = 1. \quad \square$$

From the functional equation for the Dedekind zeta function follows that

$$\lim_{s \rightarrow 0} \zeta_K(s) s^{1-r(K)-s(K)} = -\frac{h(K) \text{Reg}(K)}{w(K)}.$$

This also leads to Theorem 18.47, see [8] Theorem 4.9.12.

For the principal norm relation of the Galois group we get:

18.48 Corollary. *Let $L : K$ be a Galois extension of number fields with Galois group G . Then*

$$\left(\frac{h(K) \text{Reg}(K)}{w(K)} \right)^{\#(G)} = \prod_{H \in \Omega(G)} \left(\frac{h(L^H) \text{Reg}(L^H)}{w(L^H)} \right)^{d_G(H) \#(H)}. \quad \square$$

For an abelian extension:

18.49 Corollary. *Let $L : K$ be a abelian extension of number fields with Galois group G . Then*

$$\frac{h(L) \text{Reg}(L)}{w(L)} = \prod_{H \in \Upsilon(G)} \left(\frac{h(L^H) \text{Reg}(L^H)}{w(L^H)} \right)^{d_G^\vee(H)}. \quad \square$$

In particular for an elementary abelian p -group:

18.50 Proposition. *Let $L : K$ an abelian extension of number fields with $G = \text{Gal}(L : K)$ an elementary abelian p -group of rank r . Then*

$$\frac{h(L) \text{Reg}(L)}{w(L)} \cdot \left(\frac{h(K) \text{Reg}(K)}{w(K)} \right)^{\frac{p^r - p}{p-1}} = \prod_{H \in \mathcal{Y}_0(G)} \frac{h(L^H) \text{Reg}(L^H)}{w(L^H)}. \quad \square$$

18.51 Example. For a biquadratic extension $L : K$ of number fields with L_1, L_2 and L_3 the three intermediate fields of degree 2 over K the formula becomes

$$\frac{h(L) \text{Reg}(L)}{w(L)} \cdot \left(\frac{h(K) \text{Reg}(K)}{w(K)} \right)^2 = \prod_{i=1}^3 \frac{h(L_i) \text{Reg}(L_i)}{w(L_i)}.$$

For a biquadratic number field we retrieve the formulas of Example 9.57 (the real case) and Example 9.58 (the complex case). In chapter 9 these formulas have been derived using L -functions of Dirichlet characters. The formula for the discriminants was verified by direct computation (Exercise 9 of chapter 1). Here the formula is obtained as an application of Theorem 18.38 and Theorem 18.46.

For $L : K$ abelian proofs of Theorem 18.38 and Theorem 18.46 can be given using (generalized) Dirichlet characters. However, such proofs are based on detailed knowledge of the ramification of primes in an abelian extension: Theorem 15.52 and Theorem 17.51.

By Corollary 18.40 we have for Galois groups isomorphic to $C_p \times C_q$:

18.52 Proposition. *Let $L : K$ be a Galois extension with $G = \text{Gal}(L : K) \cong C_p \times C_q$, where p and q are prime numbers, C the subgroup of G of order p and D one of the subgroups of order q . Then*

$$h(L) \text{Reg}(L) (h(K) \text{Reg}(K))^q = h(L^C) \text{Reg}(L^C) (h(L^D) \text{Reg}(L^D))^q.$$

PROOF. Note that $\mu(L) = \mu(L^C)$ and $\mu(L^D) = \mu(K)$. Use that conjugate fields are isomorphic. \square

18.53 Example. Let K be a cubic number field with one real prime and let d be its discriminant. Then $d < 0$ and the normal closure of K is the field $L = K(\sqrt{d})$. We have $\text{Gal}(L : \mathbb{Q}) \cong S_3$ and $\text{Gal}(L : \mathbb{Q}) = \langle \sigma, \tau \rangle$, where σ and τ generate respectively $\text{Gal}(L : \mathbb{Q}(\sqrt{d}))$ and $\text{Gal}(L : K)$. Since $h(\mathbb{Q}) = \text{Reg}(\mathbb{Q}) = \text{Reg}(\mathbb{Q}(\sqrt{d})) = 1$, we have by Proposition 18.52:

$$h(L) \text{Reg}(L) = h(\mathbb{Q}(\sqrt{d})) h(K)^2 \text{Reg}(K)^2.$$

Let ε be the fundamental unit of K . Then $\text{Reg}(K) = \log \varepsilon$ and $\langle \varepsilon, \sigma(\varepsilon) \rangle$ is of finite index in \mathcal{O}_L^* and so

$$\text{Reg}(L) = (\mathcal{O}_L^* : \langle \varepsilon, \sigma(\varepsilon) \rangle) \cdot \text{Reg}(\varepsilon, \sigma(\varepsilon)).$$

Since $|\sigma(\varepsilon)| = |\sigma^2(\varepsilon)|$ and $\varepsilon\sigma(\varepsilon)\sigma^2(\varepsilon) = 1$, we have $\log \varepsilon = -2\log(\sigma(\varepsilon))$ and so $\text{Reg}(\varepsilon, \sigma(\varepsilon))$ is the absolute value of

$$\begin{vmatrix} 2 \log \varepsilon & 2 \log |\sigma(\varepsilon)| \\ 2 \log |\sigma(\varepsilon)| & 2 \log |\sigma^2(\varepsilon)| \end{vmatrix} = \begin{vmatrix} 2 \log \varepsilon & -\log \varepsilon \\ -\log \varepsilon & -\log \varepsilon \end{vmatrix} = -3 \log^2 \varepsilon.$$

It follows that

$$(\mathcal{O}_L^* : \langle \varepsilon, \sigma(\varepsilon), -1 \rangle) \cdot \text{Reg}(L) = 3 \log^2 \varepsilon = 3 \cdot \text{Reg}(K)^2$$

and so

$$3 \cdot h(L) = h(\mathbb{Q}(\sqrt{d})) \cdot h(K)^2 \cdot (\mathcal{O}_L^* : \langle \varepsilon, \sigma(\varepsilon), -1 \rangle). \quad (18.5)$$

For $L = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ we have $K = \mathbb{Q}(\sqrt[3]{2})$ and $d = -3$. In Example 5.18 and Example 5.42 the groups $\mathcal{C}(K)$ and \mathcal{O}_K^* have been computed. Example 7.17 contains computations of \mathcal{O}_L and \mathcal{O}_L^* . We have $h(K) = h(L) = 1$ and indeed $(\mathcal{O}_L^* : \langle \varepsilon, \sigma(\varepsilon), -1 \rangle) = 3$ as shown by direct computation in Example 7.17.

Finally for $G \cong A_4$ using the norm relation described in Example 18.13 we get :

18.54 Proposition. *Let $L : K$ be a Galois extension of number fields with Galois group isomorphic to A_4 . Then*

$$\frac{\zeta_L(s)}{\zeta_K(s)} = \frac{\zeta_{LV}(s)}{\zeta_K(s)} \left(\frac{\zeta_{LC}(s)}{\zeta_K(s)} \right)^3,$$

where V is the noncyclic group of order 4 and C is one of the subgroups of order 3. □

18.4 Some remarks on Artin L-functions

A powerful tool in class field theory is the L -series of a Dirichlet character. Artin introduced a generalization: an L -function determined by a representation of the Galois group of a Galois extension of number fields. In particular the main theorem of this section, Theorem 18.38, is easily proved using Artin L -functions. For $L : K$ an abelian extension of number fields a Dirichlet character $\chi \in \mathcal{H}(L : K)$ corresponds to a character of the group $\text{Gal}(L : K)$, i.e. a group homomorphism

$$\text{Gal}(L : K) \longrightarrow \mathbb{C}^*.$$

The L -series of a Dirichlet character is defined as a Dirichlet series and since a Dirichlet character is multiplicative it is also representable by an infinite product, the Euler product.

The Artin L -function is defined as an infinite product (Definition 18.56) and it is unknown whether it is in all cases the Euler product of a Dirichlet series.

Let $L : K$ be a Galois extension of number fields, $G = \text{Gal}(L : K)$, V a finite dimensional \mathbb{C} -vector space and $\rho : G \rightarrow \text{Aut}_{\mathbb{C}}(V)$ a representation of G . Thus V is a $\mathbb{C}[G]$ -module of finite complex dimension.

A representation ρ determines a map

$$\chi : G \rightarrow \mathbb{C}, \quad \sigma \mapsto \text{Tr}(\rho(\sigma)),$$

which is called the *character* of the representation ρ . It generalizes the notion of character in the degree 1 case. A basic result in the theory of group representations is that the character determines the representation up to isomorphism. Characters of G are *central functions* on G , meaning that

$$\chi(\tau\sigma\tau^{-1}) = \chi(\sigma) \quad \text{for all } \sigma, \tau \in G.$$

Central functions of G are functions on G which are constant on conjugacy classes.

The character of the trivial representation $G \rightarrow \mathbb{C}^*$, $\sigma \mapsto 1$ is called the *principal or trivial character* of G . Notation for the trivial character: $\mathbf{1}_G$ or simply $\mathbf{1}$. The corresponding $\mathbb{C}[G]$ -module is \mathbb{C} with the trivial action of G . The representation corresponding to the group algebra $\mathbb{C}[G]$ maps a group element σ to the automorphism of $\mathbb{C}[G]$ induced by the permutation $\tau \mapsto \sigma\tau$ of G . It is called the *regular representation* of G . The character of the regular representation of G is denoted by r_G . Clearly,

$$r_G(\sigma) = \begin{cases} \#(G) & \text{if } \sigma = 1, \\ 0 & \text{otherwise.} \end{cases}$$

A representation $\rho : G \rightarrow \text{Aut}_{\mathbb{C}}(V)$ is called *irreducible* if the G -module V has no nontrivial proper G -submodule. Accordingly, the G -module V is called irreducible. Irreducible representations of abelian groups G are representations of degree 1. The character of an irreducible representation is called an *irreducible character*. The irreducible characters of G form a basis of the \mathbb{C} -vector space of central functions on G . Every G -module is a direct sum of irreducible \mathbb{C} -modules and so the characters of representations of G are combinations of irreducible characters with the coefficients in \mathbb{N} . Every irreducible G -module is a G -submodule of the regular G -module $\mathbb{C}[G]$:

$$r_G = \sum_{\chi} \chi(1)\chi, \tag{18.6}$$

where the sum is over all irreducible characters of G .

18.55 Notation. Let V be a finite dimensional complex vector space and $\rho: G \rightarrow \text{Aut}_{\mathbb{C}}(V)$ a representation over \mathbb{C} of a finite group G . For $x \in \mathbb{C}[G]$ we put

$$\det_V(x) = \det(\rho(x)).$$

So \det_V is the composition $\mathbb{C}[G] \xrightarrow{\rho} \text{End}_{\mathbb{C}}(V) \xrightarrow{\det} \mathbb{C}$.

18.56 Definition. Let $L: K$ be a Galois extension of number fields and $\rho: \text{Gal}(L: K) \rightarrow \text{Aut}_{\mathbb{C}}(V)$ a representation of $\text{Gal}(L: K)$ with character χ . Then the *Artin L -function* attached to ρ is

$$\mathcal{L}(s, \chi, L: K) = \prod_{\mathfrak{p} \in \text{Max}(\mathcal{O}_K)} \frac{1}{\det_{V^{T_{\mathfrak{p}}}} \left(1 - \frac{\varphi_{\mathfrak{p}}}{N(\mathfrak{p})^s}\right)},$$

where $T_{\mathfrak{p}} = T_K(\mathfrak{q})$ for some $\mathfrak{q} \in \text{Max}(\mathcal{O}_L)$ above \mathfrak{p} and $\varphi_{\mathfrak{p}} \in Z_K(\mathfrak{q})$ restricted to $L^{T_{\mathfrak{p}}}$ is the Frobenius of $\mathfrak{q}^{T_{\mathfrak{p}}}$ over K . The infinite product converges absolutely for $\Re(s) > 1$ as will be shown below.

The definition is independent of the choice of $\varphi_{\mathfrak{p}}$, since $T_{\mathfrak{p}}$ acts trivially on $V^{T_{\mathfrak{p}}}$. Note also that $\det_{V^{T_{\mathfrak{p}}}} \left(1 - \frac{\varphi_{\mathfrak{p}}}{N(\mathfrak{p})^s}\right)$ does not depend on the choice of \mathfrak{q} : for any $\sigma \in \text{Gal}(L: K)$ we have $T_K(\sigma(\mathfrak{q})) = \sigma T_{\mathfrak{p}} \sigma^{-1}$, $\sigma \varphi_{\mathfrak{p}} \sigma^{-1}|_{L^{\sigma T_{\mathfrak{p}} \sigma^{-1}}} = \varphi_K(\sigma(\mathfrak{q})^{T_K(\sigma(\mathfrak{q}))})$ and the action of $1 - \frac{\sigma \varphi_{\mathfrak{p}} \sigma^{-1}}{N(\mathfrak{p})^s}$ on $V^{\sigma T_{\mathfrak{p}} \sigma^{-1}}$ has the same determinant as the action of $1 - \frac{\varphi_{\mathfrak{p}}}{N(\mathfrak{p})^s}$ on $V^{T_{\mathfrak{p}}}$.

Let $t > 1$. Since $\varphi_{\mathfrak{p}} \in \text{Gal}(L: K)$ acts on $V^{T_{\mathfrak{p}}}$ as an automorphism of finite order, the eigenvalues ε_i of this automorphism are roots of unity. Let n the dimension of V . Then for $\Re(s) \geq t$

$$\left| \det_{V^{T_{\mathfrak{p}}}} \left(1 - \frac{\varphi_{\mathfrak{p}}}{N(\mathfrak{p})^s}\right) \right|^{-1} = \prod_i \left| 1 - \frac{\varepsilon_i}{N(\mathfrak{p})^s} \right|^{-1} \leq \left(1 + \frac{2}{N(\mathfrak{p})^t}\right)^n.$$

The infinite product $\prod_{\mathfrak{p}} \left(1 + \frac{2}{N(\mathfrak{p})^t}\right)$ converges absolutely for $\Re(s) \geq t$, because so does the infinite sum $\sum_{\mathfrak{p}} \frac{2}{N(\mathfrak{p})^t}$. It follows that the infinite product in the definition converges absolutely in the half-plane $\Re(s) > 1$.

Dirichlet L -functions are Artin L -functions:

18.57 Proposition. Let $L: K$ be an abelian extension of number fields and $\chi \in \mathcal{H}(L: K)$. Then $\mathcal{L}(s, \chi, L: K) = L(s, \chi)$. In particular for the trivial character we have $\mathcal{L}(s, \mathbf{1}, L: K) = \zeta_K(s)$.

PROOF. The character $\chi \in \mathcal{H}(L: K)$ corresponds in a natural way to a character $\chi: \text{Gal}(L: K) \rightarrow \mathbb{C}^*$, a representation of degree 1. For each $\mathfrak{p} \in \text{Max}(\mathcal{O}_K)$ we have $\det_{\mathbb{C}} \left(1 - \frac{\varphi_{\mathfrak{p}}}{N(\mathfrak{p})^s}\right) = 1 - \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s}$. \square

The sum of characters is the character of the direct sum of the representations:

18.58 Proposition. *Let $L : K$ be a Galois extension of number fields and χ and χ' characters of $\text{Gal}(L : K)$. Then*

$$\mathcal{L}(s, \chi + \chi', L : K) = \mathcal{L}(s, \chi, L : K) \mathcal{L}(s, \chi', L : K).$$

PROOF. Let $\rho : \text{Gal}(L : K) \rightarrow \text{Aut}_{\mathbb{C}}(V)$ and $\rho' : \text{Gal}(L : K) \rightarrow \text{Aut}_{\mathbb{C}}(V')$ be representations with characters χ and χ' respectively. Then $\rho \oplus \rho' : \text{Gal}(L : K) \rightarrow \text{Aut}_{\mathbb{C}}(V \oplus V')$ is a representation with character $\chi + \chi'$, and for each $\mathfrak{p} \in \text{Max}(\mathcal{O}_K)$

$$\det_{(V \oplus V')^{T_{\mathfrak{p}}}} \left(1 - \frac{\varphi_{\mathfrak{p}}}{N(\mathfrak{p})^s} \right) = \det_{V^{T_{\mathfrak{p}}}} \left(1 - \frac{\varphi_{\mathfrak{p}}}{N(\mathfrak{p})^s} \right) \cdot \det_{V'^{T_{\mathfrak{p}}}} \left(1 - \frac{\varphi_{\mathfrak{p}}}{N(\mathfrak{p})^s} \right). \quad \square$$

Extending Galois extensions to larger Galois extensions has no effect on the Artin L -function:

18.59 Proposition. *Let $L : K$ be a Galois extension of number fields and L' an intermediate field such that also $L' : K$ is a Galois extension. Let χ' be a character of $\text{Gal}(L' : K)$ and χ the composition $\text{Gal}(L : K) \rightarrow \text{Gal}(L' : K) \xrightarrow{\chi'} \mathbb{C}$. Then*

$$\mathcal{L}(s, \chi, L : K) = \mathcal{L}(s, \chi', L' : K).$$

PROOF. Let $\rho : \text{Gal}(L' : K) \rightarrow \text{Aut}_{\mathbb{C}}(V)$ be a representation with character χ' . Then χ is the character of the representation $\text{Gal}(L : K) \rightarrow \text{Gal}(L' : K) \xrightarrow{\rho} \text{Aut}_{\mathbb{C}}(V)$. Let $\mathfrak{q} \in \text{Max}(\mathcal{O}_{L'})$ above \mathfrak{p} . Put $T_{\mathfrak{p}} = T_K(\mathfrak{q})$ and $T'_{\mathfrak{p}} = T_{L'}(\mathfrak{q} \cap L')$. The Frobenius of \mathfrak{p} in $(L')^{T'_{\mathfrak{p}}}$ is the restriction of the Frobenius of \mathfrak{p} in $L^{T_{\mathfrak{p}}}$. So the action of $\varphi_K(\mathfrak{q}^{T_{\mathfrak{p}}})$ coincides with the action of $\varphi_{L'}(\mathfrak{q} \cap L')^{T'_{\mathfrak{p}}}$ on $V^{T_{\mathfrak{p}}} = V^{T'_{\mathfrak{p}}}$. \square

Proposition 18.57 follows from this proposition. It is the special case $L' = K$:

$$\mathcal{L}(s, 1, L : K) = \mathcal{L}(s, 1, K : K) = \zeta_K(s).$$

For $L : K$ a Galois extension of number fields and K' an intermediate field, the Artin L -function attached to a representation of $\text{Gal}(L : K')$ is equal to the an Artin L -function attached to the induced representation of $\text{Gal}(L : K)$. This will be proved below. It is Theorem 18.61. In its proof two lemmas concerning representations will be used. First some generalities on induced representations are described.

18.60 Induced representations and induced characters. Let H be a subgroup of a finite group G and $\rho : H \rightarrow \text{Aut}_{\mathbb{C}}(W)$ a representation of H in the group of automorphisms of a finite dimensional \mathbb{C} vector space W with character χ . The $\mathbb{C}[H]$ -module W determines a $\mathbb{C}[G]$ -module V via extension of scalars:

$$V = \mathbb{C}[G] \otimes_{\mathbb{C}[H]} W.$$

The corresponding presentation $\rho_*: G \rightarrow \text{Aut}_{\mathbb{C}}(V)$ is called the by ρ induced representation of G . It is customary to identify W and $1 \otimes W \subseteq V$ via $x \mapsto 1 \otimes x$. Thus W is an H -submodule of V and for a system $\sigma_1, \dots, \sigma_r$ of representatives of G/H (the set of left cosets of H in G) one has

$$V = \sigma_1 W \oplus \dots \oplus \sigma_r W,$$

a direct sum of H -submodules. The character χ_* of V is called the by χ induced character of G . It is given by

$$\chi_*(\sigma) = \frac{1}{\#(H)} \sum_{\substack{\tau \in G \\ \tau^{-1}\sigma\tau \in H}} \chi(\tau^{-1}\sigma\tau) \quad \text{for all } \sigma \in G,$$

see section 7.2 of [34].

The following theorem is the main theorem on Artin L -functions.

18.61 Theorem. *Let $L : K$ be a Galois extension of number fields, K' an intermediate field of $L : K$ and χ a character of $\text{Gal}(L : K')$. Then for χ_* , the character of $\text{Gal}(L : K)$ induced by χ , we have*

$$\mathcal{L}(s, \chi_*, L : K) = \mathcal{L}(s, \chi, L : K').$$

PROOF. The proof is a bit technical, though not really difficult. Here too Theorem 7.53 is used. Well-written proofs are in e.g. [12] and [31]. \square

The Artin L -function of the regular character is the Dedekind zeta function of the extension field:

18.62 Corollary. *Let $L : K$ be a Galois extension of number fields with Galois group G . Then*

$$\mathcal{L}(s, n_G, L : K) = \zeta_L(s).$$

PROOF. The character $\mathbf{1}_*$ induced by the trivial character $\mathbf{1}$ of the subgroup $\{1\}$ of G is the regular character of G . So

$$\mathcal{L}(s, \mathbf{1}_*, L : K) = \mathcal{L}(s, \mathbf{1}, L : L) = \zeta_L(s). \quad \square$$

By equation (18.6)

$$\mathcal{L}(s, n_G, L : K) = \prod_{\chi} \mathcal{L}(s, \chi, L : K)^{\chi(1)}$$

and so:

18.63 Corollary. *Let $L : K$ be a Galois extension of number fields. Then*

$$\zeta_L(s) = \zeta_K(s) \prod_{\chi \neq 1} \mathcal{L}(s, \chi, L : K)^{\chi(1)},$$

where the product is over all irreducible characters of $\text{Gal}(L : K)$. □

This generalizes the formula for L -functions of an abelian number field extension.

The character of a finite group G induced by the trivial character of a subgroup U of G is denoted by χ_U . A norm relation of a finite group leads to a relation between these induced characters.

18.64 Theorem. *Let $\sum_{U \in \Sigma(G)} n_U U$ be a norm relation of G . Then*

$$\sum_{U \in \Sigma(G)} n_U \#(U) \chi_U = 0.$$

PROOF. The induced characters χ_U are given by

$$\chi_U(\sigma) = \frac{1}{\#(U)} \sum_{\substack{\tau \in G \\ \tau^{-1} \sigma \tau \in U}} 1 \quad \text{for all } \sigma \in G.$$

So for each $\sigma \in G$ we have by Lemma 18.37 (with $Z = \langle \tau^{-1} \sigma \tau \rangle$, $T = \{1\}$ and $d = o(\sigma)$):

$$\sum_{U \in \Sigma(G)} n_U \#(U) \chi_U = \sum_{U \in \Sigma(G)} \sum_{\substack{\tau \in G \\ \tau^{-1} \sigma \tau \in U}} n_U = \sum_{\tau \in G} \sum_{\substack{U \in \Sigma(G) \\ U \supseteq \langle \tau^{-1} \sigma \tau \rangle}} n_U = 0. \quad \square$$

A relation between characters induced by trivial characters leads to a relation between Dedekind zeta functions: for U a subgroup of G we have by Theorem 18.61 $\mathcal{L}(s, \chi_U, L : K) = \mathcal{L}(s, \mathbf{1}_H, L : L^U) = \zeta_{L^U}(s)$ and by Theorem 18.64 and the Propositions 18.57 and 18.58

$$\prod_{U \in \Sigma(G)} \zeta_{L^U}(s)^{n_U \#(U)} = 1.$$

This again proves Theorem 18.38.

18.5 Strongly exceptional groups

If the trivial norm coefficient $d_G(\{1\})$ of the Galois group G of a nontrivial Galois extension $L : K$ of number fields is nonzero, then by Corollary 18.39 the Dedekind

zeta function of L is determined by the Dedekind zeta functions of intermediate fields $\neq L$ of the extension. Clearly, this holds as well for each nontrivial subgroup of G .

18.65 Definitions. Let G be a nontrivial finite group. Then G is called *exceptional* if $d_G(\{1\}) = 0$. It is called *strongly exceptional* if all nontrivial subgroups are exceptional.

18.66 Lemma. Let G be a finite group of order $n > 1$. Then the following holds.

- a) $d_G(\{1\}) = \sum_{d|n} \mu(d)e_G(d)$, where $e_G(d)$ is the number of cyclic subgroups of order d .
- b) If $G = G_1 \times G_2$ with $\#(G_1)$ and $\#(G_2)$ relatively prime, then $d_G(\{1\}) = d_{G_1}(\{1\}) \cdot d_{G_2}(\{1\})$.

PROOF.

$$\text{a) } d_G(\{1\}) = \sum_{H \in \Omega(G)} \mu(\#(H)) = \sum_{d|n} \sum_{\substack{H \in \Omega(G) \\ \#(H)=d}} \mu(d) = \sum_{d|n} \mu(d)e_G(d).$$

- b) Put $\#(G_1) = n_1$ and $\#(G_2) = n_2$. Because $\gcd(n_1, n_2) = 1$, we have a bijection

$$\Omega(G) \xrightarrow{\sim} \Omega(G_1) \times \Omega(G_2), \quad H_1 \times H_2 \mapsto (H_1, H_2)$$

and so

$$\begin{aligned} d_G(\{1\}) &= \sum_{H \in \Omega(G)} \mu(\#(H)) = \sum_{H_1 \times H_2 \in \Omega(G)} \mu(\#(H_1 \times H_2)) \\ &= \sum_{\substack{H_1 \in \Omega(G_1) \\ H_2 \in \Omega(G_2)}} \mu(\#(H_1))\mu(\#(H_2)) \\ &= \sum_{H_1 \in \Omega(G_1)} \mu(\#(H_1)) \cdot \sum_{H_2 \in \Omega(G_2)} \mu(\#(H_2)) = d_{G_1}(\{1\}) \cdot d_{G_2}(\{1\}). \quad \square \end{aligned}$$

This lemma implies:

18.67 Proposition. Let G_1 and G_2 be nontrivial finite groups with $\#(G_1)$ and $\#(G_2)$ relatively prime. Then $G_1 \times G_2$ is nonexceptional if and only if G_1 and G_2 both are nonexceptional. \square

18.68 Proposition. Let p be a prime number and G a nontrivial p -group. Then G is exceptional if and only if G has a unique subgroup of order p . If G is exceptional, it is strongly exceptional.

PROOF. Let m be the number of subgroups of order p . Then by Lemma 18.66a) the trivial norm coefficient $d_G(\{1\})$ of G is equal to $1 - m$. So G is exceptional if and only if $m = 1$. If G has a unique subgroup of order p , then so has each nontrivial subgroup of G . \square

For p an odd prime p -groups have a unique subgroup of order p if and only if they are cyclic. For 2-groups it is a bit more complicated: a 2-group has a unique subgroup of order 2 if and only if the group is either cyclic or (generalized) quaternion, see below for the definition of quaternion groups. Proofs are in many books on group theory, e.g. [15] Theorem 12.5.2 or [6] Theorem (4.3).

18.69 Definition. Let $n \geq 3$. A generalized quaternion group of order 2^n is generated by two elements, an element σ of order 2^{n-1} and an element τ of order 2, such that

$$\sigma^{2^{n-2}} = \tau^2 \quad \text{and} \quad \tau\sigma = \sigma^{-1}\tau.$$

For $n = 3$ the group is the well known quaternion group of order 8. Generalized quaternion groups are often called just quaternion groups for short.

We will show that in some cases the existence of a collection of exceptional subgroups implies that the group itself is exceptional.

18.70 Definition. Let G be a finite group and let $\{G_i\}$ be a collection of subgroups of G indexed by a finite set I . For $J \subseteq I$ we write

$$G_J = \bigcap_{j \in J} G_j,$$

where it is understood that $G_\emptyset = G$. The collection $\{G_j\}$ is called *exceptional* if

- a) $G = \bigcup_{i \in I} G_i$,
- b) G_J is exceptional for all $J \neq \emptyset$.

18.71 Theorem. Let $\{G_i\}$ be an exceptional collection of subgroups of a finite group G . Then G is exceptional.

PROOF. For $i \in I$ and $J \subseteq I$ we write Ω_i for $\Omega(G_i)$ and Ω_J for $\Omega(G_J)$. From condition a) it follows that

$$\Omega(G) = \bigcup_{i \in I} \Omega_i.$$

For $S \subseteq \Omega(G)$ the characteristic function on $\Omega(G)$ corresponding to S is denoted by χ_S . We have

$$\begin{aligned} 0 &= \chi_{\Omega \setminus \bigcup \Omega_i} = \chi_{\bigcap (\Omega \setminus \Omega_i)} = \prod_i \chi_{\Omega \setminus \Omega_i} = \prod_i (1 - \chi_{\Omega_i}) = \sum_{J \subseteq I} (-1)^{\#J} \prod_{j \in J} \chi_{\Omega_j} \\ &= \sum_{J \subseteq I} (-1)^{\#J} \chi_{\Omega_J} \end{aligned}$$

and so

$$1 = - \sum_{\substack{J \subseteq I \\ J \neq \emptyset}} (-1)^{\#J} \chi_{\Omega_J},$$

that is for each $H \in \Omega$

$$1 = - \sum_{\substack{J \subseteq I \\ J \neq \emptyset}} (-1)^{\#J} \chi_{\Omega_J}(H).$$

Multiply by $\mu(\#H)$:

$$\mu(\#H) = - \sum_{\substack{J \subseteq I \\ J \neq \emptyset}} (-1)^{\#J} \chi_{\Omega_J}(H) \mu(\#H).$$

Summation over all $H \in \Omega$ yields

$$\begin{aligned} d_G(\{1\}) &= - \sum_{\substack{J \subseteq I \\ J \neq \emptyset}} (-1)^{\#J} \sum_{H \in \Omega} \chi_{\Omega_J}(H) \mu(\#H) = - \sum_{\substack{J \subseteq I \\ J \neq \emptyset}} (-1)^{\#J} \sum_{H \in \Omega_J} \mu(\#H) \\ &= - \sum_{\substack{J \subseteq I \\ J \neq \emptyset}} (-1)^{\#J} d_{G_J}(\{1\}) = 0. \end{aligned} \quad \square$$

18.72 Notation. By $D(G)$ we denote the intersection of all maximal cyclic subgroups of a finite group G . The collection of all maximal cyclic subgroups is exceptional if $D(G)$ is nontrivial: the intersections of such subgroups are cyclic and nontrivial since they contain $D(G)$. On the other hand, every element of G is contained in some maximal cyclic subgroup.

18.73 Corollary. *A finite group G is exceptional if $D(G)$ is nontrivial.* □

18.74 Lemma. *The subgroup $D(G)$ of a finite group G is contained in the center of G .*

PROOF. Let $h \in D(G)$ and $g \in G$. Choose a maximal cyclic subgroup M of G such that $g \in M$. Since h and g both are elements of the cyclic group M , they commute. □

18.75 Proposition. *Let G be a finite group, p a prime number and $g \in G$ of order p . Then $g \in D(G)$ if and only if $\langle g \rangle$ is the only subgroup of G of order p and g is in the center of G .*

PROOF. Suppose $g \in D(G)$. By Lemma 18.74 g is in the center of G . Let $h \in G$ be of order p . Choose a maximal cyclic subgroup M of G such that $h \in M$. Then $\langle h \rangle$ and $\langle g \rangle$ both are subgroups of the cyclic group M . They coincide because their orders are equal.

Conversely, suppose $\langle g \rangle$ is the only subgroup of order p and g is in the center of G . Let M be a cyclic subgroup of G . If $p \nmid \#(M)$, then $\langle M, g \rangle$ is a larger cyclic subgroup. So the order of every maximal cyclic subgroup is a multiple of p . Since $\langle g \rangle$ is the only subgroup of order p , it follows that g is an element of all maximal cyclic subgroups. \square

So by this proposition and Corollary 18.73:

18.76 Proposition. *Let p be a prime number and G be a finite group. If G has a unique subgroup of order p and this subgroup is in the center of G , then G is exceptional.* \square

Noncyclic groups of order pq with p and q prime are nonexceptional (Examples 18.11 and 18.12). They cannot occur as subgroups of a strongly exceptional group. If a group is not strongly exceptional it must have such subgroup:

18.77 Theorem. *A finite group is strongly exceptional if and only if it has no noncyclic subgroup of order pq with p and q prime numbers.*

PROOF. It suffices to prove that a nonexceptional finite group for which all noncyclic proper subgroups are exceptional is a noncyclic group of order pq with p and q prime. Let G be such a group. Since G nonexceptional, its Sylow subgroups are proper subgroups and are therefore exceptional. By Proposition 18.68 they are cyclic or quaternion. If they are all cyclic, then G is metacyclic, in the sense that the commutator subgroup G' and the factor group G/G' are both cyclic. ([15], Theorem 9.4.3). In this case G must be a noncyclic group of order pq with p and q prime numbers.

So we now assume that a Sylow 2-subgroup of G is quaternion. This assumption has to lead to a contradiction. Let N be a nontrivial normal subgroup of G such that G/N is noncyclic. Consider the collection $\{G_i\}$ of proper subgroups of G containing N . These subgroups correspond via $G_i \mapsto G_i/N$ to proper subgroups of G/N and since G/N is noncyclic, G/N is the union of the G_i/N . Hence G is the union of the G_i . It follows that the collection $\{G_i\}$ is an exceptional collection of subgroups of G . By Theorem 18.71 G is exceptional. This shows that for all nontrivial normal subgroups the factor group is cyclic. The commutator subgroup G' is nontrivial. If $G' = G$, then factor groups of proper normal subgroups are not cyclic either. This means that G is simple. However, it is shown by Brauer and Suzuki in [5] that simple groups do not have such a Sylow 2-subgroup. Contradiction. \square

18.78 Corollary. *Let G a finite group which is not strongly exceptional and let A be a G -module. Then either $A = A_0$ or $pA \subseteq A_0$ for some unique prime p .*

PROOF. Assume that $A \neq A_0$. The group G has a noncyclic subgroup of order pq with p and $q \leq p$ prime. Its trivial norm coefficient equals $-p$. For this p we have $pA \subseteq A_0$. If $A \neq A_0$, then there is no such a subgroup with a different trivial norm coefficient. \square

18.79 Corollary. *Let $L : K$ be a Galois extension of number fields and suppose that its Galois group is not strongly exceptional. Then $\zeta_L(s)$ is in the group generated by the Dedekind zeta functions of intermediate fields $\neq L$.*

PROOF. By Theorem 18.77 the Galois group has a noncyclic subgroup U of order pq with p and q prime. From Corollary 18.40 and Corollary 18.41 follows that $\zeta_L(s)$ is in the group generated by the Dedekind zeta functions of the intermediate fields $\neq L$ of the extension $L : L^U$. \square

EXERCISES

- Let H be a normal subgroup of a finite group G . The subgroups of G/H correspond to subgroups U of G containing H .

(i) Show that the homomorphism $\mathbb{Z}\Sigma(G/H) \rightarrow \mathbb{Z}\Sigma(G)$ given by

$$U/H \mapsto U \quad \text{for } U \in \Sigma(G) \text{ such that } U \supseteq H$$

induces a homomorphism $\text{NR}(G/H) \rightarrow \text{NR}(G)$.

(ii) Show that this homomorphism is injective.

- Let be given

G	a finite abelian group,
$\sum_{U \in \Sigma(G)} n_U U$	a norm relation for G ,
B	a (multiplicative) abelian group,
f	a map from G^\vee to B .

Prove that the map

$$F : \Sigma(G^\vee) \rightarrow B, \quad V \mapsto \prod_{\chi \in V} f(\chi)$$

satisfies

$$\prod_{U \in \Sigma(G)} F(U^\perp)^{n_U \#(U)} = 1.$$

(Hint: use Lemma 18.33.)

- By Artin's Reciprocity Theorem the dual Artin map $\check{\varphi}_K^{(L)}$ of an abelian extension $L : K$ of number fields is an isomorphism $\text{Gal}(L : K)^\vee \xrightarrow{\sim} \mathcal{H}(L : K)$. In this case we can use Dirichlet characters instead of group characters and the correspondence between subgroups $V \in \mathcal{H}(L : K)$ and subgroups $U \in \Sigma(G)$ is given by

$$V^\perp = \text{Gal}(L : K_V) \quad \text{and} \quad U^\perp = \mathcal{H}(L^U : K).$$

Using this terminology, show that exercise 2 can be translated into the following:

let be given

$L : K$	an abelian extension of number fields,
G	the Galois group of $L : K$,
$\sum_{U \in \Sigma(G)} n_U U$	a norm relation for G ,
B	a (multiplicative) abelian group,
f	a map from $\mathcal{H}(L : K)$ to B .

Then the map

$$F : \Sigma(\mathcal{H}(L : K)) \rightarrow B, \quad V \mapsto \prod_{\chi \in V} f(\chi)$$

satisfies

$$\prod_{U \in \Sigma(G)} F(U^\perp)^{n_U \#(U)} = 1.$$

4. Let $L : K$ be an abelian extension of number fields, G the Galois group of $L : K$ and $\sum_{U \in \Sigma(G)} n_U U$ a norm relation for G . Show that

$$\prod_{U \in \Sigma(G)} \zeta_{L^U}(s)^{n_U \#(U)} = 1$$

by applying exercise 3 to the map

$$f : \mathcal{H}(L : K) \rightarrow \mathbb{C}^*, \quad \chi \mapsto L(s, \chi).$$

5. Let $L : K$ be an abelian extension of number fields, G the Galois group of $L : K$ and $\sum_{U \in \Sigma(G)} n_U U$ a norm relation for G . Show that

$$\prod_{U \in \Sigma(G)} \mathfrak{d}_K(L^U)^{n_U \#(U)} = 1$$

by applying exercise 3 to the map

$$f : \mathcal{H}(L : K) \rightarrow \mathbb{C}^*, \quad \chi \mapsto L(s, \chi).$$

6. Let q be an odd prime power. Show that $\mathrm{SL}(2, \mathbb{F}_q)$ is exceptional. (Hint: the group has a unique element of order 2.) Verify: for $q > 4$ the group is nonsolvable, because the group $\mathrm{PSL}(2, \mathbb{F}_q)$ is perfect.
7. Let q be an odd prime power. Show that a Sylow 2-subgroup of $\mathrm{SL}(2, \mathbb{F}_q)$ is quaternion.
8. Prove that the ideal class group of $\mathbb{Q}(\sqrt[3]{7})$ is of order 3. (Hint: exercise 6 of chapter 12 and Example 18.53.)
9. Let $m, n, r \in \mathbb{N}^*$ be such that $\mathrm{gcd}(m, n(r-1)) = 1$ and $r^n \equiv 1 \pmod{m}$. Prove that the metacyclic group $\langle g, h \rangle$ given by $o(g) = m$, $o(h) = n$ and $hgh^{-1} = g^r$ is strongly exceptional.

19 Infinite Extensions of Number Fields

Number fields are finite extensions of \mathbb{Q} . They are all embeddable in the algebraic closure $\overline{\mathbb{Q}}$, the field of algebraic numbers. The notion of Galois extension is, if not yet done so, easily extended to infinite algebraic extensions. For a generalization of Galois theory the Galois groups have to be endowed with a topology. This will be done in section 19.5. For this we need some generalities on topological groups and more generally on topological spaces (sections 19.1 up to 19.4). Galois groups turn out to be compact and totally separated, so in these sections there is special attention to compactness and total separateness.

The union K^{ab} of all finite abelian extensions (inside \mathbb{C}) of a number field K is an example of an infinite Galois extension. Its Galois group is a totally separated compact abelian group. Totally separated compact groups (so-called profinite groups) are treated in section 19.4. The dual of an abelian profinite group is the group of its continuous characters. Pontryagin's Duality Theorem (section 19.6) describes a self duality of the category of abelian topological groups. Under this duality abelian profinite groups correspond to abelian torsion groups. In section 19.6 this part of the theorem is proved. Class field theory gives us an isomorphism

$$\text{Gal}(K^{\text{ab}} : K)^{\vee} \xrightarrow{\sim} \mathcal{H}(K)$$

induced by the dual Artin maps of the finite abelian extensions of K . It is an isomorphism of abelian torsion groups.

19.1 Infinite products of topological spaces

The main theorem of this section is Tykhonov's Theorem: a (possibly infinite) product of compact spaces is a compact space. We review the notion of infinite product of spaces, show furthermore that the product of Hausdorff spaces is a Hausdorff space and that also total disconnectedness is preserved under taking products. For completeness the definitions of these topological notions are given.

A topological space $X = (X_0, \mathcal{T})$ is a set X_0 together with the collection \mathcal{T} of its open sets. Usually in the notation no distinction is made between X and its

underlying set X_0 . If X is a topological space, its topology may be denoted by \mathcal{T}_X . A collection \mathcal{T} of subsets of a set X is said to be a *topology* on X if \mathcal{T} is closed under (possibly infinite) unions and under finite intersections.

19.1 Definition. Let $(X_i)_{i \in I}$ be a collection of topological spaces indexed by the set I . The *product* X of the X_i is the product in the categorical sense: there are continuous maps $p_i: X \rightarrow X_i$ and for each collection $(f_i)_{i \in I}$ of continuous maps $f_i: Y \rightarrow X_i$ there is a unique continuous map $f: Y \rightarrow X$ such that $p_i f = f_i$ for all $i \in I$.

This definition implies that the product is unique up to a canonical isomorphism, but its existence still has to be shown. We will use the notions of base and subbase of a topology. Let's fix the terminology.

19.2 Definitions and notations. Let X be a topological space with topology \mathcal{T} . A *base* of \mathcal{T} is a subcollection \mathcal{S} of \mathcal{T} such that every $U \in \mathcal{T}$ is the union of a subcollection of \mathcal{S} . A *subbase* of \mathcal{T} is a subcollection \mathcal{S} of \mathcal{T} such that the intersections of finite subcollections of \mathcal{S} form a base of \mathcal{T} . This base is denoted by $\mathcal{S}^\#$.

Every collection \mathcal{S} of subsets of a set X defines a topology on X by declaring \mathcal{S} to be a subbase. The base $\mathcal{S}^\#$ then consists of all intersections of finite subcollections of \mathcal{S} and the topology is the collection of all unions of subcollections of $\mathcal{S}^\#$. (Here it is understood that an empty intersection is the whole set X .)

19.3 Proposition. Let $(X_i)_{i \in I}$ be a collection of topological spaces indexed by the set I . Let X be the topological space having the cartesian product $\prod_{i \in I} X_i$ as underlying set and the sets

$$\prod_{i \in I} U_i \quad \text{with } U_i \in \mathcal{T}_{X_i} \text{ and } U_i \neq X_i \text{ for only finitely many } i \in I,$$

as a base of its topology. Then the projections $p_i: X \rightarrow X_i$ are continuous and X (with these projections) is the product of the X_i .

PROOF. For $U \in \mathcal{T}_X$ the set $p_i^{-1}(U)$ is open in X . So the maps p_i are continuous. Let $(f_i)_{i \in I}$ be a collection of continuous maps $f_i: Y \rightarrow X_i$. Since X as a set is the product of the sets X_i , there is a unique map $f: Y \rightarrow X$ such that $p_i f = f_i$ for all $i \in I$. It remains to show that f is continuous. For base elements $U = \prod_{i \in I} U_i$ of \mathcal{T}_X we have

$$f^{-1}(U) = \bigcap_{i \in I} f_i^{-1}(U_i) = \bigcap_{\substack{i \in I \\ U_i \neq X_i}} f_i^{-1}(U_i),$$

an intersection of finitely many open sets. □

Note that the so-called *cylinder sets* $p_i^{-1}(U)$ with U open in X_i form a subbase of the topology of $\prod_{i \in I} X_i$. The base it determines is the one described in the above proposition.

In various important cases properties of the factors carry over to the product space: Tykhonov's Theorem 19.7 and Propositions 19.5 and 19.10.

19.4 Definition. A topological space X is called a *Hausdorff space* if for all $x, y \in X$ with $x \neq y$ there exist $U, V \in \mathcal{T}_X$ such that $x \in U$, $y \in V$ and $U \cap V = \emptyset$.

19.5 Proposition. *The product of a collection of Hausdorff spaces is a Hausdorff space.*

PROOF. Let $X = \prod_{i \in I} X_i$, where the X_i are Hausdorff spaces. If $x, y \in X$ with $x \neq y$, then $p_j(x) \neq p_j(y)$ for some $j \in I$. Let $U, V \in \mathcal{T}_{U_j}$ such that $p_j(x) \in U$, $p_j(y) \in V$ and $U \cap V = \emptyset$. Then $x \in p^{-1}(U)$, $y \in p^{-1}(V)$ and $p^{-1}(U) \cap p^{-1}(V) = \emptyset$. \square

In the proof of Tykhonov's Theorem Alexander's Subbase Theorem will be used: for open covers to have finite subcovers it suffices that covers by sets of a given subbase have this property.

19.6 Alexander's Subbase Theorem. *Let X be a topological space with a subbase \mathcal{S} of open sets. Suppose that each subcover of \mathcal{S} has a finite subcover. Then X is compact.*

PROOF. Suppose X is not compact. Then there are open covers of X without finite subcovers. By Zorn's Lemma there is a maximal such open cover \mathcal{C} . By assumption on \mathcal{S} , the collection $\mathcal{C} \cap \mathcal{S}$ does not cover X . Let $x \in X \setminus \bigcup_{U \in \mathcal{C} \cap \mathcal{S}} U$. Since \mathcal{C} covers X , there is a $U \in \mathcal{C}$ such that $x \in U$ and, because \mathcal{S} is a subbase, there is a finite subcollection \mathcal{F} of \mathcal{S} such that $x \in \bigcap_{V \in \mathcal{F}} V \subseteq U$. By the choice of x we have $\mathcal{F} \cup \mathcal{S} = \emptyset$. By maximality of \mathcal{C} for each $V \in \mathcal{F}$ the collection $\{V\} \cup \mathcal{C}$ has a finite subcover $\{V\} \cup \mathcal{F}_V$, where \mathcal{F}_V is a finite subcollection of \mathcal{C} . Put $\mathcal{F}^* = \bigcup_{V \in \mathcal{F}} \mathcal{F}_V$. Then also $\mathcal{F} \cup \mathcal{F}^*$ is a finite cover of X . If $x \notin V$, where $V \in \mathcal{F}$, then $x \in \bigcup_{W \in \mathcal{F}_V} W$. So also $\{\bigcap_{V \in \mathcal{F}} V\} \cup \mathcal{F}^*$ is a cover of X . Since $\bigcap_{V \in \mathcal{F}} V \subseteq U$, the collection $\{U\} \cup \mathcal{F}^*$ is a cover of X . This is a finite subcover of \mathcal{C} . Contradiction. \square

19.7 Tykhonov's Theorem. *The product of a collection of compact spaces is a compact space.*

PROOF. Let X be the product of a collection $(X_i)_{i \in I}$ of compact spaces X_i and \mathcal{S} the subbase of \mathcal{T}_X consisting of the sets $p_i^{-1}(U)$ with U open in X_i . Let $\mathcal{C} \subseteq \mathcal{S}$ be an open cover of X . It determines for each i a collection \mathcal{C}_i of open sets of X_i :

$$\mathcal{C}_i = \{U \in \mathcal{T}_{X_i} \mid p_i^{-1}(U) \in \mathcal{C}\}.$$

Suppose that for all i the collection \mathcal{C}_i does not cover X_i . Then there is an $x \in X$ such that $p_i(x) \notin \bigcup_{U \in \mathcal{C}_i} U$ for all i , that is $x \notin p_i^{-1}(U)$ for all i and all $U \in \mathcal{T}_{X_i}$. Since \mathcal{C} covers X , such an x does not exist. So there is an i such that \mathcal{C}_i covers X_i . Since X_i is compact the collection \mathcal{C}_i has a finite subcover \mathcal{F}_i . Then the collection

$$\mathcal{F} = \{p_i^{-1}(U) \mid U \in \mathcal{F}_i\}$$

is a finite subcover of \mathcal{C} . By Alexander's Subbase Theorem X is compact. \square

Finally we consider total separateness.

19.8 Definition. Two points of a topological space are said to be *separated* if there is an open and closed set containing one of them and not the other. A topological space is *totally separated* if any two points are separated.

A related notion is *total disconnectedness*: X is totally disconnected if the empty set and the one point subspaces are the only connected subspaces. A space being *connected* if the empty set and the total space are the only subsets which are both open and closed. Totally separated spaces are totally disconnected, but the converse does not hold. However, for locally compact Hausdorff spaces the two notions are equivalent (exercise 1). In this book only total separateness is used.

19.9 Example. The subset \mathbb{Q} of the topological space \mathbb{R} with the relative topology is totally separated. For $a, b \in \mathbb{Q}$ with $a < b$ choose an irrational λ in the interval (a, b) . The open set $(-\infty, \lambda) \cap \mathbb{Q}$ contains a , does not contain b and its complement is the open set $(\lambda, \infty) \cap \mathbb{Q}$.

19.10 Proposition. *Totally separated spaces are Hausdorff spaces. The product of a collection of totally separated spaces is totally separated.*

PROOF. The first part of the proposition is trivially true. For the second part let $(X_i)_{i \in I}$ be a collection of totally separated spaces. Let x and y be two different points of $\prod_i X_i$, then there is an $i \in I$ such that $p_i(x) \neq p_i(y)$. Since X_i is totally separated, it contains an open and closed set U such that $p_i(x) \in U$ and $p_i(y) \notin U$. Then x is in the open and closed subset $p_i^{-1}(U)$ of $\prod_i X_i$, whereas y is not. \square

19.2 Topological groups

19.11 Definition. A topological group G is both a group and a topological space in such a way that the group operations are continuous, that is the maps

$$G \times G \rightarrow G, (x, y) \mapsto xy \quad \text{and} \quad G \rightarrow G, x \mapsto x^{-1}$$

are continuous.

19.12 Examples.

- a) Well-known topological groups are the additive group \mathbb{R} , the multiplicative group \mathbb{R}^* and the circle group $\mathbb{S}^1 = \{z \in \mathbb{C} \mid |z| = 1\}$, all with the ordinary topology. The topological group \mathbb{R}/\mathbb{Z} is isomorphic to the circle group via $x \mapsto e^{2\pi ix}$.
- b) Subgroups of topological groups are topological groups as well: $\mathbb{Q}, \mathbb{Q}^*, \mu(\mathbb{C})$. These subgroups are examples of totally separated topological groups.

- c) Every absolute value on a field determines a topology on that field. For a number field K and \mathfrak{p} a prime of K , the additive group of the completion $K_{\mathfrak{p}}$ is a topological group and so is the multiplicative group $K_{\mathfrak{p}}^*$.

19.13 Lemma. *Let G be a topological group and $g \in G$. Then the map $G \rightarrow G, x \mapsto gx$ is a homeomorphism.*

PROOF. The map is the composition of the continuous maps $G \rightarrow G \times G, x \mapsto (g, x)$ and $G \times G \rightarrow G, (x, y) \mapsto xy$. Its inverse is the map $x \mapsto g^{-1}x$. \square

As a consequence open subgroups in a compact group are quite special:

19.14 Lemma. *Let H be a subgroup of a compact group G . Then H is open if and only if it is closed and of finite index.*

PROOF. If H is open, then by Lemma 19.13 the left cosets of H form an open covering of G . Since G is compact, it is covered by finitely many of these cosets. So the index of H is finite and since its complement is the union of open sets, H is also closed. Conversely, if H is closed and of finite index, it is the complement of finitely many closed sets. \square

A compact topological group is totally separated if and only if the open subgroups form a base for the neighborhoods of 1:

19.15 Proposition. *Let G be a compact topological group and \mathcal{N} the collection of open normal subgroups of G . Then*

$$G \text{ is totally separated} \iff \bigcap_{N \in \mathcal{N}} N = \{1\}.$$

PROOF.

\Rightarrow : We will show that for every $g \in G$ with $g \neq 1$, there exists an $N \in \mathcal{N}$ such that $g \notin N$. For a given $g \in G$ with $g \neq 1$ by total separateness there exists an open and closed set U with $1 \in U$ and $g \notin U$. Let $h \in U$. The image of $U \times U$ under the multiplication map $G \times G \rightarrow G$ will be denoted by U^2 . The restriction of this map to $U \times U \rightarrow U^2$ is continuous and maps $(h, 1)$ to h . Since U is an open neighborhood of h in U^2 , there are open sets V_h and W_h of U such that $h \in V_h, 1 \in W_h$ and that the image $V_h W_h$ of $V_h \times W_h$ is contained in U .

The collection $(V_h)_{h \in U}$ is an open cover of the compact set U , so there is a finite subset $F \subset U$ such that $U = \bigcup_{h \in F} V_h$. Set $W = \bigcap_{h \in F} W_h$ and $X = W \cap W^{-1}$, where $W^{-1} = \{x^{-1} \mid x \in W\}$. Then W , and hence also X , is an open neighborhood of 1 contained in U . We have

$$UX = \bigcup_{h \in F} V_h X \subseteq \bigcup_{h \in F} V_h W \subseteq \bigcup_{h \in F} V_h W_h \subseteq U$$

and by induction $UX^i \subseteq U$ for all $i \in \mathbb{N}^*$. Set $H = \bigcup_{i=1}^{\infty} X^i$. It is an open subset of U and clearly a subgroup of G . By Lemma 19.14 H is of finite index in G . Finally, set $N = \bigcap_{x \in G} xHx^{-1}$. Then N is a normal subgroup contained in U . Because H is of finite index, it has only finitely many conjugates and so N is open as well. Since $N \subseteq U$, the element g is not in N .

\Leftarrow : Let $g_1, g_2 \in G$ such that $g_1 \neq g_2$. From $\bigcap_{N \in \mathcal{N}} N = \{1\}$ follows that $\bigcap_{N \in \mathcal{N}} g_1N = \{g_1\}$. Hence there is an $N \in \mathcal{N}$ such that $g_2 \notin g_1N$, that is $g_1N \neq g_2N$. Since N is open, the cosets g_1N and g_2N are open. \square

19.3 Inductive and projective limits

In category theory one defines inverse limits (= colimits) and direct limits (= limits) of functors $D: \mathcal{I} \rightarrow \mathcal{C}$, where \mathcal{I} is a small category, the index category. If they exist they are defined up to a canonical isomorphism. If \mathcal{I} has only identity morphisms, the direct limit is called a sum and the inverse limit a product. The product of topological spaces in section 19.1 is the product in the categorical sense. In this section we consider another special case, the case where \mathcal{I} comes from a directed set.

19.16 Definition. Let I be a set and \leq an ordering of I . Then the ordered set I is called a *directed* ordered set if for each pair $i, j \in I$ there is a $k \in I$ such that $i \leq k$ and $j \leq k$. It corresponds to a category \mathcal{I} with I as the set of objects and one morphism $i \rightarrow j$ for each pair $i, j \in I$ with $i \leq j$.

19.17 Examples.

- a) The sets \mathbb{N} and \mathbb{Z} with the usual ordering \leq are directed ordered sets.
- b) The set \mathbb{N}^* with the ordering $|$ (= divisor of).
- c) The set $\mathcal{M}(K)$ of all moduli of a number field K with the ordering $|$.

Inductive limits

19.18 Definition. Let I be a directed ordered set and \mathcal{C} a category. An *inductive system in \mathcal{C}* indexed by I is a functor $\mathcal{I} \rightarrow \mathcal{C}$, where \mathcal{I} is the with I corresponding category. More concretely, it is a collection $(X_i)_{i \in I}$ of objects in \mathcal{C} together with morphisms $f_{ij}: X_i \rightarrow X_j$ for $i, j \in I$ with $i \leq j$ such that

$$(IS1) \quad f_{ii} = 1_{X_i} \text{ for all } i \in I,$$

$$(IS2) \quad f_{jk}f_{ij} = f_{ik} \text{ for all } i, j, k \in I \text{ with } i \leq j \leq k.$$

19.19 Example. Let \mathcal{C} be a collection of subsets of a given set X such that $U \cup V \in \mathcal{C}$ if $U, V \in \mathcal{C}$. Under the ordering \subseteq they form a directed ordered set and together with the inclusion maps they form an inductive system of sets indexed by themselves.

19.20 Definition. The direct limit of an inductive system is called an *inductive limit*. Specifically: let I be a directed ordered set and $(X_i)_{i \in I}$ an inductive system in a category \mathcal{C} indexed by I . The inductive limit X of the inductive system is an object X of \mathcal{C} together with morphisms $q_i: X_i \rightarrow X$ such that

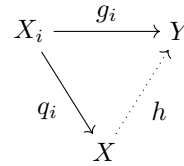
$$q_j f_{ij} = q_i \quad \text{for all } i, j \in I \text{ with } i \leq j$$

with the property that given an object Y of \mathcal{C} together with morphisms $g_i: X_i \rightarrow Y$ such that

$$g_j f_{ij} = g_i \quad \text{for all } i, j \in I \text{ with } i \leq j,$$

there is a unique morphism $h: X \rightarrow Y$ such that $h q_i = g_i$ for all $i \in I$. Notation:

$$X = \varinjlim_i X_i.$$



19.21 Example. For the system \mathcal{C} described in Example 19.19 we have

$$\varinjlim_{U \in \mathcal{C}} U = \bigcup_{U \in \mathcal{C}} U,$$

where for $V \in \mathcal{C}$ the map $q_V: V \rightarrow \bigcup_{U \in \mathcal{C}} U$ is the inclusion map.

In the next proposition the inductive limit of any inductive system of sets is constructed.

19.22 Proposition. Let I be a directed ordered set and $(X_i)_{i \in I}$ an inductive system of sets indexed by I . Its inductive limit can be constructed as the set

$$\left(\coprod_i X_i \right) / \sim,$$

where \coprod_i stands for disjoint union and \sim for the equivalence relation

$$x_i \sim x_j \iff f_{ij}(x_i) = x_j \quad (\text{for } x_i \in X_i, x_j \in X_j \text{ and } i \leq j),$$

together with the maps $q_i: X_i \rightarrow \left(\coprod_i X_i \right) / \sim$ induced by the inclusion maps $q_i: X_i \rightarrow \coprod_i X_i$. (In this description the X_i are assumed to be disjoint.)

PROOF. Let Y and g_i be as in the definition. The required unique map $h: X \rightarrow Y$ is the map induced by the $g_i: X_i \rightarrow Y$. \square

The advantage of inductive systems over arbitrary systems is that in many important cases the inductive limit has an underlying set which is the inductive limit of the underlying sets. Of course this makes sense only in cases where the objects do have underlying sets. We consider three special cases.

19.23 Proposition. *Let $(G_i)_{i \in I}$ be an inductive system of groups with group homomorphisms $f_{ij}: G_i \rightarrow G_j$. Then*

$$\varinjlim_i G_i = \left(\coprod_i G_i \right) / \sim$$

as a set. In particular it is the union of the subsets $f_i(G_i)$. The product of $q_i(g_i)$ and $q_j(g_j)$ (with $g_i \in G_i$ and $g_j \in G_j$) is defined by

$$q_i(g_i) \cdot q_j(g_j) = q_k(f_{ik}(g_i) \cdot f_{jk}(g_j)),$$

where $k \in I$ is such that $i, j \leq k$.

PROOF. Straightforward. Note that the multiplication is defined by choosing representatives in a single $q_k(G_k)$, which is possible because the index set is directed. \square

19.24 Example. The symmetric group S_n is the group of permutations of the set $\{1, \dots, n\}$. The set \mathbb{N}^* is ordered by the usual ordering \leq and obviously this ordering is directed. For $m \leq n$ we have a group homomorphism $f_{mn}: S_m \rightarrow S_n$ defined by

$$(f_{mn}(\sigma))(i) = \begin{cases} \sigma(i) & \text{if } i \leq m, \\ i & \text{otherwise.} \end{cases}$$

The groups S_n together with these maps form an inductive system of groups. For the inductive limit we can take the group S_∞ of all permutations σ of \mathbb{N}^* with $\sigma(i) \neq i$ for only finitely many i .

19.25 Example. Let \mathcal{N}_K be the collection of all number field extensions of a given number field K . Under \subseteq they form a directed ordered set and together with the inclusion maps we have an inductive system in the category of rings. The inductive limit of this system is the field $\overline{\mathbb{Q}}$, the algebraic closure in \mathbb{C} of any number field.

For topological spaces we have similarly:

19.26 Proposition. *Let $(X_i)_{i \in I}$ be an inductive system of topological spaces with continuous maps $f_{ij}: X_i \rightarrow X_j$. Then*

$$\varinjlim_i X_i = \left(\coprod_i X_i \right) / \sim$$

as a set. The space $\coprod_i X_i$ is the disjoint union of spaces and the topology of the inductive limit is given by the quotient topology. \square

19.27 Example. As for sets (Example 19.21) the inductive limit of an inductive system of subspaces of a topological space is the union of these subspaces.

Inductive limits in the category of topological groups are as for groups and for topological spaces. They just have the combined structure.

19.28 Proposition. *Inductive systems in the category of topological groups have an inductive limit in this category. Their underlying set is the inductive limit of the underlying sets. The group structure is as for inductive limits of groups and the topology is the topology for the inductive limit of topological spaces.*

PROOF. Let $(G_i)_{i \in I}$ be an inductive system of topological groups. Then the set $G = \varinjlim_i G_i$ is a group as well as a topological space. The map $G \rightarrow G$, $x \mapsto x^{-1}$ is continuous since all maps $G_i \rightarrow G_i$, $x \mapsto x^{-1}$ are continuous and \varinjlim_i is a functor from inductive systems of topological spaces to topological spaces. The system $(G_i \times G_i)_{i \in I}$ with the maps $G_j \times G_j \rightarrow G_i \times G_i$ componentwise is inductive and its inductive limit is $G \times G$. The map $G \times G \rightarrow G$, $(x, y) \mapsto xy$ is continuous because all maps $G_i \times G_i \rightarrow G_i$, $(x, y) \mapsto xy$ are. \square

19.29 Examples.

- a) The system $(\mathcal{D}_N)_{N \in \mathbb{N}^*}$ of groups of (ordinary) Dirichlet characters is an inductive system of finite abelian groups indexed by the directed set \mathbb{N}^* , ordered by $|$. The group of Dirichlet characters is its inductive limit:

$$\mathcal{D} = \varinjlim_N \mathcal{D}_N .$$

- b) Similarly for groups of Dirichlet characters of a number field K . The inductive system is $(\mathcal{H}_m)_{m \in \mathcal{M}(K)}$ and its inductive limit is the group of Dirichlet characters of K :

$$\mathcal{H}(K) = \varinjlim_m \mathcal{H}_m(K) .$$

The index set is $\mathcal{M}(K)$ ordered by $|$.

In both cases the inductive limit is an abelian torsion group. If the finite abelian groups are given the discrete topology, then the inductive limit has the discrete topology as well.

Projective limits

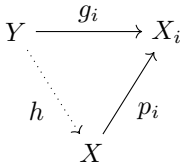
A projective system is an inductive system in the dual category.

19.30 Definition. Let I be a directed ordered set and \mathcal{C} a category. A *projective system in \mathcal{C}* indexed by I is a functor $\mathcal{I}^\circ \rightarrow \mathcal{C}$, where \mathcal{I} is the with I corresponding category; in other words it is a contravariant functor from \mathcal{I} to \mathcal{C} . More concretely, it is a collection $(X_i)_{i \in I}$ of objects in \mathcal{C} together with morphisms $f_{ij}: X_j \rightarrow X_i$ for $i, j \in I$ with $i \leq j$ such that

$$(PS1) \quad f_{ii} = 1_{X_i} \text{ for all } i \in I,$$

$$(PS2) \quad f_{ij}f_{jk} = f_{ik} \text{ for all } i, j, k \in I \text{ with } i \leq j \leq k.$$

19.31 Examples. Let X be a set and \mathcal{C} a collection of subsets of X such that $U \cap V \in \mathcal{C}$ for all $U, V \in \mathcal{C}$. With the ordering \supseteq the collection \mathcal{C} is a directed ordered set. Together with the inclusion maps the subsets in \mathcal{C} form a projective system.



19.32 Definition. The inverse limit of a projective system is called a *projective limit*. Specifically: let I be a directed ordered set and $(X_i)_{i \in I}$ a projective system in a category \mathcal{C} indexed by I . The projective limit X of the projective system is an object X of \mathcal{C} together with morphisms $p_i: X \rightarrow X_i$ such that

$$p_{ij}f_j = p_i \quad \text{for all } i, j \in I \text{ with } i \leq j$$

with the property that given an object Y of \mathcal{C} together with morphisms $g_i: Y \rightarrow X_i$ such that

$$f_{ij}g_j = g_i \quad \text{for all } i, j \in I \text{ with } i \leq j,$$

there is a unique morphism $h: Y \rightarrow X$ such that $p_i h = g_i$ for all $i \in I$. Notation:

$$X = \varprojlim_i X_i.$$

In the next proposition the projective limit of a projective system of sets is constructed.

19.33 Proposition. Let I be a directed ordered set and $(X_i)_{i \in I}$ a projective system of sets indexed by I . Its projective limit can be constructed as the set

$$X = \left\{ (x_i)_{i \in I} \in \prod_i X_i \mid f_{ij}(x_j) = x_i \text{ for all } i, j \in I \text{ with } i \leq j \right\}$$

together with the maps $p_i: X \rightarrow X_i$ induced by the projections $p_i: \prod_i X_i \rightarrow X_i$.

PROOF. Let Y and g_i be as in the definition. The required unique map $h: X \rightarrow Y$ is the map induced by the $g_i: X_i \rightarrow Y$. \square

Again in many important cases in which the objects of the category \mathcal{C} are sets together with extra structure, the projective limit exists and its underlying set is the projective limit of the underlying sets. In fact this often holds more in general for inverse limits in such categories.

19.34 Example. Let K be a discretely valued field, R its valuation ring and \mathfrak{p} the maximal ideal of R . In section 10.5 we considered the \mathfrak{p} -adic completion \hat{K} of K . It is a discretely valued field as well and its residue class field is canonically isomorphic with the residue class field of K . In 10.37 an alternative construction for the valuation ring \hat{R} was given. It is a projective limit:

$$\hat{R} = \varprojlim_{i \in \mathbb{N}^*} R/\mathfrak{p}^i.$$

The projective system is

$$\cdots \rightarrow R/\mathfrak{p}^{i+1} \rightarrow R/\mathfrak{p}^i \rightarrow \cdots \rightarrow R/\mathfrak{p},$$

where the maps $R/\mathfrak{p}^{i+1} \rightarrow R/\mathfrak{p}^i$ are induced by the identity on R . See also Notations 10.38 for the notations used in the number field case. In particular for K a number field and $\mathfrak{p} \in \text{Max}(\mathcal{O}_K)$ we have

$$\mathcal{O}_{\mathfrak{p}} = \varprojlim_{i \in \mathbb{N}^*} \mathcal{O}_K/\mathfrak{p}^i.$$

For $K = \mathbb{Q}$ and p a prime number this is the ring \mathbb{Z}_p of p -adic integers:

$$\mathbb{Z}_p = \varprojlim_{i \in \mathbb{N}^*} \mathbb{Z}/p^i.$$

In the next section projective limits of groups are considered and these limits will be endowed with a topology. Therefore, we first have a look at projective limits of topological spaces.

19.35 Proposition. Let $(X_i)_{i \in I}$ be a projective system of topological spaces with continuous maps $f_{ij}: X_j \rightarrow X_i$. Then

$$\varprojlim_i X_i = \left\{ (x_i)_{i \in I} \in \prod_i X_i \mid f_{ij}(x_j) = x_i \text{ for all } i, j \in I \text{ with } i \leq j \right\}$$

as a set. The topology of $\varprojlim_i X_i$ is the topology relative to the product topology of $\prod_i X_i$.

PROOF. The maps $p_i: \varprojlim_i X_i \rightarrow X_i$ are compositions of continuous maps: $\varprojlim_i X_i \rightarrow \prod_i X_i$ and the projection $\prod_i X_i \rightarrow X_i$. The defining properties for a projective limit are easily verified. \square

19.36 Proposition. Let $(X_i)_{i \in I}$ be a projective system of Hausdorff spaces. Then $\varprojlim_i X_i$ is a Hausdorff space and is closed in $\prod_i X_i$.

PROOF. By Proposition 19.5 the product $\prod_i X_i$ is a Hausdorff space, so the subspace $\varprojlim_i X_i$ is a Hausdorff space as well. We will prove that $\varprojlim_i X_i$ is closed in $\prod_i X_i$. Let $a = (a_i)_i \in \prod_i X_i \setminus \varprojlim_i X_i$. Then there are $j, k \in I$ such that $j \leq k$ and $f_{jk}(a_k) \neq a_j$. Since X_j is a Hausdorff space, there are disjoint open neighborhoods U and V of a_j and $f_{jk}(a_k)$ respectively. Set $V' = f_{jk}^{-1}(V)$. It is an open neighborhood of a_k in X_k . Then $p_j^{-1}(U) \cap p_k^{-1}(V')$ is an open neighborhood of a in $\prod_i X_i$ disjoint from $\varprojlim_i X_i$. \square

19.37 Theorem. *The projective limit of a projective system of compact Hausdorff spaces is a compact Hausdorff space.*

PROOF. Let $(X_i)_{i \in I}$ be a projective system of nonempty compact Hausdorff spaces. By Proposition 19.36 $\varprojlim_i X_i$ is closed in $\prod_i X_i$, which by Tykhonov's Theorem (Theorem 19.7) is compact. So $\varprojlim_i X_i$ is compact. \square

19.38 Proposition. *The projective limit of totally separated spaces is a totally separated space.*

PROOF. This follows from Proposition 19.10. \square

19.39 Example. The ring $\mathcal{O}_{\mathfrak{p}}$ in Example 19.34 is the projective limit of a system of finite rings $\mathcal{O}_K/\mathfrak{p}^i$. Endowing these finite rings with the discrete topology results in a compact totally separated topology on $\mathcal{O}_{\mathfrak{p}}$. It is in fact the topology which comes from the metric $\|\cdot\|_{\mathfrak{p}}$. In the next section we will have a closer look at projective limits of systems of finite groups.

For topological groups we again have the combination of both structures and the situation is as for inductive limits.

19.40 Proposition. *Projective systems in the category of topological groups have a projective limit in this category. Their underlying set is the projective limit of the underlying sets. The group structure is as for projective limits of groups and the topology is the topology for the projective limit of topological spaces.*

PROOF. The proof is almost identical to the proof for the inductive limit of topological groups. \square

The inductive limit of nonempty sets obviously is nonempty. For projective limits the situation is different. The following example is from the short note [38].

19.41 Example. The finite subsets of \mathbb{R} form a directed ordered set under inclusion. The sets

$$X_S = \{ f: S \rightarrow \mathbb{Z} \mid f \text{ is injective} \}$$

indexed by the finite sets form a projective system of sets: for $S \subseteq T$ a (surjective) map $X_T \rightarrow X_S$ is given by restriction. An element f of $\varprojlim_S X_S$ is a collection $(f_S)_S$ of injections $f_S: S \rightarrow \mathbb{Z}$ such that $f_S = f_T|_S$ for all finite $S, T \subseteq \mathbb{R}$ with $S \subseteq T$. This would mean that we have an injection of \mathbb{R} into \mathbb{Z} . So there are no elements in the projective limit.

Projective limits of compact spaces are nonempty:

19.42 Theorem. *Let $(X_i)_{i \in I}$ be a projective system of nonempty compact spaces. Then $\varprojlim_i X_i$ is nonempty.*

PROOF. For $l \in I$ put

$$Y_l = \left\{ (x_i)_{i \in I} \in \prod_i X_i \mid f_{ij}(x_j) = x_i \text{ for all } i, j \in I \text{ with } i \leq j \leq l \right\}.$$

Then $\varprojlim_i X_i = \bigcap_{l \in I} Y_l$ and $\prod_i X_i = \bigcup_{l \in I} Y_l$. The set Y_l is closed in $\prod_i X_i$. The proof of this is almost identical to the proof of Proposition 19.36. Suppose $\varprojlim_i X_i = \emptyset$. Then, since $\prod_i X_i$ is compact, there is a finite index set $J \subset I$ such that $\bigcap_{j \in J} Y_j = \emptyset$. Since the index set is a directed ordered set, there is an $l \in I$ such that $j \leq l$ for all $j \in J$. Take a $z \in X_l$ (the sets X_i are nonempty) and define an $(x_i)_i \in \prod_i X_i$ as follows

$$x_i = \begin{cases} f_{il}(z), & \text{if } i \leq l, \\ \text{any element of } X_i, & \text{otherwise.} \end{cases}$$

The element thus defined is an element of Y_l and hence of all Y_j with $j \in J$ because $j \leq l$ for all $j \in J$. This contradicts $\bigcap_{j \in J} Y_j = \emptyset$, which was a consequence of the projective limit being empty. \square

19.43 Corollary. *The projective limit of a projective system of nonempty finite sets is nonempty.*

PROOF. Finite sets can be regarded as discrete topological spaces. As such they are compact Hausdorff spaces. It follows that a projective limit of nonempty finite sets is nonempty. Of course a proof of this might be given not using topology. \square

Cofinal subsets

19.44 Definition. Let I be a directed set. A subset J of I is called *cofinal* if for each $i \in I$ there is a $j \in J$ with $i \leq j$.

Clearly, a cofinal subset of a directed set is a directed set as well. We will show that inductive and projective limits are unchanged when restricting the directed set to a cofinal subset. We will use the categorical definitions, so it suffices to prove this for inductive systems.

19.45 Theorem. *Let I be a directed set, $(X_i)_{i \in I}$ an inductive system in a category \mathcal{C} and J a cofinal subset of I . Then*

$$\varinjlim_{j \in J} X_j \xrightarrow{\sim} \varinjlim_{i \in I} X_i.$$

PROOF. The morphisms $q_j : X_j \rightarrow \varinjlim_{i \in I} X_i$ induce a morphism

$$\varphi : \varinjlim_{j \in J} X_j \longrightarrow \varinjlim_{i \in I} X_i.$$

For each $i \in I$ choose an $i^* \in J$ such that $i \leq i^*$. For $i \in I$ define morphisms $f_i = q_{i^*} f_{ii^*} : X_i \rightarrow \varinjlim_{j \in J} X_j$. They induce a morphism

$$\psi : \varinjlim_{i \in I} X_i \longrightarrow \varinjlim_{j \in J} X_j.$$

The categorical definition of inductive limit shows in a direct manner that $\varphi\psi$ and $\psi\varphi$ are the identity morphisms. \square

For inductive systems of sets it also follows directly from Proposition 19.22:

$$\prod_{j \in J} X_j \subseteq \prod_{i \in I} X_i$$

and since the relation \sim in the subset is the restriction of \sim it follows that

$$\left(\prod_{j \in J} X_j \right) / \sim \subseteq \left(\prod_{i \in I} X_i \right) / \sim.$$

Equality is a direct consequence of the cofinality.

Because of its importance we formulate the property for projective limits separately.

19.46 Theorem. *Let I be a directed set, $(X_i)_{i \in I}$ a projective system in a category \mathcal{C} and J a cofinal subset of I . Then*

$$\varprojlim_{i \in I} X_i \xrightarrow{\sim} \varprojlim_{j \in J} X_j. \quad \square$$

In the case of a projective system in the category of sets it also follows directly from the description of the projective limit (Proposition 19.33). The projection $\prod_{i \in I} X_i \rightarrow \prod_{j \in J} X_j$ induces by cofinality a bijection on the subsets: $\varprojlim_{i \in I} X_i \xrightarrow{\sim} \varprojlim_{j \in J} X_j$.

19.47 Examples.

- a) Cofinal subsets of (\mathbb{N}, \leq) are the unbounded subsets.
- b) The subset $\{n! \mid n \in \mathbb{N}^*\}$ is cofinal in $(\mathbb{N}^*, |)$.
- c) For I a directed set and $k \in I$ the subset $\{i \in I \mid k \leq i\}$ is cofinal.

19.48 Example. Let p be a prime number. The inductive limit $\varinjlim_{n \in \mathbb{N}^*} \mathbb{F}_{p^{n!}} = \bigcup_{n \in \mathbb{N}^*} \mathbb{F}_{p^{n!}}$ is the algebraic closure of \mathbb{F}_p .

19.49 Example. Let $L : K$ be an extension of number fields. The groups

$$\mathcal{C}_m(L : K) = \mathbb{I}^m(K) / N_K^L(\mathbb{I}^m(L)) \mathbb{S}_m(K)$$

form a projective system of finite abelian groups indexed by the directed set $\mathcal{M}(K)$. The maps $\mathcal{C}_n(L : K) \rightarrow \mathcal{C}_m(L : K)$ for $m \mid n$ are isomorphisms if m is a multiple of the conductor $\mathfrak{f}_K(L)$. The multiples of $\mathfrak{f} = \mathfrak{f}_K(L)$ form a cofinal subset of $\mathcal{M}(K)$ and so

$$\varprojlim_m \mathcal{C}_m(L : K) = \varprojlim_{\substack{m \\ \mathfrak{f} \mid m}} \mathcal{C}_m(L : K) = \mathcal{C}_{\mathfrak{f}}(L : K).$$

Exactness

For a fixed directed set I we consider functors from inductive (respectively projective) systems of topological groups indexed by I to topological groups. As usual we call a sequence

$$G' \xrightarrow{\varphi} G \xrightarrow{\psi} G''$$

of group homomorphisms *exact* if $\text{Im}(\varphi) = \text{Ker}(\psi)$. Note that this implies that $\text{Im}(\varphi)$ is a normal subgroup of G . We show that for inductive systems of topological groups the functor is exact. The projective limit is exact when restricted to compact groups.

19.50 Theorem. Let I be a directed set and let $(\varphi_i)_i : (G'_i)_i \rightarrow (G_i)_i$ and $(\psi_i)_i : (G_i)_i \rightarrow (G''_i)_i$ be morphisms of inductive systems of topological groups such that the sequences

$$G'_i \xrightarrow{\varphi_i} G_i \xrightarrow{\psi_i} G''_i$$

are exact for all $i \in I$. Then the induced sequence

$$\varprojlim_i G'_i \xrightarrow{\varphi} \varprojlim_i G_i \xrightarrow{\psi} \varprojlim_i G''_i$$

is also exact.

PROOF. Clearly $\psi\varphi$ is the trivial homomorphism. Now let $x \in \text{Ker}(\psi)$, say $x = q_i(x_i)$ for some $i \in I$ (in the notation of Definition 19.20). Then $q_i(\psi_i(x_i)) = \psi(q_i(x)) = \psi(x) = 1$. So there exists a $j \geq i$ such that $f_{ij}(q_i(\psi_i(x_i))) = 1 \in G''_j$, that is $\psi_j(f_{ij}(x_i)) = 1$. Hence there exists a $y_j \in G''_j$ such that $\varphi_j(y_j) = f_{ij}(x_i)$. Then

$$\varphi(q_j(y_j)) = q_j(\varphi_j(y_j)) = q_j(f_{ij}(x_i)) = q_i(x_i) = x. \quad \square$$

19.51 Example. Let $L : K$ be an extension of number fields. The groups $\mathcal{H}_m(L : K) = \mathcal{H}(L : K) \cap \mathcal{H}_m$ are the kernels of the conorm:

$$1 \rightarrow \mathcal{H}_m(L : K) \rightarrow \mathcal{H}_m(K) \xrightarrow{\nu_K^L} \mathcal{H}_m(L)$$

Then, because $\mathcal{H}_m(L : K) = \mathcal{H}_f(L : K) = \mathcal{H}(L : K)$ for all multiples m of the conductor f , by Theorem 19.50 we have an exact sequence

$$1 \rightarrow \mathcal{H}(L : K) \longrightarrow \varinjlim_m \mathcal{H}_m(K) \longrightarrow \varinjlim_m \mathcal{H}_m(L)$$

and thus, since $\mathcal{M}(K)$ is a cofinal subset of $\mathcal{M}(L)$, we have an exact sequence

$$1 \rightarrow \mathcal{H}(L : K) \longrightarrow \mathcal{H}(K) \longrightarrow \mathcal{H}(L),$$

which agrees with the given definition of $\mathcal{H}(L : K)$.

19.52 Theorem. *Let I be a directed set and let $(\varphi_i)_i: (G'_i)_i \rightarrow (G_i)_i$ and $(\psi_i)_i: (G_i)_i \rightarrow (G''_i)_i$ be morphisms of projective systems of compact groups such that the sequences*

$$G'_i \xrightarrow{\varphi_i} G_i \xrightarrow{\psi_i} G''_i$$

are exact for all $i \in I$. Then the induced sequence

$$\varprojlim_i G'_i \xrightarrow{\varphi} \varprojlim_i G_i \xrightarrow{\psi} \varprojlim_i G''_i$$

is also an exact sequence of compact groups.

PROOF. We consider projective limits as subspaces of products. Let $x = (x_i)_i \in \text{Ker}(\psi)$. Then $\psi_i(x_i) = 1$ for all $i \in I$. By continuity of the maps φ_i the sets $X_i = \varphi_i^{-1}(\{x_i\}) \subseteq G'_i$ form a projective system of nonempty closed subsets of the G'_i . Since G'_i is compact, the subset X_i is compact. By Theorem 19.42 $\varprojlim_i X_i \subseteq G'$ is nonempty. The homomorphism φ maps every element of $\varprojlim_i X_i$ to x . \square

19.53 Example. Let $L : K$ be an extension of number fields. Then the groups $\mathcal{C}_m(L : K)$ are cokernels of the transfer:

$$\mathcal{C}_m(L) \xrightarrow{\text{tr}_K^L} \mathcal{C}_m(K) \longrightarrow \mathcal{C}_m(L : K) \rightarrow 1.$$

The groups in this sequence are finite, so when endowed with the discrete topology they are compact. Hence by Theorem 19.52 and Example 19.49 we have an exact sequence

$$\varprojlim_m \mathcal{C}_m(L) \longrightarrow \varprojlim_m \mathcal{C}_m(K) \longrightarrow \mathcal{C}_f(L : K) \rightarrow 1,$$

where f is the conductor of $L : K$.

19.4 Profinite groups

In the next section we consider infinite Galois extensions. Their Galois groups are easily seen to be projective limits of finite Galois groups. Here we study projective limits of finite groups in general. The finite groups are regarded as finite

discrete topological groups and as a consequence the projective limits are topological groups. The groups that arise this way can be characterized intrinsically by their topology, independent of their construction as a projective limit.

19.54 Definition. Totally separated compact groups are called *profinite groups*.

19.55 Theorem. *Projective limits of finite discrete groups are profinite groups.*

PROOF. Finite discrete sets are totally separated compact spaces. The theorem follows from Proposition 19.30 and Theorem 19.37. \square

Conversely:

19.56 Theorem. *Let G be a profinite group and \mathcal{N} the collection of open normal subgroups of G . Then $G = \varprojlim_{N \in \mathcal{N}} G/N$. So profinite groups are projective limits of finite discrete groups.*

PROOF. The collection \mathcal{N} is a directed ordered set under \supseteq , so we have a projective system of groups G/N with $N \in \mathcal{N}$ and for $N_1, N_2 \in \mathcal{N}$ with $N_1 \supseteq N_2$ a canonical homomorphism $f_{N_1, N_2}: G/N_2 \rightarrow G/N_1$. The canonical homomorphisms $G \rightarrow G/N$, $x \mapsto xN$ induce a homomorphism of topological groups

$$h: G \longrightarrow \varprojlim_{N \in \mathcal{N}} G/N, \quad x \mapsto (xN)_N.$$

By Lemma 19.14 the groups G/N are finite. We will show that h is an isomorphism of topological groups. By Lemma 19.15 we have $\text{Ker}(h) = \bigcap_{N \in \mathcal{N}} N = \{1\}$, so h is injective. For surjectivity let $(x_N N)_{N \in \mathcal{N}} \in \varprojlim_{N \in \mathcal{N}} G/N$. Then to prove that $\bigcap_{N \in \mathcal{N}} x_N N \neq \emptyset$. Suppose $\bigcap_{N \in \mathcal{N}} x_N N = \emptyset$. Since G is compact and the sets $x_N N$ are closed, there is a finite subcollection \mathcal{N}_0 of \mathcal{N} such that $\bigcap_{N \in \mathcal{N}_0} x_N N = \emptyset$. Choose $M \in \mathcal{N}$ such that $N \supseteq M$ for all $N \in \mathcal{N}_0$, e.g. $M = \bigcap_{N \in \mathcal{N}_0} N$. Then $x_N N \supseteq x_N M = x_M M$ for all $N \in \mathcal{N}_0$ and so $\bigcap_{N \in \mathcal{N}_0} x_N N \supseteq x_M M$. Contradiction: $x_M M$ is nonempty. \square

In general in a profinite group closed subgroups are intersections of open subgroups:

19.57 Theorem. *Let H be a subgroup of a profinite group G . Then*

- a) H is open if and only if H is closed and of finite index,
- b) H is closed if and only if H is an intersection of open subgroups,
- c) H is normal and closed if and only if H is an intersection of open normal subgroups.

PROOF.

- a) This follows from Lemma 19.14 since profinite groups are compact.

- b) Open subgroups are closed and so is their intersection. Let H be closed and \mathcal{N} the collection of open normal subgroups of G . For each $N \in \mathcal{N}$ the subgroup HN is the union of the open sets hN with $h \in H$ and is therefore an open subgroup. We will show that $H = \bigcap_{N \in \mathcal{N}} HN$. By Lemma 19.15 we have

$$\bigcap_{N \in \mathcal{N}} HN \supseteq H \left(\bigcap_{N \in \mathcal{N}} N \right) = H.$$

Let $g \in \bigcap_{N \in \mathcal{N}} HN$ and suppose that $g \notin H$. Then $1 \notin Hg$ and so

$$\bigcap_{N \in \mathcal{N}} (N \cap Hg) = \left(\bigcap_{N \in \mathcal{N}} N \right) \cap Hg = \{1\} \cap Hg = \emptyset.$$

Because G is compact, there is a finite subcollection \mathcal{N}_0 of \mathcal{N} such that

$$\emptyset = \bigcap_{N \in \mathcal{N}_0} (N \cap Hg) = \left(\bigcap_{N \in \mathcal{N}_0} N \right) \cap Hg.$$

Hence $g \notin H \left(\bigcap_{N \in \mathcal{N}_0} N \right)$. However, the subgroup $\bigcap_{N \in \mathcal{N}_0} N$ is open and therefore $g \notin \bigcap_{N \in \mathcal{N}} HN$. Contradiction.

- c) This follows from b): if H is a normal subgroup, then so are the groups HN . □

Next we consider dense subsets of a profinite group. A subset of a topological space X is dense if X is its closure. This is equivalent to: each nonempty open subset of X contains an element of S . We will use the following lemma.

19.58 Lemma. *Let $(G_i)_{i \in I}$ be a projective system of finite discrete groups and $G = \varprojlim_i G_i$. Then the cosets of $\text{Ker}(p_i: G \rightarrow G_i)$ form a base of the topology of G .*

PROOF. A subbase \mathcal{B} for the topology of G is the collection of sets $p_i^{-1}(x_i)$ with $i \in I$ and $x_i \in G_i$. The set $p_i^{-1}(x_i)$ is a coset of $\text{Ker}(p_i)$. For $k \leq i$ in I , the set $p_i^{-1}(x_i)$ is a union of (a finite number of) cosets of $\text{Ker}(p_k)$. The intersection of a coset of $\text{Ker}(p_i)$ and a coset of $\text{Ker}(p_j)$ is the union of cosets of $\text{Ker}(p_k)$, where $k \in I$ such that $i, j \leq k$. So the subbase \mathcal{B} is actually a base. □

19.59 Theorem. *Let $(G_i)_{i \in I}$ be a projective system of finite discrete groups and $G = \varprojlim_i G_i$. Then a subset S of G is dense in G if and only if $p_i(S) = p_i(G)$ for all $i \in I$.*

PROOF. Suppose S is dense. For $x_i \in p_i(G)$, the set $p_i^{-1}(x_i)$ is open in G . Hence it contains an element y of S and so $x_i = p_i(y) \in p_i(S)$. Conversely, if $p_i(S) = p_i(G)$ for all $i \in I$, then the nonempty open sets $p_i^{-1}(x_i)$ with $x_i \in G_i$ contain an element of S . These open sets form by Lemma 19.58 a base of the topology of G . □

19.60 Examples.

- a) Let p be a prime number. The maps $\mathbb{Z} \rightarrow \mathbb{Z}/p^i$ are surjective. The subset \mathbb{Z} of the ring \mathbb{Z}_p of p -adic integers is dense.
- b) The finite rings \mathbb{Z}/n form a projective system indexed by $(\mathbb{N}^*, |)$. For $m | n$ we have ring homomorphisms $f_{mn}: \mathbb{Z}/n \rightarrow \mathbb{Z}/m$. Its projective limit is denoted by $\hat{\mathbb{Z}}$ and is sometimes referred to as the *Prüfer ring*:

$$\hat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n.$$

It follows from the Chinese Remainder Theorem that we have an isomorphism of profinite groups

$$\hat{\mathbb{Z}} \simeq \prod_p \mathbb{Z}_p,$$

where the product is over all prime numbers (exercise 2). Here too the subring \mathbb{Z} is dense in $\hat{\mathbb{Z}}$.

- c) The finite groups $(\mathbb{Z}/n)^*$, the units of \mathbb{Z}/n , form a projective system indexed by $(\mathbb{N}^*, |)$. For $m | n$ we have group homomorphisms $f_{mn}: (\mathbb{Z}/n)^* \rightarrow (\mathbb{Z}/m)^*$, the restrictions of the f_{mn} of the previous example. We have

$$\varprojlim_n (\mathbb{Z}/n)^* = \hat{\mathbb{Z}}^*.$$

Some generalities on subgroups, quotient groups and homomorphisms of profinite groups.

19.61 Theorem.

- (i) Let G be a profinite group and H a subgroup of G with the relative topology. Then H is profinite if and only if H is closed.
- (ii) Let G be a profinite group and N a normal subgroup of G . Then G/N with the quotient topology is a profinite group if and only if N is closed.

PROOF.

- (i) H is totally separated. H is compact if and only if it is closed in G .
- (ii) G/N is compact. Let \mathcal{M} be the collection of open normal subgroups containing N . Then by Theorem 19.57 N is closed if and only if $\bigcap_{M \in \mathcal{M}} M = N$. This is equivalent to $\bigcap_{M \in \mathcal{M}} M/N = \{N\}$, which by Lemma 19.15 is equivalent to G/N being totally separated. \square

Finally we consider the abelianization of profinite groups.

19.62 Definition and notation. Let G be a profinite group. The commutator subgroup G' of G is a normal subgroup and so is its closure $\overline{G'}$. The factor group $G/\overline{G'}$ is called the *abelianization* of G and is denoted by G^{ab} . It clearly is the largest profinite group under the factor groups G/N with G/N profinite and abelian.

19.63 Proposition. Let $(G_i)_{i \in I}$ be a projective system of finite discrete groups and $G = \varprojlim_i G_i$. Assume that the projections $p_i: G \rightarrow G_i$ are surjective. Then $G^{\text{ab}} = \varprojlim_i G_i^{\text{ab}}$.

PROOF. The short exact sequences

$$1 \rightarrow G'_i \rightarrow G_i \rightarrow G_i^{\text{ab}} \rightarrow 1$$

form a short exact sequence of projective systems of finite discrete groups indexed by I . By Theorem 19.52 a short exact sequence

$$1 \rightarrow \varprojlim_i G'_i \rightarrow G \rightarrow \varprojlim_i G_i^{\text{ab}} \rightarrow 1$$

of profinite groups is induced. Since $\varprojlim_i G_i^{\text{ab}}$ is abelian we have $G' \subseteq \varprojlim_i G'_i$. The maps $G' \rightarrow G'_i$ are surjective because the $G \rightarrow G_i$ are. By Theorem 19.59 G' is dense in $\varprojlim_i G'_i$. Hence $\overline{G'} = \varprojlim_i G'_i$ and consequently $G^{\text{ab}} = \varprojlim_i G_i^{\text{ab}}$. \square

19.5 Infinite Galois extensions

19.64 Definition. An algebraic field extension $L : K$ is called a *Galois extension* if it is normal and separable. The group of K -algebra automorphisms of L is called the *Galois group* of $L : K$. Notation: $\text{Gal}(L : K)$.

So far Galois extensions were assumed to be finite. This notion is now extended to algebraic extensions. Many of the properties of finite Galois extensions clearly hold for Galois extensions in general as well.

19.65 Proposition. Let $L : K$ be a Galois extension and M an intermediate field of $L : K$. Then $L : M$ is a Galois extension.

PROOF. The minimal polynomial of an $\alpha \in L$ over M is a divisor in $M[X]$ of the minimal polynomial over K . \square

19.66 Notation. For a Galois extension $L : K$ the collection of intermediate fields M such that $M : K$ is a finite Galois extension is denoted by $\mathcal{F}(L : K)$. It is an inductive system, ordered by \subseteq .

19.67 Proposition. Let $L : K$ be a Galois extension and $\mathcal{F} = \mathcal{F}(L : K)$. Then $L = \varinjlim_{M \in \mathcal{F}} M = \bigcup_{M \in \mathcal{F}} M$.

PROOF. Let $\alpha \in L$. The extension is normal, so the minimal polynomial of α over K splits in L . Hence L contains a splitting field M of this minimal polynomial over K and by separability $M : K$ is a Galois extension. \square

19.68 Corollary. *Let \bar{K} be an algebraic closure of a field K , L an intermediate field of $\bar{K} : K$ such that $L : K$ is a Galois extension and σ an embedding of L in \bar{K} fixing K . Then $\sigma(L) = L$.*

PROOF. In the notation of Proposition 19.67:

$$\sigma(L) = \sigma\left(\bigcup_{M \in \mathcal{F}} M\right) = \bigcup_{M \in \mathcal{F}} \sigma(M) = \bigcup_{M \in \mathcal{F}} M = L. \quad \square$$

19.69 Proposition. *Let $L : K$ be an algebraic field extension, M an intermediate field of $L : K$, \bar{K} an algebraic closure of K and $\sigma : M \rightarrow \bar{K}$ an embedding fixing K . Then there exists a prolongation $\tau : L \rightarrow \bar{K}$ of σ .*

PROOF. Let Φ be the ordered set of all pairs (N, ρ) consisting of an intermediate field N of $L : M$ and a prolongation ρ of σ to N . Clearly, a linearly ordered subset of Φ has an upper bound, so by Zorn's Lemma there is a maximal element in Φ , say (N, τ) is maximal. Then $N = L$, since otherwise there is an $\alpha \in L \setminus M$ and a prolongation of τ to $N(\alpha)$: send α to a zero of $f^\tau \in \bar{K}[X]$. \square

19.70 Proposition. *Let $L : K$ be a Galois extension, M an intermediate field of $L : K$ such that $M : K$ is a Galois extension. Then the restriction of automorphisms in $\text{Gal}(L : K)$ to the subfield M induces a group isomorphism*

$$\text{Gal}(L : K) / \text{Gal}(L : M) \xrightarrow{\sim} \text{Gal}(M : K).$$

PROOF. By Proposition 19.69 every $\sigma \in \text{Gal}(M : K)$ has a prolongation τ of σ to L and by Corollary 19.68 $\sigma(L) = L$. Hence restriction of automorphisms is a surjective group homomorphism $\text{Gal}(L : K) \rightarrow \text{Gal}(M : K)$. The kernel is $\text{Gal}(L : M)$. \square

19.71 Theorem. *Let $L : K$ be a Galois extension and $G = \text{Gal}(L : K)$. Then $L^G = K$.*

PROOF. For each $M \in \mathcal{F} = \mathcal{F}(L : K)$ by Proposition 19.70 the group G acts on M via $\text{Gal}(M : K)$. Hence $M^G = K$ and

$$L^G = \left(\bigcup_{M \in \mathcal{F}} M\right)^G = \bigcup_{M \in \mathcal{F}} M^G = K. \quad \square$$

19.72 Theorem. *Let $L : K$ be a Galois extension and M an intermediate field of $L : K$. Then $M : K$ is a Galois extension if and only if $\text{Gal}(L : M)$ is a normal subgroup of $\text{Gal}(L : K)$.*

PROOF. If $M : K$ is a Galois extension, then by Proposition 19.70 the group $\text{Gal}(L : M)$ is a normal subgroup of $\text{Gal}(L : K)$. For the converse suppose that $\text{Gal}(L : M)$ is a normal subgroup of $\text{Gal}(L : K)$. Let $\alpha \in M$. Then $\text{Gal}(L : M) \subseteq \text{Gal}(L : K(\alpha))$ and for each $\sigma \in \text{Gal}(L : K)$:

$$\text{Gal}(L : K(\sigma(\alpha))) = \sigma \text{Gal}(L : K(\alpha)) \sigma^{-1} \supseteq \sigma \text{Gal}(L : M) \sigma^{-1} = \text{Gal}(L : M).$$

So $\sigma(\alpha) \in M$ for all $\alpha \in M$ and all $\sigma \in \text{Gal}(L : K)$. Hence $M : K$ is a Galois extension. \square

For a Galois extension $L : K$ the groups $\text{Gal}(M : K)$ with $M \in \mathcal{F} = \mathcal{F}(L : K)$ form a projective system indexed by \mathcal{F} . The maps $f_{MN} : \text{Gal}(L : N) \rightarrow \text{Gal}(L : M)$ in this system are the restrictions of automorphisms to M .

19.73 Theorem. *Let $L : K$ be a Galois extension. Then the restrictions $\psi_M : \text{Gal}(L : K) \rightarrow \text{Gal}(M : K)$ of automorphisms induce a group isomorphism*

$$\psi : \text{Gal}(L : K) \xrightarrow{\sim} \varprojlim_{M \in \mathcal{F}} \text{Gal}(M : K).$$

PROOF. As a group homomorphism ψ is given by the definition of projective limit. We have

$$\text{Ker}(\psi) = \bigcap_{M \in \mathcal{F}} \text{Ker}(\psi_M) = \bigcap_{M \in \mathcal{F}} \text{Gal}(L : M).$$

The restriction of a $\sigma \in \text{Ker}(\psi)$ to an $M \in \mathcal{F}$ is the identity on M . Since $L = \bigcup_{M \in \mathcal{F}} M$, it follows that $\sigma = 1$. Hence ψ is injective. For a $(\sigma_M)_M \in \varprojlim_M \text{Gal}(M : K)$ define a $\sigma \in \text{Gal}(L : K)$ by

$$\sigma(\alpha) = \sigma_M(\alpha) \quad \text{if } \alpha \in M.$$

Thus σ is a well defined embedding of L in L . It is an isomorphism: the embedding given by $\alpha \mapsto \sigma_M^{-1}(\alpha)$ for $\alpha \in M$ is its inverse. \square

By Theorem 19.55 the Galois group of an infinite Galois extension is a profinite group. By Lemma 19.58 a base of its topology is the collection of the inverse images under ψ_M of automorphisms in $\text{Gal}(L : M)$, where $M \in \mathcal{F}$. Such an inverse image is a coset $\sigma \text{Gal}(L : M)$. This topology is known as the *Krull topology* of $\text{Gal}(L : K)$.

The Main Theorem of Galois Theory generalizes to general (possibly infinite) Galois extensions:

19.74 Theorem. *Let $L : K$ be a Galois extension and $G = \text{Gal}(L : K)$. Then we have a one-to-one correspondence*

intermediate fields of $L : K \quad \longleftrightarrow \quad$ closed subgroups of G

$$N \quad \longleftarrow \quad \text{Gal}(L : N)$$

$$L^H \quad \longleftarrow \quad H$$

PROOF. First we show that for intermediate fields N the groups $\text{Gal}(L : N)$ are closed. For $\alpha \in L$ choose an $M \in \mathcal{F}$ such that $\alpha \in M$. Then $\text{Gal}(L : M)$ is a subgroup of finite index of $\text{Gal}(L : K(\alpha))$. So $\text{Gal}(L : K(\alpha))$ is the union of finitely many cosets of $\text{Gal}(L : M)$. These cosets are open and closed. So also $\text{Gal}(L : K(\alpha))$ is open and closed. Let N be an intermediate field of $L : K$. Then $N = \bigcup_{\alpha \in N} K(\alpha)$ and so $\text{Gal}(L : N) = \bigcap_{\alpha \in N} \text{Gal}(L : K(\alpha))$, an intersection of closed subgroups.

For N an intermediate field by Proposition 19.65 $L : N$ is a Galois extension and so by Theorem 19.71 $N^{\text{Gal}(L:N)} = N$.

Let H be a subgroup of G . The extension $L : L^H$ is a Galois extension and its Galois group is a profinite group:

$$\text{Gal}(L : L^H) = \varprojlim_M \text{Gal}(L : L^M),$$

where $M \in \mathcal{F}(L : L^H)$. The map of H to $\text{Gal}(M : L^H)$ is surjective by the Main Theorem of Galois Theory for finite Galois extensions. Hence H is dense in $\text{Gal}(L : L^H)$. If H is closed, then $H = \text{Gal}(L : L^H)$. \square

19.75 Example. Let p be a prime number. For each $n \in \mathbb{N}^*$ there is a unique subfield \mathbb{F}_{p^n} of the algebraic closure $\overline{\mathbb{F}_p}$. We have

$$\text{Gal}(\overline{\mathbb{F}_p} : \mathbb{F}_p) = \varprojlim_n \text{Gal}(\mathbb{F}_{p^n} : \mathbb{F}_p) \xrightarrow{\sim} \varprojlim_n \mathbb{Z}/n = \hat{\mathbb{Z}}.$$

19.76 Example. Let \mathbb{Q}^{ab} be the union of the collection \mathcal{A} of all abelian number fields. They form a directed set. By the Kronecker-Weber Theorem the cyclotomic fields form a cofinal subset of \mathcal{A} . Hence

$$\text{Gal}(\mathbb{Q}^{\text{ab}} : \mathbb{Q}) = \varprojlim_{K \in \mathcal{A}} \text{Gal}(K : \mathbb{Q}) = \varprojlim_n \text{Gal}(\mathbb{Q}(\zeta_n) : \mathbb{Q}) \xrightarrow{\sim} \varprojlim_n (\mathbb{Z}/n)^* = \hat{\mathbb{Z}}^*.$$

19.77 Definitions and notations. Let \overline{K} be an algebraic closure of the field K . The *separable closure* of K (in \overline{K}) is the intermediate field

$$K^{\text{sep}} = \{ \alpha \in \overline{K} \mid \alpha \text{ is separable over } K \}.$$

The extension $K^{\text{sep}} : K$ is a Galois extension and its Galois group is called the *absolute Galois group* of K . Notation: $\text{Gal}(K) = \text{Gal}(K^{\text{sep}} : K)$. The collection $\mathcal{F}(\overline{K} : K) = \mathcal{F}(K^{\text{sep}} : K)$ is denoted by \mathcal{F}_K .

19.78 Example. Let K be a number field. Then $K^{\text{sep}} = \overline{K} = \overline{\mathbb{Q}}$ and

$$\text{Gal}(K) = \text{Gal}(\overline{\mathbb{Q}} : K) = \varprojlim_{L \in \mathcal{F}_K} \text{Gal}(L : K),$$

where \mathcal{F}_K is the collection of number fields L containing K and $L : K$ a Galois extension.

Abelian extensions are subfields of the separable closure.

19.79 Definition and notations. Let K be a field. The intermediate field of $K^{\text{sep}} : K$ corresponding to $\overline{\text{Gal}(K)'}^{\text{ab}}$ is denoted by K^{ab} . It is the maximal abelian extension of K . Clearly $\text{Gal}(K^{\text{ab}} : K) = \text{Gal}(K)^{\text{ab}}$. The collection $\mathcal{F}(K^{\text{ab}} : K)$ is denoted by \mathcal{A}_K .

19.80 Theorem. Let K be a field. For $L \in \mathcal{F}_K$ denote the subfield of L corresponding to $\text{Gal}(L : K)'$ by L' . Then

$$\text{Gal}(K^{\text{ab}} : K) = \varprojlim_{L \in \mathcal{A}_K} \text{Gal}(L : K) \quad \text{and} \quad \text{Gal}(K^{\text{ab}} : K) = \varprojlim_{L \in \mathcal{F}_K} \text{Gal}(L' : K).$$

PROOF. The first identity follows from Theorem 19.73 and the second from Proposition 19.63. \square

19.81 Example. For an abelian extension of number fields by Artin's Reciprocity Theorem we have isomorphisms

$$\mathcal{C}(L : K) := \mathcal{C}_{\mathfrak{f}}(L : K) \xrightarrow{\sim} \text{Gal}(L : K) \quad (\mathfrak{f} = \mathfrak{f}_K(L))$$

induced by the Artin maps $\varphi_K^{(L)} : \mathbb{I}^{\mathfrak{f}}(K) \rightarrow \text{Gal}(L : K)$. Thus we have an isomorphism of profinite groups

$$\varprojlim_{L \in \mathcal{A}_K} \mathcal{C}(L : K) \xrightarrow{\sim} \varprojlim_{L \in \mathcal{A}_K} \text{Gal}(L : K) = \text{Gal}(K^{\text{ab}} : K).$$

The class fields $K_{\mathcal{H}_m}$ for the groups $\mathcal{H}_m = \mathcal{H}_m(K)$ form a cofinal subset of \mathcal{A}_K :

$$\varprojlim_{\mathfrak{m}} \mathcal{C}_{\mathfrak{m}}(K) \xrightarrow{\sim} \varprojlim_{\mathfrak{m}} \text{Gal}(K_{\mathcal{H}_m} : K) = \text{Gal}(K^{\text{ab}} : K).$$

19.82 Example. Let F be a local field. In section 16.1 for each $E \in \mathcal{A}_F$ a local Artin map $\vartheta_F^{(E)} : F^* \rightarrow \text{Gal}(E : F)$ has been constructed. By the consistency property for these maps (Proposition 16.7(i)) they combine to a *local reciprocity map*

$$\vartheta_F : F^* \longrightarrow \varprojlim_{E \in \mathcal{A}_F} \text{Gal}(E : F) = \text{Gal}(F^{\text{ab}} : F).$$

19.6 Duality

Pontryagin duality is an equivalence of the category of abelian Hausdorff locally compact groups with its dual. The category of abelian torsion groups and the category of abelian profinite groups are both full subcategories of this category and by Pontryagin duality it follows that the first is equivalent to the dual of the second. In this section only this equivalence is constructed, not the full Pontryagin duality.

19.83 Notations. For G and H topological groups, the set of continuous homomorphisms of G to H is denoted by $\text{Hom}_{\text{cont}}(G, H)$. The category of all abelian discrete torsion groups is denoted by \mathcal{T} and the category of all abelian profinite groups with the continuous homomorphisms is denoted by \mathcal{P} . Both these categories are full subcategories of the category of abelian Hausdorff locally compact groups.

The group $\text{Hom}_{\text{cont}}(G, H)$ may be endowed with the *compact open topology*. A subbase for this topology consists of all subsets

$$V(K, U) = \{ f \in \text{Hom}_{\text{cont}}(G, H) \mid f(K) \subseteq U \},$$

where K is a compact subset of G and U an open subset of H . Since we will consider only special types of topological groups G and H , this generality is not needed here.

19.84 Definition. The *circle group* \mathbb{S}^1 is the group of complex numbers of norm 1 endowed with the topology relative to the standard topology of \mathbb{C} :

$$\mathbb{S}^1 = \{ z \in \mathbb{C} \mid |z| = 1 \}.$$

19.85 Lemma. Let $(A_i)_{i \in I}$ be an inductive system of finite abelian groups. Then $\varinjlim_{i \in I} A_i$ is an abelian torsion group.

PROOF. The inductive limit is a homomorphic image of the abelian torsion group $\bigoplus_{i \in I} A_i$. \square

Let $(A_i)_{i \in I}$ be an inductive system of finite abelian groups and

$$A = \varinjlim_{i \in I} A_i.$$

The homomorphisms $f_{ij}: A_i \rightarrow A_j$ induce homomorphisms $f_{ij}^\vee: A_j^\vee \rightarrow A_i^\vee$, thus forming a projective system $(A_i^\vee)_{i \in I}$.

19.86 Proposition. Let $(A_i)_{i \in I}$ be an inductive system of finite abelian groups and A the abelian torsion group $\varinjlim_{i \in I} A_i$. Then the homomorphisms $q_i: A_i \rightarrow A$ induce an isomorphism

$$\text{Hom}(A, \mathbb{S}^1) \xrightarrow{\sim} \varprojlim_{i \in I} A_i^\vee,$$

of abelian groups. In particular the group $\text{Hom}(A, \mathbb{S}^1)$ is a profinite group.

PROOF. By the definition of inductive limit we have

$$\text{Hom}(A, \mathbb{S}^1) = \text{Hom}\left(\varinjlim_{i \in I} A_i, \mathbb{S}^1\right) \xrightarrow{\sim} \varprojlim_{i \in I} \text{Hom}(A_i, \mathbb{S}^1) = \varprojlim_{i \in I} A_i^\vee. \quad \square$$

Similarly, if $(A_i)_{i \in I}$ is a projective system of finite abelian groups and

$$A = \varprojlim_{i \in I} A_i,$$

then the homomorphisms $f_{ij}: A_j \rightarrow A_i$ induce homomorphisms $f_{ij}^\vee: A_i^\vee \rightarrow A_j^\vee$.

19.87 Proposition. *Let $(A_i)_{i \in I}$ be an projective system of finite abelian groups and A the profinite group $\varprojlim_{i \in I} A_i$. Then the homomorphisms $p_i: A \rightarrow A_i$ induce an isomorphism*

$$\varinjlim_{i \in I} A_i^\vee \xrightarrow{\sim} \text{Hom}_{\text{cont}}(A, \mathbb{S}^1),$$

of abelian groups.

PROOF. The homomorphism $p_i: A \rightarrow A_i$ is continuous, so we have

$$\varinjlim_{i \in I} A_i^\vee = \varinjlim_{i \in I} \text{Hom}_{\text{cont}}(A_i, \mathbb{S}^1) \xrightarrow{\sim} \text{Hom}_{\text{cont}}\left(\varprojlim_{i \in I} A_i, \mathbb{S}^1\right) = \text{Hom}_{\text{cont}}(A, \mathbb{S}^1). \quad \square$$

19.88 Definition. Let A be either a discrete abelian torsion group or a profinite group. Then its *dual* A^\vee is a topological group with underlying group

$$A^\vee = \text{Hom}_{\text{cont}}(A, \mathbb{S}^1)$$

For A an abelian torsion group A^\vee is an abelian profinite group (Proposition 19.86) and for A profinite the group is a discrete abelian torsion group (Proposition 19.87). Taking the dual obviously is functorial.

Let A be a discrete abelian torsion group and \mathcal{F} the inductive set of finite subgroups of A . Then by the Propositions 19.86 and 19.87 we have functorial isomorphisms

$$A^{\vee\vee} \xrightarrow{\sim} \left(\varinjlim_{B \in \mathcal{F}} B^\vee\right)^\vee \xrightarrow{\sim} \varinjlim_{B \in \mathcal{F}} B^{\vee\vee}.$$

The functorial isomorphism

$$B \xrightarrow{\sim} B^{\vee\vee}, \quad b \mapsto (\chi \mapsto \chi(b))$$

for finite abelian groups B shows that for discrete abelian torsion groups A we have isomorphisms

$$\varepsilon_A: A \xrightarrow{\sim} A^{\vee\vee}, \quad a \mapsto (\chi \mapsto \chi(a)) \quad (19.1)$$

as well. Similarly, for A an abelian profinite group and \mathcal{N} the inductive set of subgroups of finite index we have by the same propositions

$$A^{\vee\vee} \xrightarrow{\sim} \left(\varinjlim_{B \in \mathcal{N}} (A/B)^\vee \right)^\vee \xrightarrow{\sim} \varprojlim_{B \in \mathcal{N}} (A/B)^{\vee\vee}.$$

So also for abelian profinite groups we have isomorphisms as given in (19.1). Thus, in categorical terms:

19.89 Theorem. *The functors*

$$\mathcal{P} \rightarrow \mathcal{T}^\circ, A \mapsto A^\vee \quad \text{and} \quad \mathcal{T} \rightarrow \mathcal{P}^\circ, A \mapsto A^\vee.$$

establish an equivalence of the categories \mathcal{P} and \mathcal{T}° . □

19.90 Example. For an abelian extension $L : K$ of number fields the Artin map induces an isomorphism

$$\varphi_K^{(L)} : \mathcal{C}(L : K) \xrightarrow{\sim} \text{Gal}(L : K).$$

By the consistency property for these maps they induce an isomorphism on the projective limits:

$$\varphi_K : \varprojlim_{L \in \mathcal{A}_K} \mathcal{C}(L : K) \xrightarrow{\sim} \varprojlim_{L \in \mathcal{A}_K} \text{Gal}(L : K) = \text{Gal}(K^{\text{ab}} : K).$$

Since the class fields $K_{\mathcal{H}_m(K)}$ form a cofinal subset of \mathcal{A}_K , another description is

$$\varphi_K : \varprojlim_{\mathfrak{m}} \mathcal{C}_{\mathfrak{m}}(K) \xrightarrow{\sim} \text{Gal}(K^{\text{ab}} : K).$$

The group $\mathcal{H}_m(K)$ is the dual of $\mathcal{C}_m(K)$. Therefore, the group $\mathcal{H}(K)$ is the dual of the profinite group $\varprojlim_{\mathfrak{m}} \mathcal{C}_m(K)$ and the dual Artin maps induce an isomorphism

$$\check{\varphi}_K : \text{Gal}(K^{\text{ab}} : K)^\vee \xrightarrow{\sim} \mathcal{H}(K).$$

In the last chapter the ‘idèle class group’ $\mathcal{C}(K)$ will be constructed and a reciprocity map

$$\vartheta_K : \mathcal{C}(K) \rightarrow \text{Gal}(K^{\text{ab}} : K)$$

which has properties similar to those of the local reciprocity map

$$\vartheta_F : F^* \rightarrow \text{Gal}(F^{\text{ab}} : F)$$

for a local field F . As shown in the last chapter, the idèle approach to class field theory yields a firm link between the local and global reciprocity maps.

EXERCISES

1. (i) Prove that a totally separated topological space is totally disconnected.
 (ii) Prove the converse of (i) for locally compact Hausdorff spaces.
 (iii) A space which is totally disconnected but not totally separated is the so-called *Cantor teepee*, which is the *Krasner-Kuratowski fan* with the top deleted. Do an internet search for a description of this space and verify.
2. For $n \in \mathbb{N}^*$ we have by the Chinese Remainder Theorem isomorphisms

$$\mathbb{Z}/n \xrightarrow{\sim} \prod_p (\mathbb{Z}/p^{v_p(n)}) \quad \text{and} \quad (\mathbb{Z}/n)^* \xrightarrow{\sim} \prod_p (\mathbb{Z}/p^{v_p(n)})^*,$$

where the product is over all prime numbers p . Show that in the limit (the projective limit) we have

$$\hat{\mathbb{Z}} \xrightarrow{\sim} \prod_p \mathbb{Z}_p \quad \text{and} \quad \hat{\mathbb{Z}}^* \xrightarrow{\sim} \prod_p \mathbb{Z}_p^*,$$

isomorphisms of profinite groups.

3. (i) Let $1 \rightarrow A \rightarrow B \rightarrow C \rightarrow 1$ be a short exact sequence of abelian torsion groups. Show that $1 \rightarrow C^\vee \rightarrow B^\vee \rightarrow A^\vee \rightarrow 1$ is a short exact sequence of abelian profinite groups.
 (ii) Let $1 \rightarrow A \rightarrow B \rightarrow C \rightarrow 1$ be a short exact sequence of abelian profinite groups. Show that $1 \rightarrow C^\vee \rightarrow B^\vee \rightarrow A^\vee \rightarrow 1$ is a short exact sequence of abelian torsion groups.
 (iii) Let A be an abelian torsion group. Establish a correspondence between subgroups of A and closed subgroups of the profinite group A^\vee .
4. Let K be a number field. Show that abelian extensions of K (inside $\overline{\mathbb{Q}}$) correspond to subgroups of $\mathcal{H}(K)$.

20 Idèlic Class Field Theory

Chevalley introduced the idèle group of a number field for a global class field theory of infinite abelian extensions. Some years later he used this for constructing global class field theory from local class field theory. In this theory all primes of a number field are considered simultaneously. The basic notions are given in the first two sections. Some topological algebra as described in the previous chapter is needed here. Of particular importance is the idèle class group of a number field. Its role is similar to the role of the multiplicative group in local class field theory. In section 20.3 the relation to ray class groups is described and in section 20.4 the idèlic global classification theorem is derived from the classification theorem of chapter 15. Finally the close connection between local reciprocity and the idèlic global reciprocity is given in section 20.5.

20.1 The adèle ring of a number field

In chapter 1 we embedded a number field K in the \mathbb{R} -algebra $\mathbb{R} \otimes_{\mathbb{Q}} K = \mathbb{R}^{r(K)} \times \mathbb{C}^{s(K)} = \prod_{\mathfrak{p} \in \mathcal{P}_{\infty}(K)} K_{\mathfrak{p}}$ and in chapter 5 it is shown that the subring \mathcal{O}_K maps under this embedding to a lattice Λ_K : a discrete subring of the \mathbb{R} -algebra and the quotient is a compact abelian group. In this section the field K will be embedded in a locally compact ring $\mathbb{A}(K)$ such that (the image of) K itself is a discrete subring of $\mathbb{A}(K)$ with compact quotient group $\mathbb{A}(K)/K$.

20.1 Definition. Let S be a finite saturated collection of primes of K . Then the topological ring

$$\mathbb{A}^S(K) = \prod_{\mathfrak{p} \in S} K_{\mathfrak{p}} \times \prod_{\mathfrak{p} \notin S} \mathcal{O}_{\mathfrak{p}}$$

is called the *ring of S -adèles* of K . (Its topology is the product topology.)

For S_{∞} we have

$$\mathbb{A}^{S_{\infty}}(K) = \prod_{\mathfrak{p} | \infty} K_{\mathfrak{p}} \times \prod_{\mathfrak{p} \nmid \infty} \mathcal{O}_{\mathfrak{p}}.$$

Here ∞ stands for the modulus of K induced by the modulus ∞ of \mathbb{Q} .

20.2 Lemma. *The ring $\mathbb{A}^S(K)$ of S -adèles of K is locally compact.*

PROOF. The completions $K_{\mathfrak{p}}$ are locally compact and so is a finite product of them. For finite \mathfrak{p} the rings $\mathcal{O}_{\mathfrak{p}}$ are compact and by Tykhonov's Theorem (Theorem 19.7) an infinite product of these rings is compact as well. \square

The finite saturated collections of primes form a directed set under inclusion. For $S \subseteq T$ we have an inclusion map $\mathbb{A}^S(K) \rightarrow \mathbb{A}^T(K)$:

$$\prod_{\mathfrak{p} \in S} K_{\mathfrak{p}} \times \prod_{\mathfrak{p} \in T \setminus S} \mathcal{O}_{\mathfrak{p}} \times \prod_{\mathfrak{p} \notin T} \mathcal{O}_{\mathfrak{p}} \xrightarrow{\subseteq} \prod_{\mathfrak{p} \in S} K_{\mathfrak{p}} \times \prod_{\mathfrak{p} \in T \setminus S} K_{\mathfrak{p}} \times \prod_{\mathfrak{p} \notin T} \mathcal{O}_{\mathfrak{p}}.$$

We take the direct limit.

20.3 Definition. The *adèle ring* of K is the topological ring

$$\mathbb{A}(K) = \varinjlim_S \mathbb{A}^S(K) = \bigcup_S \mathbb{A}^S(K),$$

the limit taken over the finite saturated collections of primes of K .

So

$$\mathbb{A}(K) = \left\{ (\alpha_{\mathfrak{p}})_{\mathfrak{p}} \in \prod_{\mathfrak{p}} K_{\mathfrak{p}} \mid \alpha_{\mathfrak{p}} \notin \mathcal{O}_{\mathfrak{p}} \text{ for only finitely many finite primes } \mathfrak{p} \right\}.$$

It's also called the *restricted product* of the groups $K_{\mathfrak{p}}$. Notation:

$$\mathbb{A}(K) = \prod_{\mathfrak{p}} K_{\mathfrak{p}}.$$

20.4 Lemma. *For each finite saturated collection S of primes of K the ring $\mathbb{A}^S(K)$ of S -adèles is open in $\mathbb{A}(K)$.*

PROOF. A subset of $\mathbb{A}(K)$ is open if and only if its intersection with $\mathbb{A}^T(K)$ is open in $\mathbb{A}^T(K)$ for each saturated collection T of primes. Let S and T be saturated collections of primes. Then $\mathbb{A}^S(K) \cap \mathbb{A}^T(K) = \mathbb{A}^{S \cap T}(K)$ and this is open in $\mathbb{A}^T(K)$. \square

20.5 Lemma. *The topological ring $\mathbb{A}(K)$ is locally compact.*

PROOF. This follows from Lemma 20.2 and Lemma 20.4. \square

For each $\alpha \in K$ we have $\alpha \notin \mathcal{O}_{\mathfrak{p}}$ for only a finite number of finite primes \mathfrak{p} . So $\alpha \mapsto (\alpha)_{\mathfrak{p}}$ is an embedding of the field K in the adèle ring $\mathbb{A}(K)$. We thus view K as a subring of $\mathbb{A}(K)$.

Be careful with the meaning of the notations: in the notation $(\alpha)_{\mathfrak{p}}$ for $\alpha \in K$ we already considered K as a subfield of $K_{\mathfrak{p}}$ and this so for every \mathfrak{p} . So we have many incompatible identifications. The embedding $K \rightarrow \mathbb{A}(K)$ projects to $K \rightarrow \prod_{\mathfrak{p}|\infty} K_{\mathfrak{p}}$ and this is the embedding $\iota: K \rightarrow \mathbb{R}^r \times \mathbb{C}^s$ described in section 1.1, which we did not define by $\iota(\alpha) = (\alpha, \dots, \alpha)$. There we used the convention that number fields are subfields of \mathbb{C} . Later, in chapter 10 on completions we often considered number fields as subfields of other fields, in particular of their completions.

20.6 Proposition. K is discrete in $\mathbb{A}(K)$.

PROOF. The set

$$\{(\alpha_{\mathfrak{p}})_{\mathfrak{p}} \mid \|\alpha_{\mathfrak{p}}\|_{\mathfrak{p}} < 1\}$$

is open in each $\mathbb{A}^S(K)$ and therefore also in $\mathbb{A}(K)$. The product formula (Proposition 10.24), $\prod_{\mathfrak{p}} \|\alpha\|_{\mathfrak{p}} = 1$ for all $\alpha \in K^*$, implies that 0 is the only element of K in this open set. \square

20.7 Proposition. $\mathbb{A}(K) = K + \mathbb{A}^{S\infty}(K)$.

PROOF. Let $\alpha = (\alpha_{\mathfrak{p}})_{\mathfrak{p}}$ be a nonzero element of $\mathbb{A}(K)$. Take $m \in \mathbb{N}^*$ such that $m\alpha_{\mathfrak{p}} \in \mathcal{O}_{\mathfrak{p}}$ for all finite primes of K . Let S be the collection of finite primes \mathfrak{p} of K with $v_{\mathfrak{p}}(m) > 0$. Let $N \in \mathbb{N}^*$ such that $N \geq v_{\mathfrak{p}}(m)$ for each $\mathfrak{p} \in S$. Take for each $\mathfrak{p} \in S$ a $\beta_{\mathfrak{p}} \in \mathcal{O}_K$ such that $\beta_{\mathfrak{p}} \equiv m\alpha_{\mathfrak{p}} \pmod{\mathfrak{p}^N}$. By the Chinese remainder theorem there is a $\gamma \in \mathcal{O}_K$ such that

$$\gamma \equiv \beta_{\mathfrak{p}} \pmod{\mathfrak{p}^N} \quad \text{for all } \mathfrak{p} \in S.$$

Then for each $\mathfrak{p} \in S$

$$v_{\mathfrak{p}}\left(\frac{\gamma}{m} - \alpha_{\mathfrak{p}}\right) = v_{\mathfrak{p}}(\gamma - m\alpha_{\mathfrak{p}}) - v_{\mathfrak{p}}(m) = v_{\mathfrak{p}}(\gamma - \beta_{\mathfrak{p}}) - v_{\mathfrak{p}}(m) \geq N - N = 0$$

and for each finite prime $\mathfrak{q} \notin S$

$$v_{\mathfrak{q}}\left(\frac{\gamma}{m} - \alpha_{\mathfrak{q}}\right) = v_{\mathfrak{q}}(\gamma - m\alpha_{\mathfrak{q}}) \geq 0.$$

Hence $\frac{\gamma}{m} - \alpha \in \mathbb{A}^{S\infty}(K)$. It follows that $\mathbb{A}(K) \subseteq K + \mathbb{A}^{S\infty}(K)$. \square

20.8 Theorem. The additive topological group $\mathbb{A}(K)/K$ is compact. A fundamental domain in $\mathbb{A}(K)$ for $\mathbb{A}(K)/K$ is

$$F \times \prod_{\mathfrak{p} \nmid \infty} \mathcal{O}_{\mathfrak{p}},$$

where F is a fundamental parallelopete for the lattice Λ_K in \mathbb{R}^n (as defined on page 108).

PROOF. Because $K \cap \mathbb{A}^{S\infty}(K) = \mathcal{O}_K$, by Proposition 20.7 the inclusion $\mathbb{A}^{S\infty} \subset \mathbb{A}(K)$ induces an isomorphism

$$\mathbb{A}^{S\infty}(K)/\mathcal{O}_K \xrightarrow{\sim} \mathbb{A}(K)/K.$$

The ker-coker sequence of

$$\begin{array}{ccc} \mathcal{O}_K & \longrightarrow & \mathbb{A}^{S_\infty}(K) \\ & \searrow & \swarrow \\ & \prod_{\mathfrak{p}|\infty} K_{\mathfrak{p}} & \end{array}$$

reduces to

$$0 \longrightarrow \prod_{\mathfrak{p}|\infty} \mathcal{O}_{\mathfrak{p}} \longrightarrow \mathbb{A}^{S_\infty}(K)/\mathcal{O}_K \longrightarrow \mathbb{R}^n/\Lambda_K \longrightarrow 0$$

and from this the theorem easily follows. □

20.2 The idèle group and the idèle class group

Again we fix a number field K . The idèle group of K is the unit group of its adèle ring. It is a topological group.

20.9 Definition. Let S be a finite saturated collection of primes of K . The topological group of S -idèles of K is

$$\mathbb{J}^S(K) = \mathbb{A}^S(K)^* = \prod_{\mathfrak{p} \in S} K_{\mathfrak{p}}^* \times \prod_{\mathfrak{p} \notin S} \mathcal{O}_{\mathfrak{p}}^*$$

endowed with the product topology. The idèle group of K , denoted by $\mathbb{J}(K)$, is the injective limit of the groups of S -idèles:

$$\begin{aligned} \mathbb{J}(K) &= \varinjlim_S \mathbb{J}^S(K) = \bigcup_S \mathbb{J}^S(K) \\ &= \left\{ (\alpha_{\mathfrak{p}})_{\mathfrak{p}} \in \prod_{\mathfrak{p}} K_{\mathfrak{p}}^* \mid \alpha_{\mathfrak{p}} \notin \mathcal{O}_{\mathfrak{p}}^* \text{ for only finitely many finite primes } \mathfrak{p} \right\} \\ &= \mathbb{A}(K)^* = \prod_{\mathfrak{p}} K_{\mathfrak{p}}^*, \end{aligned}$$

the restricted product in analogy to the one used for the adèle ring.

The topology of $\mathbb{J}(K)$ is not the topology induced by the inclusion $\mathbb{J}(K) \subset \mathbb{A}(K)$. In the induced topology inversion is in this case not continuous. In general for the topology on the unit group of a topological ring R one takes the topology induced by the injective map $R^* \rightarrow R \times R, x \mapsto (x, x^{-1})$.

As for the adèle ring we have for the idèle group:

20.10 Lemma. *For each finite saturated collection S of primes of K the group $\mathbb{J}^S(K)$ is open in $\mathbb{J}(K)$.* \square

The embedding $K \rightarrow \mathbb{A}(K)$ restricts to an embedding $K^* \rightarrow \mathbb{J}(K)$ and we will view K^* as a subgroup of $\mathbb{J}(K)$. Clearly, $K^* \cap \mathbb{J}^{S_\infty}(K) = \mathcal{O}_K^*$ and more generally for S a finite saturated collection of primes $K^* \cap \mathbb{J}^S(K) = K^S$, the group of S -units.

20.11 Proposition. *K^* is discrete in $\mathbb{J}(K)$.*

PROOF. The set

$$\{ (\alpha_p)_p \in \mathbb{J}(K) \mid \|\alpha_p - 1\|_p < 1 \}$$

is open in $\mathbb{J}(K)$, because its intersection with $\mathbb{J}^S(K)$ is open in each $\mathbb{J}^S(K)$. Again by the product formula, $\prod_p \|\alpha - 1\|_p = 1$ for all $\alpha \in K \setminus \{1\}$, the only element of K^* in the open set is 1. \square

20.12 Definition. The group $\mathbb{J}(K)/K^*$ is called the *idèle class group* of K and is denoted by $\mathcal{C}(K)$. For S a finite saturated collection of primes of K the group $\mathbb{J}^S(K)/K^S$ is called *S -idèle class group* of K . The S -idèle class group is denoted by $\mathcal{C}^S(K)$.

There is a natural map from the idèle group to the group of fractional ideals. This map will be the link between the idèle and the ideal approach to class field theory. This will be made concrete in the next section. Here we show that the ideal class group is a homomorphic image of the idèle class group.

20.13 Notation. For $\alpha = (\alpha_p)_p \in \mathbb{J}(K)$ we write

$$(\alpha) = \prod_{p \nmid \infty} \mathfrak{p}^{v_p(\alpha_p)} \in \mathbb{I}(K).$$

Thus we have a group homomorphism

$$(\cdot): \mathbb{J}(K) \rightarrow \mathbb{I}(K), \alpha \mapsto (\alpha)$$

and for $\alpha \in K^*$ the notation (α) stands for the principal fractional ideal $\alpha\mathcal{O}_K$. This homomorphism is clearly surjective and its kernel is $\mathbb{J}^{S_\infty}(K)$, an open subgroup of $\mathbb{J}(K)$. The subgroup K^* of $\mathbb{J}(K)$ maps to $\mathbb{P}(K)$, the group of principal fractional ideals. So we proved:

20.14 Proposition. *The homomorphism $(\cdot): \mathbb{J}(K) \rightarrow \mathbb{I}(K)$ induces an isomorphism*

$$\mathbb{J}(K)/K^*\mathbb{J}^{S_\infty}(K) \xrightarrow{\sim} \mathcal{C}(K). \quad \square$$

In the next section we will show that not only the ideal class group is a homomorphic image of the idèle class group, but so is every ray class group.

The absolute values on the various completions on a number field give rise to a continuous group homomorphism from the idèle class group to the positive reals.

20.15 Definition. Let $\alpha = (\alpha_{\mathfrak{p}})_{\mathfrak{p}} \in \mathbb{J}(K)$. The \mathfrak{p} -value $\|\alpha\|_{\mathfrak{p}}$ of α is defined to be the absolute value of $\alpha_{\mathfrak{p}} \in K_{\mathfrak{p}}$:

$$\|\alpha\|_{\mathfrak{p}} = \|\alpha_{\mathfrak{p}}\|_{\mathfrak{p}}.$$

The *content* $\|\alpha\|$ of α is the product of its \mathfrak{p} -values:

$$\|\alpha\| = \prod_{\mathfrak{p}} \|\alpha\|_{\mathfrak{p}}.$$

The product is well defined since $\|\alpha\|_{\mathfrak{p}} \neq 1$ for only finitely many \mathfrak{p} .

20.16 Lemma. *The map $\mathbb{J}(K) \rightarrow \mathbb{R}^{>0}$, $\alpha \mapsto \|\alpha\|$ is a surjective continuous group homomorphism.*

PROOF. It clearly is a group homomorphism. For surjectivity take for each $a \in \mathbb{R}^{>0}$ an element $b \in K_{\mathfrak{p}}^*$ for one of the infinite primes such that $\|b\|_{\mathfrak{p}} = a$. Then $\alpha \in \mathbb{J}(K)$ defined by $\alpha_{\mathfrak{p}} = b$ and $\alpha_{\mathfrak{q}} = 1$ for all $\mathfrak{q} \neq \mathfrak{p}$ satisfies $\|\alpha\| = a$. Continuity: for $(1 - \varepsilon, 1 + \varepsilon) \subset \mathbb{R}^{>0}$ take for each $\mathfrak{p} \mid \infty$ the open neighborhood

$$U_{\mathfrak{p}} = \{ \alpha_{\mathfrak{p}} \mid \|\alpha_{\mathfrak{p}} - 1\|_{\mathfrak{p}} < \sqrt[n]{\varepsilon} \}$$

of $1 \in K_{\mathfrak{p}}$. Then the image of the open set $\prod_{\mathfrak{p} \mid \infty} U_{\mathfrak{p}} \times \prod_{\mathfrak{p} \nmid \infty} \mathcal{O}_{\mathfrak{p}}^*$ is contained in $(1 - \varepsilon, 1 + \varepsilon)$. □

20.17 Notation. The kernel of the map $\mathbb{J}(K) \rightarrow \mathbb{R}^{>0}$, $\alpha \mapsto \|\alpha\|$ is denoted by $\mathbb{J}_0(K)$. The product formula, $\prod_{\mathfrak{p}} \|\alpha\|_{\mathfrak{p}} = 1$ for $\alpha \in K^*$, implies that the map induces a surjective continuous homomorphism $\mathcal{C}(K) \rightarrow \mathbb{R}^{>0}$. The kernel of this map is denoted by $\mathcal{C}_0(K)$. Thus K^* is a closed subgroup of $\mathbb{J}_0(K)$ and $\mathbb{J}_0(K)/K^* = \mathcal{C}_0(K)$.

We will show that the group $\mathcal{C}_0(K)$ is compact. The proof uses the following generalization of Proposition 5.31.

20.18 Proposition. *Let for each prime \mathfrak{p} of K be given a $c_{\mathfrak{p}} \in \mathbb{R}^{>0}$ such that $c_{\mathfrak{p}} \neq 1$ for only finitely many primes \mathfrak{p} and*

$$\prod_{\mathfrak{p}} c_{\mathfrak{p}} \geq \left(\frac{2}{\pi}\right)^{s(K)} \sqrt{|\text{disc}(K)|}.$$

Then there exists a $\beta \in K^$ such that*

$$\|\beta\|_{\mathfrak{p}} \leq c_{\mathfrak{p}} \quad \text{for all primes } \mathfrak{p} \text{ of } K.$$

PROOF. For each finite prime \mathfrak{p} let $k_{\mathfrak{p}}$ be the unique integer such that

$$N(\mathfrak{p})^{-(k_{\mathfrak{p}}+1)} < c_{\mathfrak{p}} \leq N(\mathfrak{p})^{-k_{\mathfrak{p}}}.$$

Then $k_{\mathfrak{p}} = 0$ if and only if $c_{\mathfrak{p}} = 1$, so in particular $k_{\mathfrak{p}} \neq 0$ for only finitely many \mathfrak{p} . Put $\mathfrak{a} = \prod_{\mathfrak{p} \neq \infty} \mathfrak{p}^{-k_{\mathfrak{p}}} \in \mathbb{I}(K)$. By Proposition 2.28 there exists a $\mathfrak{b} \in \mathbb{I}^+(K)$ such that $\mathfrak{a}\mathfrak{b}$ is a principal fractional ideal and $v_{\mathfrak{p}}(\mathfrak{b}) = 0$ for each finite prime \mathfrak{p} satisfying $k_{\mathfrak{p}} \neq 0$. Let $\gamma \in K^*$ be such that $\mathfrak{a}\mathfrak{b} = \gamma\mathcal{O}_K$. For each prime \mathfrak{p} put $d_{\mathfrak{p}} = c_{\mathfrak{p}}\|\gamma\|_{\mathfrak{p}}$. Then for finite \mathfrak{p} with $k_{\mathfrak{p}} = 0$

$$d_{\mathfrak{p}} = \|\gamma\|_{\mathfrak{p}} = N(\mathfrak{p})^{-v_{\mathfrak{p}}(\mathfrak{b})} \leq 1$$

and for finite \mathfrak{p} with $k_{\mathfrak{p}} \neq 0$

$$d_{\mathfrak{p}} = c_{\mathfrak{p}}N(\mathfrak{p})^{-v_{\mathfrak{p}}(\mathfrak{a})} = c_{\mathfrak{p}}N(\mathfrak{p})^{k_{\mathfrak{p}}} \leq 1.$$

Hence $d_{\mathfrak{p}} \leq 1$ for all finite \mathfrak{p} and therefore

$$\prod_{\mathfrak{p}|\infty} d_{\mathfrak{p}} \geq \prod_{\mathfrak{p}} d_{\mathfrak{p}} = \prod_{\mathfrak{p}} c_{\mathfrak{p}}\|\gamma\|_{\mathfrak{p}} = \prod_{\mathfrak{p}} c_{\mathfrak{p}} \geq \left(\frac{2}{\pi}\right)^{s(K)} \sqrt{|\text{disc}(K)|}.$$

By Proposition 5.31 there exists a nonzero $\delta \in \mathcal{O}_K$ such that $\|\delta\|_{\mathfrak{p}} \leq d_{\mathfrak{p}}$ for all infinite \mathfrak{p} . Since $\delta \in \mathcal{O}_K$ we also have $\|\delta\|_{\mathfrak{p}} \leq 1 = d_{\mathfrak{p}}$ for all finite \mathfrak{p} . Take $\beta = \delta\gamma^{-1}$. Then for all primes \mathfrak{p} of K

$$\|\beta\|_{\mathfrak{p}} = \frac{\|\delta\|_{\mathfrak{p}}}{\|\gamma\|_{\mathfrak{p}}} \leq \frac{d_{\mathfrak{p}}}{\|\gamma\|_{\mathfrak{p}}} = c_{\mathfrak{p}}. \quad \square$$

20.19 Theorem. *The topological group $\mathcal{C}_0(K)$ is compact.*

PROOF. The group $\mathcal{C}_0(K)$ is the kernel of the surjective continuous homomorphism

$$\mathcal{C}(K) \rightarrow \mathbb{R}^{>0}, \quad \bar{\alpha} \mapsto \|\alpha\| \quad (\text{for } \alpha \in \mathbb{J}(K)).$$

The subgroup $\mathcal{C}_0(K)$ is homeomorphic to each of its cosets. So it suffices to prove that it has a compact coset. Cosets are the subsets

$$Y_{\rho} = \{ \bar{\alpha} \mid \alpha \in \mathbb{J}(K) \text{ and } \|\alpha\| = \rho \}$$

of $\mathcal{C}(K)$, where $\rho \in \mathbb{R}^{>0}$. Let $\rho \geq \left(\frac{2}{\pi}\right)^{s(K)} \sqrt{|\text{disc}(K)|}$. We show that Y_{ρ} is compact. For each prime \mathfrak{p} the subset

$$X_{\mathfrak{p}} = \{ \alpha \in K_{\mathfrak{p}} \mid 1 \leq \|\alpha\|_{\mathfrak{p}} \leq \rho \}$$

of $K_{\mathfrak{p}}^*$ is compact. There are only finitely many finite primes \mathfrak{p} of K for which $N(\mathfrak{p}) < \rho$. Let S be the collection of these primes together with the infinite primes.

It is a finite saturated collection of primes of K . For $\mathfrak{p} \notin S$ we have $X_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}^*$. Hence the set

$$X = \prod_{\mathfrak{p}} X_{\mathfrak{p}}$$

is a subset of $\mathbb{J}^S(K)$. It is compact, since all factors are compact. Let $\bar{\alpha} \in Y_{\rho}$, where $\alpha \in \mathbb{J}(K)$ with $\|\alpha\| = \prod_{\mathfrak{p}} \|\alpha\|_{\mathfrak{p}} = \rho$. By Proposition 20.18 there is a $\beta \in K^*$ such that

$$\|\beta\|_{\mathfrak{p}} \leq \|\alpha\|_{\mathfrak{p}} \quad \text{for all primes } \mathfrak{p} \text{ of } K.$$

So $\|\frac{\alpha}{\beta}\|_{\mathfrak{p}} \geq 1$ for all primes \mathfrak{p} . Since $\prod_{\mathfrak{p}} \|\frac{\alpha}{\beta}\|_{\mathfrak{p}} = \prod_{\mathfrak{p}} \|\alpha\|_{\mathfrak{p}} = \rho$, we have $\|\frac{\alpha}{\beta}\|_{\mathfrak{p}} \leq \rho$ for each prime \mathfrak{p} . Hence $\frac{\alpha}{\beta} \in X$. It follows that the closed subset Y_{ρ} of $\mathcal{C}(K)$ is contained in the image of X under the canonical projection $\mathbb{J}(K) \rightarrow \mathcal{C}(K)$. Since X is compact, this image is compact and so is Y_{ρ} . \square

20.3 Idèle class groups and moduli

In idèlic class field theory the role of the idèle class group is similar to the role of the multiplicative group of a local field in local class field theory.

20.20 Lemma. *Let \mathfrak{p} be a prime of K . A subgroup of $K_{\mathfrak{p}}^*$ is open if and only if it contains $U_{\mathfrak{p}}^{(n)}$ for some $n \in \mathbb{N}^*$.*

PROOF. The only open subgroup of \mathbb{C}^* is \mathbb{C}^* itself. The group \mathbb{R}^* has two open subgroups: \mathbb{R}^* and $\mathbb{R}^{>0}$. For \mathfrak{p} finite the cosets of all $U_{\mathfrak{p}}^{(n)}$ form a basis for the topology. So an open subgroup of $K_{\mathfrak{p}}^*$ must contain $U_{\mathfrak{p}}^{(n)}$ for some $n \in \mathbb{N}^*$. And if a subgroup contains an open subgroup, then it is the union of cosets of this open subgroup and so it is open as well. \square

20.21 Definitions and notations. Let \mathfrak{m} be a modulus of K . The subgroup $W_{\mathfrak{m}}(K)$ of $\mathbb{J}(K)$ is defined as follows:

$$W_{\mathfrak{m}}(K) = \prod_{\mathfrak{p}} U_{\mathfrak{p}}^{(v_{\mathfrak{p}}(\mathfrak{m}))}$$

The cokernel of $W_{\mathfrak{m}}(K) \rightarrow \mathbb{J}(K)/K^*(= \mathcal{C}(K))$ is called the *idèle class group modulo \mathfrak{m}* of K and is denoted by $\mathcal{C}_{\mathfrak{m}}(K)$:

$$\mathcal{C}_{\mathfrak{m}}(K) = \mathbb{J}(K)/W_{\mathfrak{m}}(K)K^*.$$

20.22 Lemma. *The groups $W_{\mathfrak{m}}(K)$ are open subgroups of $\mathbb{J}(K)$.*

PROOF. The subgroup $W_{\mathfrak{m}_{\infty}}(K)$ of $W_{\mathfrak{m}}(K)$ is open in $\mathbb{J}(K)$ since it is open in $\mathbb{J}^S(K)$ for each finite saturated collection S of primes of K . Therefore, $W_{\mathfrak{m}}(K)$ is open. \square

20.23 Proposition. *A subgroup of $\mathbb{J}(K)$ is open if and only if it contains a $W_{\mathfrak{m}}(K)$ for some modulus \mathfrak{m} of K .*

PROOF. If a subgroup of $\mathbb{J}(K)$ contains a $W_{\mathfrak{m}}(K)$, then it is open because $W_{\mathfrak{m}}(K)$ is. Conversely, if H is an open subgroup of $\mathbb{J}(K)$, then $H \cap \mathbb{J}^{S_\infty}(K)$ is an open subgroup of $\mathbb{J}^{S_\infty}(K)$, which is an infinite product and by definition of the product topology and Lemma 20.20 it follows that it must contain a group $W_{\mathfrak{m}}(K)$. \square

We will show that the idèle class group modulo a modulus \mathfrak{m} , $\mathcal{C}_{\mathfrak{m}}(K)$, is in a natural way isomorphic to the ray class group $\mathcal{C}_{\mathfrak{m}}^1(K)$ defined in chapter 13 (Definitions and notations 13.1).

20.24 Definition. Let \mathfrak{m} be a modulus of K . A subgroup $\mathbb{J}^{\mathfrak{m}}(K)$ of $\mathbb{J}(K)$ is defined as follows

$$\mathbb{J}^{\mathfrak{m}}(K) = \left\{ \alpha \in \mathbb{J}(K) \mid \alpha_{\mathfrak{p}} \in U_{\mathfrak{p}}^{(v_{\mathfrak{p}}(\mathfrak{m}))} \text{ for } \mathfrak{p} \mid \mathfrak{m} \right\} = \prod_{\mathfrak{p} \mid \mathfrak{m}} U_{\mathfrak{p}}^{(v_{\mathfrak{p}}(\mathfrak{m}))} \times \prod_{\mathfrak{p} \nmid \mathfrak{m}} K_{\mathfrak{p}}^*.$$

Restriction of the map $(\cdot): \mathbb{J}(K) \rightarrow \mathbb{I}(K)$ to $\mathbb{J}^{\mathfrak{m}}(K)$ yields a surjective homomorphism $(\cdot): \mathbb{J}^{\mathfrak{m}}(K) \rightarrow \mathbb{I}^{\mathfrak{m}}(K)$. By the definitions of $W_{\mathfrak{m}}(K)$ and $\mathbb{J}^{\mathfrak{m}}(K)$ we obviously have

$$W_{\mathfrak{m}}(K) = \text{Ker}(\mathbb{J}^{\mathfrak{m}}(K) \xrightarrow{(\cdot)} \mathbb{I}^{\mathfrak{m}}(K)).$$

For any modulus \mathfrak{m} each idèle class is represented by an idèle in $\mathbb{J}^{\mathfrak{m}}(K)$:

20.25 Lemma. *For any modulus \mathfrak{m} of K we have*

$$\mathbb{J}(K) = \mathbb{J}^{\mathfrak{m}}(K)K^* \quad \text{and} \quad \mathbb{J}^{\mathfrak{m}} \cap K^* = K_{\mathfrak{m}}^1.$$

PROOF. By the definitions of $\mathbb{J}^{\mathfrak{m}}(K)$ and $K_{\mathfrak{m}}^1$ it is immediate that $\mathbb{J}^{\mathfrak{m}} \cap K^* = K_{\mathfrak{m}}^1$. Let $\alpha \in \mathbb{J}(K)$. For each $\mathfrak{p} \mid \mathfrak{m}$ choose a $\beta_{\mathfrak{p}} \in K^*$ such that $\beta_{\mathfrak{p}} \equiv \alpha_{\mathfrak{p}} \pmod{U_{\mathfrak{p}}^{(v_{\mathfrak{p}}(\mathfrak{m}))}}$. Since the system $\mathfrak{m} \mapsto K^*/K_{\mathfrak{m}}^1$ is multiplicative, there is a $\beta \in K^*$ such that $\beta \equiv \beta_{\mathfrak{p}} \pmod{K_{\mathfrak{p}}^1(v_{\mathfrak{p}}(\mathfrak{m}))}$ for all $\mathfrak{p} \mid \mathfrak{m}$. Then $\beta \equiv \alpha_{\mathfrak{p}} \pmod{U_{\mathfrak{p}}^{(v_{\mathfrak{p}}(\mathfrak{m}))}}$ and so $\beta^{-1}\alpha \in \mathbb{J}^{\mathfrak{m}}(K)$. \square

20.26 Lemma. *For any modulus \mathfrak{m} of K the inclusion map $\mathbb{J}^{\mathfrak{m}}(K) \rightarrow \mathbb{J}(K)$ induces isomorphisms*

$$\mathbb{J}^{\mathfrak{m}}(K)/K_{\mathfrak{m}}^1 \xrightarrow{\sim} \mathbb{J}(K)/K^* \quad \text{and} \quad \mathbb{J}^{\mathfrak{m}}(K)/W_{\mathfrak{m}}(K)K_{\mathfrak{m}}^1 \xrightarrow{\sim} \mathbb{J}(K)/W_{\mathfrak{m}}(K)K^*.$$

PROOF. The first map being an isomorphism is a consequence of the previous lemma. The second isomorphism is in turn induced by the first. \square

The composition $\mathbb{J}^{\mathfrak{m}}(K) \rightarrow \mathbb{I}^{\mathfrak{m}}(K) \rightarrow \mathbb{I}^{\mathfrak{m}}(K)/\mathbb{S}_{\mathfrak{m}}(K)$ is surjective and the group $W_{\mathfrak{m}}(K)K_{\mathfrak{m}}^1$ is contained in its kernel. On the other hand for α in the kernel one has $(\alpha) = (\beta)$ for some $\beta \in K_{\mathfrak{m}}^1$. Then $(\beta^{-1}\alpha) = (1)$, that is $\beta^{-1}\alpha \in \mathbb{J}^{\mathfrak{m}}(K) \cap \mathbb{J}^{S_{\infty}}(K) = W_{\mathfrak{m}}(K)K_{\mathfrak{m}}^1$. Hence the inclusion $\mathbb{J}^{\mathfrak{m}}(K) \rightarrow \mathbb{J}(K)$ induces an isomorphism $\mathbb{J}^{\mathfrak{m}}(K)/W_{\mathfrak{m}}(K)K_{\mathfrak{m}}^1 \xrightarrow{\sim} \mathbb{I}^{\mathfrak{m}}(K)/\mathbb{S}_{\mathfrak{m}}(K)$. Thus we have isomorphisms

$$\mathcal{C}_{\mathfrak{m}}(K) = \mathbb{J}(K)/W_{\mathfrak{m}}(K)K^* \xleftarrow{\sim} \mathbb{J}^{\mathfrak{m}}(K)/W_{\mathfrak{m}}(K)K_{\mathfrak{m}}^1 \xrightarrow{\sim} \mathbb{I}^{\mathfrak{m}}(K)/\mathbb{S}_{\mathfrak{m}}(K) = \mathcal{C}_{\mathfrak{m}}(K).$$

So all ray class groups are factor groups of the idèle class group:

20.27 Theorem. *Let \mathfrak{m} be a modulus of K . Then $(\cdot): \mathbb{J}^{\mathfrak{m}}(K) \rightarrow \mathbb{I}^{\mathfrak{m}}(K)$ induces an isomorphism $\mathcal{C}_{\mathfrak{m}}(K) \xrightarrow{\sim} \mathcal{C}_{\mathfrak{m}}(K)$. \square*

So the map $\mathcal{C}_{\mathfrak{m}}(K) \rightarrow \mathcal{C}_{\mathfrak{m}}(K)$ is as follows: having an idèle class, choose a representative $\alpha \in \mathbb{J}^{\mathfrak{m}}(K)$ of this class and take the class of the fractional ideal (α) in the ray class group.

For \mathfrak{m} and \mathfrak{n} moduli of K satisfying $\mathfrak{m} \mid \mathfrak{n}$ we have $W_{\mathfrak{m}}(K) \supseteq W_{\mathfrak{n}}(K)$ and therefore the diagram

$$\begin{array}{ccc} & & \mathcal{C}_{\mathfrak{n}}(K) \\ & \nearrow & \downarrow \\ \mathcal{C}(K) & & \mathcal{C}_{\mathfrak{m}}(K) \\ & \searrow & \end{array}$$

of natural projections commutes. By the Classification Theorem of section 15.3 (Theorem 15.29) ray class groups $\mathcal{C}_{\mathfrak{m}}(K)$ correspond to ray class fields $K_{\mathcal{H}_{\mathfrak{m}}(K)}$ and the Artin map induces an isomorphism $\mathcal{C}_{\mathfrak{m}}(K) \xrightarrow{\sim} \text{Gal}(K_{\mathcal{H}_{\mathfrak{m}}(K)} : K)$. For $\mathfrak{m} \mid \mathfrak{n}$ the diagram

$$\begin{array}{ccc} \mathcal{C}_{\mathfrak{n}}(K) & \longrightarrow & \mathcal{C}_{\mathfrak{n}}(K) \\ \downarrow & & \downarrow \\ \mathcal{C}_{\mathfrak{m}}(K) & \longrightarrow & \mathcal{C}_{\mathfrak{m}}(K) \end{array}$$

commutes. The vertical map on the right is compatible with the restriction of automorphisms. We obtain a continuous map, the *global reciprocity map*,

$$\vartheta_K: \mathcal{C}(K) \longrightarrow \varprojlim_{\mathfrak{m}} \mathcal{C}_{\mathfrak{m}}(K) \xrightarrow{\sim} \varprojlim_{\mathfrak{m}} \mathcal{C}_{\mathfrak{m}}(K) \xrightarrow{\sim} \text{Gal}(K^{\text{ab}} : K).$$

The last isomorphism is given by the Classification Theorem (Theorem 15.29) of global class field theory. Note that $\varprojlim_{\mathfrak{m}} \mathcal{C}_{\mathfrak{m}}(K)$ is the Pontryagin dual of $\mathcal{H}(K)$.

20.28 Proposition. *The map ϑ_K is surjective.*

PROOF. The maps $\mathcal{C}(K) \rightarrow \mathcal{C}_{\mathfrak{m}}(K) \xrightarrow{\sim} \mathcal{C}_{\mathfrak{m}}(K) \xrightarrow{\sim} \text{Gal}(K_{\mathcal{H}_{\mathfrak{m}}(K)} : K)$ are surjective, so by Theorem 19.59 the image of $\mathcal{C}(K)$ is dense in $\text{Gal}(K^{\text{ab}} : K)$. The group $\mathcal{C}_0(K)$ is the kernel of $\mathcal{C}(K) \rightarrow \mathbb{R}^{>0}$ and since the maps $\mathcal{C}(K) \rightarrow \mathcal{C}_{\mathfrak{m}}(K)$ are continuous maps to discrete groups, the restrictions $\mathcal{C}_0(K) \rightarrow \varprojlim_{\mathfrak{m}} \mathcal{C}_{\mathfrak{m}}(K)$ are surjective. So the image of $\mathcal{C}_0(K)$ in $\varprojlim_{\mathfrak{m}} \mathcal{C}_{\mathfrak{m}}(K)$ is dense as well. Since $\mathcal{C}_0(K)$ is compact its image is compact and is therefore equal to the whole group $\varprojlim_{\mathfrak{m}} \mathcal{C}_{\mathfrak{m}}(K)$. \square

Finite abelian extensions of K correspond to open subgroups of the profinite group $\text{Gal}(K^{\text{ab}} : K)$ and by the Classification Theorem and Theorem 20.27 also to open subgroups of $\varprojlim_{\mathfrak{m}} \mathcal{C}_{\mathfrak{m}}(K)$.

20.29 Theorem. *Open subgroups of $\text{Gal}(K^{\text{ab}} : K)$ correspond via ϑ_K to open subgroups of $\mathcal{C}(K)$.*

PROOF. Let $D(K)$ be the kernel of the map $\vartheta_K : \mathcal{C}(K) \rightarrow \text{Gal}(K^{\text{ab}} : K)$ is equal to the kernel of $\mathcal{C}(K) \rightarrow \varprojlim_{\mathfrak{m}} \mathcal{C}_{\mathfrak{m}}(K)$. So

$$D(K) = \bigcap_{\mathfrak{m}} W_{\mathfrak{m}}(K)K^*/K^*.$$

The open subgroups of $\varprojlim_{\mathfrak{m}} \mathcal{C}_{\mathfrak{m}}(K)$ correspond to the open subgroups of $\mathcal{C}(K)$ which contain $D(K)$. By Proposition 20.23 each open subgroup of $\mathcal{C}(K)$ contains a subgroup $W_{\mathfrak{m}}(K)K^*/K^*$ for some modulus \mathfrak{m} of K . \square

The correspondence in this theorem is obtained via the Artin isomorphism

$$\varprojlim_{\mathfrak{m}} \mathcal{C}_{\mathfrak{m}}(K) \xrightarrow{\sim} \text{Gal}(K^{\text{ab}} : K).$$

Its formulation depends on the ideal-theoretic version of class field theory. In the next section we translate this into a pure idèlic version.

20.4 The Classification Theorem (idèlic version)

In this section $L : K$ is a number field extension of degree n . For \mathfrak{q} a prime of L above a prime \mathfrak{p} of K , we can take $K_{\mathfrak{p}}$ to be a subfield of $L_{\mathfrak{q}}$. Thus we have an injective homomorphism

$$\mathbb{J}(K) \rightarrow \mathbb{J}(L),$$

mapping $\alpha = (\alpha_{\mathfrak{p}})_{\mathfrak{p}}$ to $\alpha' = (\alpha'_{\mathfrak{q}})_{\mathfrak{q}}$, where $\alpha'_{\mathfrak{q}} = \alpha_{\mathfrak{p}}$ if $\mathfrak{q} \mid \mathfrak{p}$. The group $\mathbb{J}(K)$ is often seen as a subgroup of $\mathbb{J}(L)$: an idèle $(\alpha_{\mathfrak{q}})_{\mathfrak{q}} \in \mathbb{J}(L)$ is in $\mathbb{J}(K)$ if and only if $\alpha_{\mathfrak{q}} = \alpha_{\mathfrak{q}'} \in K_{\mathfrak{p}}$ for all primes \mathfrak{p} of K and all $\mathfrak{q}, \mathfrak{q}'$ above \mathfrak{p} .

An isomorphism $\sigma: L \xrightarrow{\sim} \sigma(L)$ of number fields obviously respects absolute values: $\|\sigma(\alpha)\|_{\sigma(\mathfrak{q})} = \|\alpha\|_{\mathfrak{q}}$ for all $\alpha \in L$ and every prime \mathfrak{p} of K . So by definition of completion it determines an isomorphism of the completions:

$$\begin{array}{ccc} L & \xrightarrow[\sim]{\sigma} & \sigma(L) \\ \downarrow & & \downarrow \\ L_{\mathfrak{q}} & \xrightarrow{\sigma} & L_{\sigma(\mathfrak{q})} \end{array}$$

This in turn determines an isomorphism of adèle rings:

$$\sigma: \mathbb{A}(L) \xrightarrow{\sim} \mathbb{A}(\sigma(L)): (\alpha_{\mathfrak{q}})_{\mathfrak{q}} \mapsto (\sigma(\alpha)_{\sigma(\mathfrak{q})})_{\sigma(\mathfrak{q})}$$

and similarly for idèle groups.

20.30 Notations. For \mathfrak{p} a prime of K we write

$$L_{\mathfrak{p}} = \prod_{\mathfrak{q}|\mathfrak{p}} L_{\mathfrak{q}}$$

and for \mathfrak{p} a finite prime of K

$$\mathcal{O}_{\mathfrak{p}}^{(L)} = \prod_{\mathfrak{q}|\mathfrak{p}} \mathcal{O}_{\mathfrak{q}}.$$

For S a finite saturated collection of primes of K we write

$$\mathbb{A}^S(L) = \prod_{\mathfrak{p} \in S} L_{\mathfrak{p}} \times \prod_{\mathfrak{p} \notin S} \mathcal{O}_{\mathfrak{p}}^{(L)}$$

and

$$\mathbb{J}^S(L) = \prod_{\mathfrak{p} \in S} L_{\mathfrak{p}}^* \times \prod_{\mathfrak{p} \notin S} \mathcal{O}_{\mathfrak{p}}^{(L)*}.$$

Then

$$\mathbb{A}(L) = \varinjlim_S \mathbb{A}^S(L) = \bigcup_S \mathbb{A}^S(L) = \prod_{\mathfrak{p}} L_{\mathfrak{p}},$$

the restricted product consisting of all $(\alpha_{\mathfrak{p}})_{\mathfrak{p}}$, where $\alpha_{\mathfrak{p}} \in L_{\mathfrak{p}}$ such that $\alpha_{\mathfrak{p}} \in \mathcal{O}_{\mathfrak{p}}^{(L)}$ for all but finitely many finite primes \mathfrak{p} . Each $L_{\mathfrak{p}}$ is via the diagonal embedding $K_{\mathfrak{p}} \rightarrow L_{\mathfrak{p}}$ a commutative $K_{\mathfrak{p}}$ -algebra and as a $K_{\mathfrak{p}}$ -vector space its dimension equals $\sum_{\mathfrak{q}|\mathfrak{p}} [L_{\mathfrak{q}} : K_{\mathfrak{p}}] = \sum_{\mathfrak{q}|\mathfrak{p}} e_{\mathfrak{p}}^{(L)} f_{\mathfrak{p}}^{(L)} = [L : K]$. The diagonal embeddings $K_{\mathfrak{p}} \rightarrow L_{\mathfrak{p}}$ induce an embedding

$$\mathbb{A}(K) \rightarrow \mathbb{A}(L), \quad (\alpha_{\mathfrak{p}})_{\mathfrak{p}} \mapsto (\alpha_{\mathfrak{p}})_{\mathfrak{p}}$$

and since the idèles are the units of the adèle ring by restriction we obtain again the inclusion

$$\mathbb{J}(K) \rightarrow \mathbb{J}(L).$$

If $L : K$ is a Galois extension with Galois group G , then the $L_{\mathfrak{p}}$ and $\mathcal{O}_{\mathfrak{p}}^{(L)}$ are G -modules and so are $\mathbb{A}(L)$, $\mathbb{J}(L)$ and $\mathcal{C}(L)$. For the adèle ring and the idèle group we have Galois descent:

20.31 Proposition. *Let $L : K$ be a Galois extension with Galois group G . Then $\mathbb{A}(L)^G = \mathbb{A}(K)$ and $\mathbb{J}(L)^G = \mathbb{J}(K)$.*

PROOF. The second identity follows from the first. For S a finite saturated collection of primes of K and we have

$$\mathbb{A}^S(L)^G = \prod_{\mathfrak{p} \in S} L_{\mathfrak{p}}^G \times \prod_{\mathfrak{p} \notin S} (\mathcal{O}_{\mathfrak{p}}^{(L)})^G = \prod_{\mathfrak{p} \in S} K_{\mathfrak{p}} \times \prod_{\mathfrak{p} \notin S} \mathcal{O}_{\mathfrak{p}}.$$

Therefore, $\mathbb{A}(L)^G = \mathbb{A}(K)$. □

The behavior of idèle class groups under field extensions differs considerably from the behavior of the ideal class groups.

20.32 Proposition. *The embedding $K \rightarrow L$ induces an injective homomorphism*

$$\mathcal{C}(K) \rightarrow \mathcal{C}(L), \quad \bar{\alpha} = \alpha K^* \mapsto \alpha L^* = \bar{\alpha}.$$

PROOF. We have to show that $\mathbb{J}(K) \cap L^* = K^*$. Let $M : K$ be the normal closure of $L : K$ and $G = \text{Gal}(M : K)$. Then

$$\mathbb{J}(K) \cap L^* \subseteq \mathbb{J}(K) \cap M^* \subseteq (\mathbb{J}(K) \cap M^*)^G = \mathbb{J}(K) \cap (M^*)^G = \mathbb{J}(K) \cap K^* = K^*. \quad \square$$

As a consequence we can view $\mathcal{C}(K)$ as the subgroup of $\mathcal{C}(L)$ consisting of all $\bar{\alpha} = \alpha L^*$ with $\alpha \in \mathbb{J}(K)$.

20.33 Theorem. *Let $L : K$ be a Galois extension of number fields with Galois group G . Then $\mathcal{C}(L)^G = \mathcal{C}(K)$.*

PROOF. The short exact sequence

$$1 \rightarrow L^* \rightarrow \mathbb{J}(L) \rightarrow \mathcal{C}(L) \rightarrow 1$$

induces an exact sequence

$$1 \rightarrow (L^*)^G \rightarrow \mathbb{J}(L)^G \rightarrow \mathcal{C}(L)^G$$

and since $(L^G)^* = K^*$ and $\mathbb{J}(L)^G = \mathbb{J}(K)$ the theorem will follow from the surjectivity of $\mathbb{J}(L)^G \rightarrow \mathcal{C}(L)^G$. Let $\alpha \in \mathbb{J}(L)$ such that $\bar{\alpha} \in \mathcal{C}(L)^G$. Then $\sigma(\bar{\alpha}) = \bar{\alpha}$ for all $\sigma \in G$. So $\frac{\sigma(\alpha)}{\alpha} \in L^*$ for all $\sigma \in G$. Take $\gamma \in K^*$ such that

$$\delta = \sum_{\sigma} \frac{\sigma(\alpha)}{\alpha} \sigma(\gamma) \neq 0.$$

Then for each $\tau \in G$

$$\tau(\delta) = \sum_{\sigma} \frac{\tau\sigma(\alpha)}{\tau(\alpha)} \tau\sigma(\gamma) = \frac{\alpha}{\tau(\alpha)} \sum_{\sigma} \frac{\tau\sigma(\alpha)}{\alpha} \tau\sigma(\gamma) = \frac{\alpha}{\tau(\alpha)} \delta.$$

So $\tau(\delta\alpha) = \delta\alpha$ for all $\tau \in G$ and therefore $\delta\alpha \in \mathbb{J}(L)^G$. Since $\delta \in L^*$ we have $\frac{\delta\alpha}{\delta} = \bar{\alpha} \in \mathcal{C}(L)^G$. \square

20.34 Definition. The *norm* map $N_K^L: \mathbb{A}(L) \rightarrow \mathbb{A}(K)$ is the map defined on the components $L_{\mathfrak{p}}$ by

$$N_K^L(\alpha)_{\mathfrak{p}} = \prod_{\mathfrak{q}|\mathfrak{p}} N_{\mathfrak{p}}^{\mathfrak{q}}(\alpha_{\mathfrak{q}}) \quad \text{for } \alpha = (\alpha_{\mathfrak{q}})_{\mathfrak{q}} \in L_{\mathfrak{p}}.$$

Its restriction to $\mathbb{J}(L) \rightarrow \mathbb{J}(K)$ is a group homomorphism.

By Corollary 10.47 the norm map $N_K^L: \mathbb{J}(L) \rightarrow \mathbb{J}(K)$ is compatible with the norm map $N_K^L: L^* \rightarrow K^*$, so we can define a norm for idèle classes:

20.35 Definition. The *norm* $N_K^L: \mathcal{C}(L) \rightarrow \mathcal{C}(K)$ is induced by the norm of idèles:

$$N_K^L(\bar{\alpha}) = \overline{N_K^L(\alpha)} \quad \text{for } \alpha \in \mathbb{J}(L).$$

20.36 Definition. The cokernel of $N_K^L: \mathcal{C}(L) \rightarrow \mathcal{C}(K)$ is called the *idèle class group associated with $L:K$* . Notation: $\mathcal{C}(L:K)$. So we have an exact sequence

$$\mathcal{C}(L) \xrightarrow{N_K^L} \mathcal{C}(K) \longrightarrow \mathcal{C}(L:K) \rightarrow 0.$$

20.37 Proposition. Let $L:K$ be abelian. The open subgroup of $\mathcal{C}(K)$ corresponding via ϑ_K to the open subgroup $\text{Gal}(K^{\text{ab}}:L)$ of $\text{Gal}(K^{\text{ab}}:K)$ is the group $N_K^L(\mathcal{C}(L))$.

PROOF. Let \mathfrak{m} be a multiple of the conductor of $L:K$. We have the following commutative diagram

$$\begin{array}{ccccccc}
 \mathcal{C}(L) & \longrightarrow & \varprojlim_{\mathfrak{m}} \mathcal{C}_{\mathfrak{m}}(L) & \xrightarrow{\sim} & \varprojlim_{\mathfrak{m}} \mathcal{C}_{\mathfrak{m}}(L) & \xrightarrow{\sim} & \text{Gal}(L^{\text{ab}} : L) \\
 \downarrow N_K^L & & \downarrow (N_K^L)_{\mathfrak{m}} & & \downarrow (N_K^L)_{\mathfrak{m}} & & \downarrow \\
 \mathcal{C}(K) & \longrightarrow & \varprojlim_{\mathfrak{m}} \mathcal{C}_{\mathfrak{m}}(K) & \xrightarrow{\sim} & \varprojlim_{\mathfrak{m}} \mathcal{C}_{\mathfrak{m}}(K) & \xrightarrow{\sim} & \text{Gal}(K^{\text{ab}} : K) \\
 \downarrow & & \downarrow & & \downarrow & & \downarrow \\
 \mathcal{C}(K)/N_K^L(\mathcal{C}(L)) & \longrightarrow & \mathcal{C}(L : K) & \xrightarrow{\sim} & \mathcal{C}(L : K) & \xrightarrow{\sim} & \text{Gal}(L : K) \\
 \downarrow & & \downarrow & & \downarrow & & \downarrow \\
 1 & & 1 & & 1 & & 1
 \end{array}$$

The composition of the maps in the two top rows are the reciprocity maps ϑ_L and ϑ_K . The image of $\text{Gal}(L^{\text{ab}} : L)$ in $\text{Gal}(K^{\text{ab}} : K)$ is $\text{Gal}(K^{\text{ab}} : L)$. We have to show that $\mathcal{C}(K)/N_K^L(\mathcal{C}(L)) \rightarrow \mathcal{C}(L : K)$ is an isomorphism. By Theorem 20.29 the map $\mathcal{C}(K) \rightarrow \varprojlim_{\mathfrak{m}} \mathcal{C}_{\mathfrak{m}}(K)$ is surjective. Because \mathfrak{m} is a multiple of the conductor, we have

$$U_{\mathfrak{p}}^{v_{\mathfrak{p}}(\mathfrak{m})} \subseteq N_{\mathfrak{p}}^{\mathfrak{q}}(L_{\mathfrak{q}}) \quad \text{for all } \mathfrak{p} \in \mathcal{P}(K) \text{ and } \mathfrak{q} \in \mathcal{P}(L) \text{ above } \mathfrak{p}.$$

Hence

$$W_{\mathfrak{m}}(K) = \prod_{\mathfrak{p}} U_{\mathfrak{p}}^{v_{\mathfrak{p}}(\mathfrak{m})} \subseteq N_K^L(\mathbb{J}(L))$$

and for the images in $\mathcal{C}(K)$:

$$\text{Ker}(\mathcal{C}(K) \rightarrow \mathcal{C}(L : K)) = W_{\mathfrak{m}}(K)K^*/K^* \subseteq N_K^L(\mathcal{C}(L)).$$

Therefore, $\mathcal{C}(K)/N_K^L(\mathcal{C}(L)) \rightarrow \mathcal{C}(L : K)$ is injective. \square

So the full idèlic version of global class field theory becomes:

20.38 Classification Theorem. *Let K be a number field. The map*

$$\begin{array}{ccc}
 \begin{array}{l} \text{finite abelian} \\ \text{extensions of } K \end{array} & \longrightarrow & \begin{array}{l} \text{open subgroups of} \\ \mathcal{C}(K) \end{array} \\
 L : K & \longmapsto & N_K^L(\mathcal{C}(L))
 \end{array}$$

is a bijection. For $L : K$ a finite abelian extension the global reciprocity map $\vartheta_K : \mathcal{C}(K) \rightarrow \text{Gal}(K^{\text{ab}} : K)$ induces an isomorphism

$$\mathcal{C}(K)/N_K^L(\mathcal{C}(L)) \xrightarrow{\sim} \text{Gal}(L : K). \quad \square$$

20.5 Local and global reciprocity

The idèlic approach to class field theory clarifies the relationship between local and global class field theory considerably.

For a number field K we have local reciprocity maps for primes \mathfrak{p} of K

$$\vartheta_{K_{\mathfrak{p}}} : K_{\mathfrak{p}}^* \rightarrow \text{Gal}(K_{\mathfrak{p}}^{\text{ab}} : K_{\mathfrak{p}})$$

and the global reciprocity map

$$\vartheta_K : \mathcal{C}(K) \rightarrow \text{Gal}(K^{\text{ab}} : K).$$

Let's fix an abelian number field extension $L : K$. For a prime \mathfrak{p} of K and a prime \mathfrak{q} of L above \mathfrak{p} the local reciprocity map yields a short exact sequence

$$1 \rightarrow N_{\mathfrak{p}}^{\mathfrak{q}}(L_{\mathfrak{q}}^*) \longrightarrow K_{\mathfrak{p}}^* \xrightarrow{\vartheta_{K_{\mathfrak{p}}}^{(L_{\mathfrak{q}})}} \text{Gal}(L_{\mathfrak{q}} : K_{\mathfrak{p}}) \rightarrow 1$$

and via the natural isomorphism $\text{Gal}(L_{\mathfrak{q}} : K_{\mathfrak{p}}) \xrightarrow{\sim} Z_{\mathfrak{p}}^{(L)}$ a short exact sequence

$$1 \rightarrow N_{\mathfrak{p}}^{\mathfrak{q}}(L_{\mathfrak{q}}^*) \longrightarrow K_{\mathfrak{p}}^* \xrightarrow{\vartheta_{\mathfrak{p}}^{(L)}} Z_{\mathfrak{p}}^{(L)} \rightarrow 1.$$

For primes \mathfrak{p} of K there is a natural embedding

$$K_{\mathfrak{p}}^* \rightarrow \mathbb{J}(K), \quad \alpha \mapsto \alpha^{\mathfrak{p}},$$

where $\alpha^{\mathfrak{p}}$ is given by

$$\alpha_{\mathfrak{p}}^{\mathfrak{p}} = \alpha \quad \text{and} \quad \alpha_{\mathfrak{p}'}^{\mathfrak{p}} = 1 \quad \text{for all } \mathfrak{p}' \neq \mathfrak{p}.$$

The composition with $\mathbb{J}(K) \rightarrow \mathcal{C}(K)$ is injective as well; it is the map

$$K_{\mathfrak{p}}^* \rightarrow \mathcal{C}(K), \quad \alpha \mapsto [\alpha^{\mathfrak{p}}],$$

where, as before, $[\alpha^{\mathfrak{p}}]$ denotes the idèle class of the idèle $\alpha^{\mathfrak{p}}$.

20.39 Theorem. *The square*

$$\begin{array}{ccc} K_{\mathfrak{p}}^* & \xrightarrow{\vartheta_{\mathfrak{p}}^{(L)}} & Z_{\mathfrak{p}}^{(L)} \\ \downarrow & & \downarrow \subseteq \\ \mathcal{C}(K) & \xrightarrow{\vartheta_K^{(L)}} & \text{Gal}(L : K) \end{array}$$

commutes. (The vertical map on the left is the map described above and $\vartheta_K^{(L)}$ is the composition of ϑ_K with the map $\text{Gal}(K^{\text{ab}} : K) \rightarrow \text{Gal}(L : K)$ given by restriction of automorphisms.)

PROOF. Let $\alpha \in L^*$. We have to show that $\vartheta_K^{(L)}([\alpha^{\mathfrak{p}}]) = \vartheta_{\mathfrak{p}}^{(L)}(\alpha)$. First we follow the definition of $\vartheta_{\mathfrak{p}}^{(L)}$. Let \mathfrak{n} be a modulus for $L : K$. Put $\mathfrak{n} = \mathfrak{p}^t \mathfrak{m}$ with $\mathfrak{p} \nmid \mathfrak{m}$. Choose a $\beta \in K_{\mathfrak{m}}^1$ such that $\beta \equiv \alpha \pmod{U_{\mathfrak{p}}^{(t)}}$. Then $v_{\mathfrak{p}}(\beta) = v_{\mathfrak{p}}(\alpha)$ and $\vartheta_{\mathfrak{p}}^{(L)}(\alpha) = \varphi_K^{(L)}(\mathfrak{a})^{-1}$, where $\mathfrak{a} = (\beta)\mathfrak{p}^{-v_{\mathfrak{p}}(\alpha)} \in \mathbb{I}^{\mathfrak{n}}(K)$.

We have $(\beta^{-1}\alpha^{\mathfrak{p}}) = \beta^{-1}\mathfrak{p}^{v_{\mathfrak{p}}(\alpha)} = \mathfrak{a}^{-1} \in \mathbb{I}^{\mathfrak{n}}(K)$. Therefore,

$$\vartheta_K^{(L)}([\alpha^{\mathfrak{p}}]) = \varphi_K^{(L)}((\beta^{-1}\alpha^{\mathfrak{p}})) = \varphi_K^{(L)}(\mathfrak{a}^{-1}) = \vartheta_{\mathfrak{p}}^{(L)}(\alpha). \quad \square$$

Final remarks

A modern approach to class field theory is top down: start with local class field theory, independent of the global one, and for global class field theory use the approach with idèles. After that, one may translate the results into the language of ideals. In our bottom up approach the use of idèles clarifies the definition of local Artin maps (Proposition 20.39) and their relation to the global Artin map:

Conductor. Let $L : K$ be an abelian number field extension. The conductor \mathfrak{f} of $L : K$ is the least modulus divisible by all ramifying primes such that $S_{\mathfrak{f}}(K)$ is contained in the kernel of the Artin map $\varphi_K^{(L)} : \mathbb{I}^L(K) \rightarrow \text{Gal}(L : K)$. By Theorem 15.56 the conductor \mathfrak{f} is the product of all $\mathfrak{p}^{n_{\mathfrak{p}}}$, where $n_{\mathfrak{p}} \in \mathbb{N}$ is the least such that

$$U_{\mathfrak{p}}^{(n_{\mathfrak{p}})} \subseteq N_{\mathfrak{p}}^q(L_{\mathfrak{q}}^*). \quad (20.1)$$

The power $\mathfrak{p}^{n_{\mathfrak{p}}}$ is the local conductor at \mathfrak{p} of the extension $L : K$. The modulus \mathfrak{f} is the least one such that L is contained in its ray class field. In terms of idèles this means $W_{\mathfrak{f}}(K) \subseteq N_K^L(\mathbb{I}(L))$, which by definition of $W_{\mathfrak{f}}(K)$ comes down again to condition (20.1).

Product formula. Let $L : K$ be an abelian number field extension and $\alpha \in K$. By Theorem 16.22 we have a product for norm residue symbols. In terms of local Artin maps this is the formula

$$\prod_{\mathfrak{p} \in \mathcal{P}(K)} \vartheta_{\mathfrak{p}}^{(L)}(\alpha) = 1.$$

Using idèlic class field theory this formula is easily obtained as follows. Let S be a saturated collection of primes of K containing all primes \mathfrak{p} with $v_{\mathfrak{p}}(\alpha) \neq 0$. Let α^S be the idèle defined by

$$\alpha_{\mathfrak{p}}^S = \begin{cases} \alpha & \text{if } \mathfrak{p} \in S \\ 1 & \text{otherwise.} \end{cases}$$

Then $\alpha^{-1}\alpha^S \in W_{\mathfrak{f}}(K)$ and so

$$\prod_{\mathfrak{p}} \vartheta_{\mathfrak{p}}^{(L)}(\alpha) = \prod_{\mathfrak{p} \in S} \vartheta_{\mathfrak{p}}^{(L)}(\alpha) = \prod_{\mathfrak{p} \in S} \vartheta_K^{(L)}([\alpha^{\mathfrak{p}}]) = \vartheta_K^{(L)}([\alpha^S]) = \vartheta_K^{(L)}([\alpha^{-1}\alpha^S]) = 1.$$

EXERCISES

1. Let $L : K$ be a Galois extension of number fields. Show that

$$\mathcal{G}(L : K) \rightarrow \text{Ab}, \quad K' \mapsto \mathbb{A}(K')/K'$$

is an acyclic Galois module.

2. Let K be a number field and p a prime number. Show that we have a \mathbb{Q}_p -algebra isomorphism

$$\mathbb{Q}_p \otimes_{\mathbb{Q}} K \xrightarrow{\sim} \prod_{\mathfrak{p}|p} K_{\mathfrak{p}},$$

where the product is over all primes of K above p . So $\mathbb{Q}_p \otimes_{\mathbb{Q}} K \xrightarrow{\sim} K_p$ (Notations 20.30).

3. Show that

$$\mathbb{J}(\mathbb{Q}) \xrightarrow{\sim} \mu_2 \times \mathbb{R}^{>0} \times \prod_p \mathbb{Z}_p^* \times \bigoplus_p \mathbb{Z},$$

where the direct product and the direct sum are over all prime numbers p .

4. Show that

$$\mathbb{C}(\mathbb{Q}) \cong \mathbb{R}^{>0} \times \hat{\mathbb{Z}}^* \quad \text{and} \quad C_0(\mathbb{Q}) \cong \hat{\mathbb{Z}}^*.$$

References

- [1] H. Bass, J. Milnor, and J.-P. Serre, *Solution of the congruence subgroup problem for SL_n ($n \geq 3$) and Sp_{2n} ($n \geq 2$)*, Inst. Hautes Études Sci. Publ. Math. **33** (1967), 59-137.
- [2] H. Bass, *Algebraic K-Theory*, Mathematics Lecture Note Series, W.A. Benjamin, New York, 1968.
- [3] Z.I. Borevich and I.R. Shafarevich, *Number Theory*, Academic Press, New York, 1966.
- [4] R. Brauer, *Beziehungen zwischen Klassenzahlen von Teilkörpern eines galoisschen Körpers*, Math. Nachr. **4** (1951), 158-174.
- [5] R. Brauer and M. Suzuki, *On finite groups of even order whose 2-Sylow group is a quaternion group*, Proc. Nat. Acad. Sci. **45** (1959), 1757-1759.
- [6] K.S. Brown, *Cohomology of Groups*, Springer-Verlag, New York, etc., 1982.
- [7] J.W.S. Cassels and A. Fröhlich (eds.), *Algebraic Number Theory*, 2nd ed., London Mathematical Society, 2010.
- [8] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, Berlin, etc., 1993.
- [9] G. Cornell, *A Note on the Class Group of Composita*, Journal of Number Theory **39** (1991), 1-4.
- [10] G. Cornell and M. Rosen, *Group-Theoretic Constraints on the Structure of the Class Group*, Journal of Number Theory **13** (1981), 1-11.
- [11] A. Fröhlich, *On the class group of relatively abelian fields*, Quat. J. Math. Oxford Series (2) **3** (1952), 98-106.
- [12] A. Fröhlich and M. Taylor, *Algebraic Number Theory*, Cambridge studies in advanced mathematics, vol. 27, Cambridge University Press, Cambridge, U.K., 1993.
- [13] E.S. Golod and I.R. Shafarevich, *On class field towers. (Russian)*, Izv. Akad. Nauk SSSR **28** (1964), 261-272.
- [14] G. Gras, *Class Field Theory*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2003.
- [15] M. Hall Jr., *The Theory of Groups*, The Macmillan Company, New York, 1959.
- [16] H. Hasse, *Beweis eines Satzes und Wiederlegung einer Vermutung über das allgemeinen Normenrestsymbol*, Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse (1931), 64-69.
- [17] ———, *Vorlesungen über Klassenkörpertheorie*, Physica-Verlag, Würzburg, 1967.
- [18] D. Hilbert, *Die Theorie der Algebraischen Zahlkörper*, Jahresbericht der Deutschen Mathematiker-Vereinigung **4** (1897), 175-546; English transl. in D. Hilbert, *The theory of algebraic number fields* (1998).

References

- [19] D. Hilbert, *The theory of algebraic number fields*, Springer-Verlag, Berlin, 1998.
- [20] G.J. Janusz, *Algebraic Number Fields: Second Edition*, Graduate Studies in Mathematics, vol. 7, American Mathematical Society, 1996.
- [21] M. Keune, *The Hasse Norm Theorem and Biquadratic Fields*, Master's Thesis, radboud University, Nijmegen, 2021, www.math.ru.nl/~bosma/Students/MerlijnKeuneMsc.pdf.
- [22] F. Keune, *Quadratic reciprocity and finite fields*, Nieuw Archief voor Wiskunde **4** (1991), no. 9, 263–266.
- [23] H. Kiselevsky, *Some Results Related to Hilbert's Theorem 94*, Journal of Number Theory **2** (1970), 199–206.
- [24] S. Kuroda, *Über die Klassenzahlen algebraischer Zahlkörper*, Nagoya Math. J. **1** (1950), 1–10.
- [25] S. Lang, *Algebraic Number Theory: Second Edition*, Springer-Verlag, New York, 1986.
- [26] B.A. Magurn, *An Algebraic Introduction to K-Theory*, Encyclopedia of Mathematics and its Applications, Cambridge University Press, Cambridge, UK, 2002.
- [27] Y.I. Manin and A.A. Panchishkin, *Introduction to Modern Number Theory: Second Edition*, Encyclopaedia of Mathematical Sciences, Springer-Verlag, New York, 2005.
- [28] D.A. Marcus, *Number Fields, second edition*, Universitext, Springer International Publishing AG, Cham, Switzerland, 2018.
- [29] J. Milnor, *Introduction to Algebraic K-Theory*, Annals of Mathematical Studies, Princeton University Press, Princeton, New Jersey, 1971.
- [30] H. Nehr Korn, *Über absolute Idealklassengruppen und Einheiten in algebraischer Zahlkörpern*, Abh. Math. Sem, Univ. Hamburg **9** (1933), 318–334.
- [31] J. Neukirch, *Algebraische Zahlentheorie*, Springer-Verlag, New York, 1992; English transl. in *Algebraic Number Theory*, Grundlehren der mathematischen Wissenschaften, Springer-Verlag, New York, 1999.
- [32] P. Samuel, *Théorie algébrique des nombres*, Hermann, Paris, 1967; English transl. in *Algebraic Theory of Numbers*, Dover, New York, 1972.
- [33] ———, *Algebraic Theory of Numbers*, Dover, New York, 1972.
- [34] J.-P. Serre, *Représentations linéaires des groupes finis*, Hermann, Paris, 1967.
- [35] I. Stewart, *Galois Theory*, 5th ed., Chapman and Hall / CRC, Boca Raton, etc., 2022.
- [36] H.P.F. Swinnerton-Dyer, *A Brief Guide to Algebraic Number Theory*, London Mathematical Society Texts, Cambridge University Press, 2001.
- [37] L.C. Washington, *Introduction to Cyclotomic Fields: Second Edition*, Graduate Texts in Mathematics, Springer-Verlag, New York, 1982.
- [38] W.C. Waterhouse, *An empty inverse limit*, Proc. Amer. Math. Soc. **36** (1972), 618.

Notations

$A \subseteq B$	A is a subset of B
$A \subset B$	A is a proper subset of B
$\#(A)$	the number of elements of a finite set A
$H \leq G$	H is a subgroup of G
$H < G$	H is a proper subgroup of G
$o(g)$	the order of an element g in a group, p. ix
$(G : H)$	the index of the subgroup H in the group G
$N \trianglelefteq G$	N is a normal subgroup of G
$N \triangleleft G$	N is a proper normal subgroup of G
$\langle g_1, \dots, g_n \rangle$	the subgroup of a given group generated by g_1, \dots, g_n
$\langle g \mid P(g) \rangle$	the subgroup of a given group generated by all g such that $P(g)$
\mathbb{N}	the set $\{0, 1, 2, 3, \dots\}$ of natural numbers
\mathbb{N}^*	the set $\{1, 2, 3, \dots\}$ of natural numbers $\neq 0$
\mathbb{Z}	the ring of (rational) integers
\mathbb{Q}	the field of rational numbers
\mathbb{R}	the field of real numbers
\mathbb{C}	the field of complex numbers
ζ_m	the primitive m -th root of unity $e^{2\pi i/m}$ of \mathbb{C}
$\mu(K)$	the group of roots of unity of a field K
μ	$= \mu(\mathbb{C})$, the group of roots of unity of \mathbb{C}
$\Re(z)$	the real part of $z \in \mathbb{C}$
$\Im(z)$	the imaginary part of $z \in \mathbb{C}$
\mathbb{F}_q	a field with q elements
\mathbb{Z}/n	the ring of integers modulo n
(a_1, \dots, a_n)	the ideal of a given commutative ring generated by a_1, \dots, a_n
$(a \mid P(a))$	the ideal of a given commutative ring generated by all a such that $P(a)$
R^*	the group of invertible elements in the ring R
$\deg(f)$	the degree of a polynomial f
ζ_n	the primitive n -th root of unity $e^{\frac{2\pi i}{n}}$ in \mathbb{C}

Notations

nA	for A a (multiplicative) abelian group and $n \in \mathbb{N}^*$: the subgroup of all $a \in A$ with $a^n = 1$
C_n	the cyclic group of order n
V_4	the Klein four group
D_n	the n -th dihedral group
S_n	the n -th symmetric group: permutations of the set $\{1, \dots, n\}$
A_n	the n -th alternating group: even permutations of the set $\{1, \dots, n\}$
$N_G(H)$	the normalizer of H in G , p. ix
$[L : K]$	the degree of a field extension $L : K$
$\text{Gal}(L : K)$	the Galois group of a Galois extension $L : K$
$s^n(X_1, \dots, X_n)$	the n -th elementary symmetric polynomial, p. ix
r, s	for a number field K a standard notation: r is the number of real embeddings of K and s the number of pairs of complex embeddings, p. 4
\mathcal{O}	the integral domain of integral algebraic numbers, p. 6
ω_m	for m a squarefree integer $\neq 1$: \sqrt{m} if $m \equiv 2, 3 \pmod{4}$, $\frac{1}{2} + \frac{1}{2}\sqrt{m}$ if $m \equiv 1 \pmod{4}$, p. 8
\mathcal{O}_K	the ring of integers of a number field K , p. 9
$\Delta_T(X)$	characteristic polynomial of a linear transformation T , p. 9
$\Delta_\alpha^{L:K}(X)$	the characteristic polynomial of $\alpha \in L$ over K , where $L : K$ is a finite field extension, p. 9
$\text{Tr}_K^L(\alpha)$	the trace of $\alpha \in L$ over K , where $L : K$ is a finite field extension, p. 9
$N_K^L(\alpha)$	the norm of $\alpha \in L$ over K , where $L : K$ is a finite field extension, p. 9
N	the norm $\mathbb{R}^r \times \mathbb{C}^s \rightarrow \mathbb{R}$, p. 12
$\text{disc}_K(\alpha_1, \dots, \alpha_n)$	the discriminant of a K -base of an extension field L , p. 15
$\mathfrak{a} \mid \mathfrak{b}$	the ideal \mathfrak{a} is a divisor of the ideal \mathfrak{b} , p. 34
$\text{Max}(R)$	the set of the maximal ideals of a ring R , p. 35
$\text{Spec}(R)$	the set of prime ideals of a ring R , p. 35
$\mathbb{I}^+(R)$	the monoid of nonzero ideals of an integral domain R , p. 36
$v_{\mathfrak{p}}(\mathfrak{a})$	the \mathfrak{p} -valuation of a (fractional) ideal \mathfrak{a} , p. 37
$\mathfrak{a} \sim \mathfrak{b}$	the nonzero ideals \mathfrak{a} and \mathfrak{b} of a Dedekind domain are equivalent, p. 40
$\mathcal{C}(R)$	the ideal class group of a Dedekind domain R , p. 41
$[\mathfrak{a}]$	the ideal class of a nonzero ideal \mathfrak{a} of a Dedekind domain, p. 41
$\mathbb{I}(R)$	the group of fractional ideals of a Dedekind domain R , p. 42
$\mathbb{P}(R)$	the group of principal fractional ideals of a Dedekind domain R , p. 42

$e(\mathfrak{p})$	the ramification index of \mathfrak{p} (over \mathbb{Q}), p. 50
$f(\mathfrak{p})$	the residue class degree of \mathfrak{p} (over \mathbb{Q}), p. 50
$e_{\mathfrak{p}}^{(K)}$	the ramification index of the prime number p in the number field K , p. 56
$f_{\mathfrak{p}}^{(K)}$	the residue class degree of the prime number p in the number field K , p. 56
$N(\mathfrak{a})$	the norm of a nonzero ideal \mathfrak{a} of a ring of integers of a number field, p. 57
$\mathcal{C}(K)$	the ideal class group of the number field K , p. 59
$\mathbb{I}(K)$	the group of fractional ideals of the number field K , p. 59
$\mathbb{P}(K)$	the group of principal fractional ideal of the number field K , p. 59
$\mathbb{I}^+(K)$	the monoid of nonzero ideals of the ring of integers of the number field K , p. 59
$\left(\frac{a}{p}\right)$	the Legendre symbol ($a \in \mathbb{Z}$ and p an odd prime), p. 66
n^*	for odd $n \in \mathbb{Z}$, $n^* = (-1)^{\frac{n-1}{2}}n$, p. 67
$\left(\frac{a}{b}\right)$	the Jacobi symbol ($a, b \in \mathbb{Z}$ and odd), p. 69
$\text{disc}(\gamma)$	the discriminant of the quadratic number γ , p. 71
Az	action of $A \in \text{GL}_2(\mathbb{Z})$ on $z \in \mathbb{C} \setminus \mathbb{Q}$, p. 72
$z_1 \simeq z_2$	equivalence of $z_1, z_2 \in \mathbb{C} \setminus \mathbb{Q}$, p. 72
$\langle x_1, \dots, x_n \rangle$	continued fraction of length n , p. 79
$p_n(x_1, \dots, x_n)$	numerator of continued fraction of length n , p. 80
$q_n(x_1, \dots, x_n)$	denominator of continued fraction of length n , p. 80
$\langle a_1, a_2, a_3, \dots \rangle$	infinite continued fraction, p. 82
$x \sim_{\varphi} y$	tail equivalence of irrational numbers x and y , p. 87
$\delta(F)$	the volume of a mesh of a lattice F in \mathbb{R}^n , p. 106
Λ_K	the image of \mathcal{O}_K under the embedding of a number field K in $\mathbb{R}^r \times \mathbb{C}^s$, p. 108
$L: \mathbb{R}^{*r} \times \mathbb{C}^{*s} \rightarrow \mathbb{R}^{r+s}$	the ‘logarithmic’ map, p. 115
$l: K^* \rightarrow \mathbb{R}^{r+s}$	the embedding ι composed with the ‘logarithmic’ map L , p. 115
$\psi: \mathcal{O}_K^* \rightarrow \mathbb{R}^{r+s}$	the map L restricted to \mathcal{O}_K^* , p. 115
H_m	the subspace of \mathbb{R}^m of vectors with coordinate sum 0, p. 116
$Q(L)$	Hasse index of a CM-field L , p. 125
$\text{Reg}(\varepsilon_1, \dots, \varepsilon_{r+s-1})$	the regulator of a group of units, p. 128
$\text{Reg}(K)$	the regulator of a number field K , p. 128
$\text{Reg}(X)$	the regulator of a group of units X in a number field, p. 128

Notations

$S^{-1}R$	the ring of fractions of an integral domain R with denominators in a multiplicative system S of R , p. 134
$R_{\mathfrak{p}}$	the localization of an integral domain R at a prime ideal \mathfrak{p} of R , p. 134
R_P	the localization of a Dedekind domain R at a set P of maximal ideals of R , p. 137
K_P	for a number field K the localization of \mathcal{O}_K at a set $P \subseteq \text{Max}(\mathcal{O}_K)$, p. 141
$\mathbb{I}_P(K)$	for a number field K the subgroup of $\mathbb{I}(K)$ generated by $P \subseteq \text{Max}(\mathcal{O}_K)$, p. 141
$\mathcal{C}_P(K)$	for a number field K the group $\mathcal{C}(K)$ modulo all $[\mathfrak{p}] \in \mathcal{C}(K)$ with \mathfrak{p} in $P \subseteq \text{Max}(\mathcal{O}_K)$, p. 141
K^+	the subgroup of totally positive elements of a number field K , p. 143
$\mathcal{C}^+(K)$	the narrow ideal class group of a number field K , p. 143
$e_K(\mathfrak{q})$	the ramification index of \mathfrak{q} over K , p. 146
$f_K(\mathfrak{q})$	the residue class degree of \mathfrak{q} over K , p. 146
$e_{\mathfrak{p}}^{(L)}$	the ramification index of \mathfrak{p} in L , p. 151
$f_{\mathfrak{p}}^{(L)}$	the residue class degree of \mathfrak{p} in L , p. 151
$\mathfrak{d}_R(L)$	the R -discriminant of the extension field L of the field of fractions of the Dedekind domain R , p. 155
$\mathfrak{d}_K(L)$	the discriminant of the number field L over the number field K , p. 159
$Z_K(\mathfrak{q})$	the decomposition group of \mathfrak{q} over K , p. 160
$T_K(\mathfrak{q})$	the inertia group of \mathfrak{q} over K , p. 161
$Z_{\mathfrak{p}}^{(L)}$	the decomposition group of \mathfrak{p} in L , p. 162
$T_{\mathfrak{p}}^{(L)}$	the inertia group of \mathfrak{p} in L , p. 162
$V_{K,i}(\mathfrak{q})$	the i -th ramification group of \mathfrak{q} over K , p. 169
$N_R^S(\mathfrak{a})$	the norm of $\mathfrak{a} \in \mathbb{I}(S)$ in $\mathbb{I}(R)$, p. 174
$\text{tr}_R^S(C)$	transfer of a $C \in \mathcal{C}(S)$ in $\mathcal{C}(R)$, p. 175
$j_L^K(\mathfrak{a})$	the fractional ideal $\mathfrak{a}\mathcal{O}_L$, p. 176
$N_K^L(\mathfrak{a})$	the norm of the fractional ideal \mathfrak{a} in $\mathbb{I}(K)$, p. 176
$j_L^K([\mathfrak{a}])$	the ideal class $[\mathfrak{a}\mathcal{O}_L]$, p. 176
$\text{tr}_K^L([\mathfrak{a}])$	the ideal class $[N_K^L(\mathfrak{a})]$, p. 176
$\varphi_K(\mathfrak{q})$	the Frobenius automorphism of \mathfrak{q} over K , p. 177
$\varphi_{\mathfrak{p}}^{(L)}$	the Frobenius automorphism of \mathfrak{p} in $\text{Gal}(L : K)$, p. 178
$w(K)$	$= \#(\mu(K))$, the number of roots of unity in the field K , p. 188
$\zeta(s)$	the Riemann zeta function, p. 192

$Z(s)$	the completed zeta function, p. 196
$\zeta_{\mathbb{Q}(\sqrt{m})}(s)$	Dedekind zeta function of a number field K , p. 198
$\zeta_C(s)$	the partial Dedekind zeta function of an ideal class of a number field, p. 198
$\delta(P)$	Dirichlet density of a collection P of prime ideals of a number field, p. 202
$[\![\sigma]\!]$	division represented by σ , p. 207
N_K	the conductor of an abelian number field K , p. 214
G^\vee	the character group of a group G , p. 215
f^\vee	the dual of a group homomorphism f , p. 215
\mathcal{D}_N	the group of Dirichlet characters modulo N , p. 218
$\bar{\chi}$	inverse of a Dirichlet character χ , p. 218
$i_N^M(\chi)$	Dirichlet character modulo N induced by $\chi \in \mathcal{D}_M$, p. 219
N_χ	the conductor of a Dirichlet character χ , p. 221
N_X	the conductor of a finite group X of Dirichlet characters, p. 222
$\mathcal{D}(K)$	the group of Dirichlet characters associated to an abelian number field K , p. 223
\mathbb{Q}_X	the number field associated to a finite group X of Dirichlet characters, p. 223
$L(s, \chi)$	the L series of a Dirichlet character, p. 226
$g(\chi)$	the standard Gauß sum of a Dirichlet character χ , p. 232
$g_k(\chi)$	a Gauß sum of a Dirichlet character χ , p. 232
\mathcal{C}_m	the group of cyclotomic units in $\mathbb{Q}(\zeta_m)$, p. 246
\mathcal{C}_m^+	the group of cyclotomic units in $\mathbb{Q}(\zeta_m + \zeta_m^{-1})$, p. 246
$\ \cdot\ _\sigma$	the absolute value given by the complex embedding σ , p. 256
$\ \cdot\ _v$	the absolute value determined by a discrete valuation, p. 256
$\mathcal{P}(K)$	the collection of primes of a number field K , p. 266
$\mathcal{P}_0(K)$	the collection of finite primes of a number field K , p. 266
$\mathcal{P}_\infty(K)$	the collection of infinite primes of a number field K , p. 266
\mathcal{O}_F	the valuation ring of a complete discretely valued field F , p. 271
v_F	the valuation of a complete discretely valued field F , p. 271
\mathfrak{p}_F	the maximal ideal of the valuation ring of a complete discretely valued field F , p. 271
k_F	the residue class field of a complete discretely valued field F , p. 271
$K_{\mathfrak{p}}$	the completion of a discretely valued field K at a maximal ideal \mathfrak{p} , p. 272

Notations

$R_{\mathfrak{p}}$	the valuation ring of the completion of a discretely valued field K at a maximal ideal \mathfrak{p} , p. 272
$\mathcal{O}_{\mathfrak{p}}$	the valuation ring of the completion of a number field K at a maximal ideal \mathfrak{p} , p. 272
$\hat{\mathfrak{p}}$	the maximal ideal of $\mathcal{O}_{\mathfrak{p}}$, p. 272
\mathbb{Q}_p	the field of p -adic numbers, p. 272
\mathbb{Z}_p	the ring of p -adic integers, p. 272
$e_F^{(E)}$	the ramification index of an extension of complete discretely valued fields, p. 274
$e_F^{(E)}$	the residue class degree of an extension of complete discretely valued fields, p. 274
exp	exponential function on a local field, p. 285
log	logarithm on a local field, p. 287
$\mathbb{Z}[G]$	the group ring of a group G , p. 294
$R[G]$	the group algebra over a commutative ring R of a group G , p. 294
N_G	the norm element in the group ring of a finite group G , p. 294
A^G	the subgroup of invariants of a module A over a group G , p. 294
A_G	the factor group of invariants of a module A over a group G , p. 295
$H_m(G, A)$	the m -th homology group of G with coefficients in A , p. 296
$H^m(G, A)$	the m -th cohomology group of G with coefficients in A , p. 296
$\hat{H}^m(G, A)$	m -th Tate cohomology group of a finite group G with coefficients in a G -module A , p. 296
N_A	multiplication by N_G of elements of a G -module A , the group G being understood, p. 296
Δ_A	multiplication by $\Delta = 1 - \sigma$ of elements of a cyclic G -module, the group G and its generator σ being understood, p. 296
$H^0(A)$	the 0-th cohomology group of a module A over a cyclic group, p. 297
$H^1(A)$	the 1-st cohomology group of a module A over a cyclic group, p. 297
$q(A)$	the Herbrand quotient of a module A over a cyclic group, p. 299
$\mathcal{G}(L : K)$	the category of all intermediate fields of a Galois extension $L : K$ and their K -embeddings, p. 305
$\mathcal{M}(K)$	the ordered monoid of moduli of a number field K , p. 320
$\mathbb{I}^{\mathfrak{m}}(K)$	the group of fractional ideals of a number field K ‘away’ from \mathfrak{m}_0 , p. 320
$K_{\mathfrak{m}}$	the localization of a number field K at the finite primes of a modulus \mathfrak{m} , p. 320

$K_{\mathfrak{m}}^1$	the subgroup of the multiplicative group of a number field K consisting of elements congruent to 1 modulo a modulus \mathfrak{m} , p. 320
$\mathbb{S}_{\mathfrak{m}}(K)$	the ray modulo a modulus \mathfrak{m} of a number field K , p. 321
$\mathcal{C}_{\mathfrak{m}}(K)$	the ray class group modulo a modulus \mathfrak{m} of a number field K , p. 321
$i_{\mathfrak{n}}^{\mathfrak{m}}(\chi)$	Dirichlet character modulo \mathfrak{n} , induced by a character modulo $\mathfrak{m} \mid \mathfrak{n}$, p. 330
f_{χ}	the conductor of a Dirichlet character χ of a number field, p. 331
$\mathcal{H}_{\mathfrak{m}}(K)$	the group of Dirichlet characters of a number field K with conductor a divisor of \mathfrak{m} , p. 331
f_X	the conductor of a finite group X of Dirichlet characters, p. 331
$\text{tr}_{K}^L(C)$	transfer of a $C \in \mathcal{C}_{\mathfrak{m}}(L)$ to $\mathcal{C}_{\mathfrak{m}}(K)$, p. 333
$\mathcal{C}_{\mathfrak{m}}(L : K)$	for $L : K$ a number field extension and \mathfrak{m} a modulus of K : the cokernel of the transfer from $\mathcal{C}_{\mathfrak{m}}(L)$ to $\mathcal{C}_{\mathfrak{m}}(K)$, p. 333
ν_L^K	the conorm map of Dirichlet characters of number fields, p. 333
$\mathcal{H}(L : K)$	the group of Dirichlet characters of a number field extension $L : K$, p. 333
$\mathcal{H}_{\mathfrak{m}}(L : K)$	for $L : K$ a number field extension and a modulus \mathfrak{m} of K : the Dirichlet characters of $L : K$ with conductor dividing \mathfrak{m} , p. 333
$\zeta(s, C)$	the partial zeta function of a ray class C of a number field, p. 334
$N(\mathfrak{m})$	the norm of a modulus \mathfrak{m} , p. 335
$\text{Reg}(\mathfrak{m})$	the regulator of a modulus \mathfrak{m} , p. 335
$L(s, \chi)$	the L -series of a Dirichlet character of a number field, p. 337
$f_K(L)$	the conductor of an abelian extension $L : K$ of number fields, p. 339
$\mathbb{I}^L(K)$	for $L : K$ an abelian number field extension the subgroup of $\mathbb{I}(K)$ generated by the nonramifying prime ideals of K , p. 340
$\varphi_K^{(L)}$	the Artin map of an abelian number field extension $L : K$, p. 340
K_X	the class field for a finite group of Dirichlet characters of a number field K , p. 343
$\check{\varphi}_K^{(L)}$	the dual Artin isomorphism of an abelian number field extension $L : K$, p. 362
K^S	the group of S -units of a number field K , p. 376
$\mathcal{C}^S(K)$	the S -ideal class group of a number field K of a saturated collection S of primes, p. 376
K_X	the class field for a finite group X of Dirichlet characters of a number field K , p. 379
$\vartheta_K^{(L)}$	global description of the local Artin map, p. 388
$\vartheta_{\mathfrak{p}}^{(L)}$	the local Artin map at \mathfrak{p} , p. 389

Notations

$U_{\mathfrak{p}}^{(n)}$	a subgroup of $K_{\mathfrak{p}}^*$, see Notation 15.54, p. 393
$\mathfrak{f}_{\mathfrak{p}}(L)$	the local conductor of an abelian extension $L : K$ of number fields at a prime \mathfrak{p} of K , p. 393
$\iota_K^{K'}$	the canonical map $\mathcal{H}(K') \rightarrow \mathcal{H}(K)$ for a number field extension $K' : K$, p. 394
$\varphi_K^{(L)}$	the generalized Artin map of a Galois extension $L : K$, p. 394
$\check{\varphi}_K^{(L)}$	the generalized dual Artin map of a Galois extension $L : K$, p. 395
V_H^G	the transfer from a Group G to a subgroup H of finite index, p. 397
$\vartheta_F^{(E)}$	the Artin map of an extension $E : F$ of local fields, p. 409
F_X	the class field for a subgroup of finite index of F^* for a local field F , p. 411
$U_F^{(i)}$	for F a local field a subgroup of F^* as described in 16.16, p. 413
$\mathfrak{f}_F(E)$	the conductor of an extension $E : F$ of local fields, p. 413
$\left(\frac{a, L : K}{\mathfrak{p}}\right)$	the value in a of the norm residue symbol of an abelian number field extension $L : K$ at a prime \mathfrak{p} , p. 415
$(\alpha, \beta)_n$	the n -th Hilbert symbol for α, β in a given local field, p. 417
$\left(\frac{a, b}{\mathfrak{p}}\right)_n$	the n -th Hilbert symbol at a prime \mathfrak{p} of a given number field, p. 417
$(a, b)_v$	the tame symbol on a given discretely valued field, p. 421
$\left(\frac{\alpha}{\mathfrak{p}}\right)_n$	the n -th power residue symbol, p. 423
$\left(\frac{\alpha}{\mathfrak{b}}\right)_n, \left(\frac{\alpha}{\beta}\right)_n$	generalizations of the Jacobi symbol, p. 424
$i(\sigma)$	for σ an automorphism of a local field, the least exponent i such that σ does not induce the identity modulo the prime ideal to the power i , p. 438
φ_G	continuous piecewise linear function determined by the orders of the ramification groups, p. 441
$\psi_G(x)$	the inverse map of $\varphi_G(x)$, p. 442
$*\mathfrak{a}$	the dual of the fractional ideal \mathfrak{a} , p. 448
$\mathfrak{c}_R(L)$	the complementary fractional ideal of L over R , p. 449
$\partial_R(L)$	the different of L over R , p. 449
$\partial_K(L)$	for a number field extension $L : K$ the different of L over K , p. 449
$\partial_K^L(\alpha)$	the different of $\alpha \in L$ over K , p. 453
$\partial_F(E)$	the different of an extension $E : F$ of local fields, p. 455

$V_{F,i}(E)$	the i -th ramification group of a Galois extension $E : F$ of local fields, p. 455
$W_F^{(i)} E$	the image of $U_F^{(i)}$ in the Galois group of a Galois extension of local fields under the local Artin map, p. 458
$\Omega(G)$	the collection of cyclic subgroups of a finite group G , p. 472
$\Omega_0(G)$	the collection of nontrivial cyclic subgroups of a finite group G , p. 472
$\Omega'(G)$	the collection of noncyclic subgroups of a finite group G , p. 472
$\Sigma(G)$	the collection of subgroups of a finite group G , p. 472
$\Sigma_0(G)$	the collection of nontrivial subgroups of a finite group G , p. 472
$\Upsilon(G)$	the collection of normal subgroups H of G such that G/H is a finite cyclic group, p. 472
$\Upsilon_0(G)$	the collection of $H \neq G$ in $\Upsilon(G)$, p. 472
$\mathbb{Z}X$	the free abelian group on a set X , p. 472
$\text{NR}(G)$	the group of norm relations of a finite group G , p. 472
$d_G(H)$	the norm coefficient of a subgroup H of a finite group G , p. 473
ε_χ	idempotent related to $\chi \in G^\vee$ in the group algebra over $\mathbb{Z}[\frac{1}{n}, \zeta_n]$ of an abelian group G , p. 477
$\Upsilon(G)$	the collection of subgroups H of an abelian group G with G/H cyclic, p. 478
V^\perp	for V a subgroup of the dual of a given abelian group G : the subgroup of G on which all $\chi \in V$ vanish, p. 478
U^\perp	for U a subgroup of a given abelian group G : the group of all $\chi \in G^\vee$ vanishing on U , p. 478
ε_H	idempotent in the group ring of an abelian group G related to a subgroup H with G/H cyclic, p. 479
$\mathbf{1}_G$	trivial character of a group G , p. 493
$\mathcal{L}(s, \chi, L : K)$	Artin L -function of a Galois extension of number fields, p. 494
$D(G)$	the intersection of all maximal cyclic subgroups of a group G , p. 500
$S^\#$	the base of a topology generated by a subbase S , p. 506
$\varinjlim_i X_i$	the inductive limit of an inductive system $(X_i)_{i \in I}$, p. 511
$\varprojlim_i X_i$	the projective limit of a projective system $(X_i)_{i \in I}$, p. 514
G^{ab}	the abelianization of a profinite group G , p. 524
K^{sep}	the separable closure of a field K , p. 527
$\text{Gal}(K)$	the absolute Galois group of a field K , p. 527
\mathcal{F}_K	the inductive system of finite Galois extensions of a field K , p. 527
K^{ab}	the maximal abelian extension of a field K , p. 528

Notations

\mathcal{A}_K	the inductive system of finite abelian extensions of a field K , p. 528
ϑ_F	the local reciprocity map for F a local field, p. 528
$\text{Hom}_{\text{cont}}(G, H)$	the set of continuous homomorphisms from a topological group G to a topological group H , p. 529
\mathcal{T}	the category of abelian discrete torsion groups, p. 529
\mathcal{P}	the category of abelian profinite groups, p. 529
\mathbb{S}^1	the circle group, p. 529
$\mathbb{A}^S(K)$	the ring of S -adèles of a number field K for a saturated collection S of primes, p. 533
$\mathbb{A}(K)$	the adèle ring of a number field K , p. 534
$\prod_{\mathfrak{p}} K_{\mathfrak{p}}$	the restricted product of the completions of a number field K (= adèle ring of K), p. 534
$\mathbb{J}^S(K)$	the S -idèle group of a number field K , p. 536
$\mathbb{J}(K)/K^*$	the idèle class group of a number field K , p. 537
$\mathbb{J}^S(K)/K^S$	the S -idèle class group of a number field K for a saturated collection S of primes, p. 537
$\ \alpha\ _{\mathfrak{p}}$	the \mathfrak{p} -value of an idèle α , p. 538
$\ \alpha\ $	the content of an idèle α , p. 538
$J_0(K)$	the group of idèles with content 1 of a number field K , p. 538
$J_0(K)$	the group of idèles with content 1 of a number field K , p. 538
$C_0(K)$	the group of idèle classes of a number field K represented by idèles of content 1, p. 538
$W_{\mathfrak{m}}(K)$	the group of idèles of a number field K which are 1 modulo a modulus \mathfrak{m} , p. 540
$C_{\mathfrak{m}}(K)$	the idèles class group modulo a modulus \mathfrak{m} of a number field K , p. 540
$L_{\mathfrak{p}}$	for $L : K$ a numberfield extension and \mathfrak{p} a prime of K : the product of all $L_{\mathfrak{q}}$, where \mathfrak{q} above \mathfrak{p} , p. 544
$N_K^L(\alpha)$	the norm of the adèle $\alpha \in \mathbb{A}(L)$, p. 546
$N_K^L(\bar{\alpha})$	the norm of the class of the idèle $\alpha \in \mathbb{J}(L)$, p. 546
$\mathcal{C}(L : K)$	idèle class group associated with a number field extension $L : K$, p. 546

Index

- abelian number field
 - associated to a group of Dirichlet characters, 223
- abelianization
 - of a profinite group, 524
- abscissa of convergence, 193
- absolute extension
 - of number fields, 145
- absolute value, 255
 - archimedean, 259
 - equivalence, 257
 - nonarchimedean, 259
 - place, 257
- action of $GL_2(\mathbb{Z})$ on $\mathbb{C} \setminus \mathbb{Q}$, 72
- adèle
 - of a number field, 533
- adèle ring
 - of a number field, 534
- Alexander's Subbase Theorem, 507
- algebraic integer, 6
- algebraic K-theory, 419, 422
- arithmetic function, 196
 - completely multiplicative, 196
 - multiplicative, 196
- arithmetic projective system, 323
 - multiplicative, 323
 - quasi-multiplicative, 323
- Artin L -function, 494
- Artin kernel
 - of an abelian extension of number fields, 340
- Artin map, 340
 - for local fields, 409
 - local, 389
- Artin symbol, 340
- Artin's Reciprocity Law, 358
- base
 - generated by a subbase, 506
 - of a topology, 506
- bicartesian, 217
- cancellation law, 34
- cartesian square, 217
- Cauchy sequence, 262
- central function
 - on a group, 493
- character
 - induced, 495
 - of a group, 215
 - of a representation, 493
 - principal, 215, 493
 - trivial, 215, 493
- character group, 215
- characteristic polynomial, 9
- Chebotarev's Density Theorem, 382
- class field
 - for a finite group of Dirichlet characters, 343, 363
- class number
 - of a number field, 191
- class number formula, 201
- Classification Theorem
 - for abelian number fields, 223
 - global
 - idèlic version, 547
 - ideal-theoretic version, 379
 - local, 412
- CM-field, 124

- cocartesian square, 217
- cofinal subset, 517
- cohomology group, 297
- cohomology groups
 - of a group action, 296
- comaximal ideals, 38
- complementary fractional ideal, 449
- complete field, 262
- Complete Splitting Theorem, 386
- completed zeta function, 196
- completely multiplicative arithmetic function, 196
- completion of a valued field, 262
 - construction, 262
- complex embedding, 5
- complex infinite prime
 - of a number field, 266
- conductor
 - of a Dirichlet character, 221, 222
 - of a Dirichlet character of a number field, 331
 - of a finite group of Dirichlet characters, 222
 - of a finite group of Dirichlet characters of a number field, 331
 - of an abelian number field, 214
 - of an extension of abelian number fields, 339
 - of an extension of local fields, 413
- conductor of a quadratic number field, 214
- Conductor-Discriminant Formula, 250
 - local, 467
- Conductor-Discriminant Formula (global), 468
- conorm map
 - for Dirichlet characters, 333
- consistency property
 - for Artin maps, 342
 - for local Artin maps, 390
- content
 - of an idèle, 538
- continued fraction, 79
- continued fraction expansion, 83
 - period of repeating, 83
 - purely repeating, 83
 - repeating, 83
- convergent sequence, 262
 - limit, 262
- converging infinite product, 196
- convex subset of \mathbb{R}^n , 107
- cyclotomic unit, 246
- decomposition field, 160
- decomposition group, 160, 162
 - of an infinite prime, 268
- Dedekind domain, 34
- Dedekind zeta function, 198
 - partial, 198
- degree
 - of a rational function, 142
 - of number field, 3
- different, 449
 - of an element, 453
 - of an extension of local fields, 455
- directed ordered set, 510
- Dirichlet character, 218
 - associated to an abelian number field, 223
 - conductor, 221
 - even, 223
 - inverse, 218
 - modulus, 218
 - odd, 223
 - of a number field, 329
 - primitive, 219, 330
 - principal, 219
 - product, 218, 219
 - quadratic, 218
 - trivial, 219
- Dirichlet characters
 - product, 221
- Dirichlet density, 202
- Dirichlet pre-character, 221, 331
- Dirichlet series, 192
- Dirichlet's Unit Theorem, 119
- discrete subgroup
 - of \mathbb{R}^n , 105

- discrete valuation, 131
- discrete valuation ring, 132
- discriminant, 155, 159
 - of a basis, 15
 - of a number field, 20
 - of a quadratic number, 71
- divisible abelian group, 215
- division
 - of a group, 207
 - of ideals, 34
- dual
 - of a fractional ideal, 448
 - of a group, 215
 - of a group homomorphism, 215
- dual Artin isomorphism, 362
- dual basis, 17
- dual group, 215

- Eisenstein \mathfrak{p} -polynomial, 153
- Eisenstein's Reciprocity Theorem, 434
- embedding
 - of valued fields, 255
- equivalence
 - of ideals of a Dedekind domain, 40
 - of irrational numbers, 72
 - of lattices, 73
- Euler product, 196
 - of a Dirichlet series, 196
- Euler's criterion, 66
- exact hexagon, 297
- exceptional collection of subgroups, 499
- exceptional group, 498
- Existence Theorem
 - local, 412
- exponent of a group, 295
- exponential function
 - on a local field, 285

- finite prime
 - of a number field, 266
- First Fundamental Inequality, 339
- fractional ideal
 - invertible, 43
 - of a Dedekind domain, 42
 - of a number field, 59
 - principal, 42
- Frobenius automorphism, 178
 - of a prime ideal, 177
- Frobenius Density Theorem, 207
 - for abelian extensions, 206
- functor, 215
 - contravariant, 215
 - left exact, 215
- fundamental parallelootope, 106
- fundamental unit, 14

- Galois cohomology, 293
- Galois extension
 - infinite, 524
- Galois group
 - absolute, 527
- Galois module, 305, 306
 - acyclic, 309
 - with descent, 306
 - with transfers, 308
- Gauß Lemma, 7
- Gauß sum
 - of a Dirichlet character, 232
- generalized Artin map, 394
- generalized dual Artin map, 395
- generalized Frobenius automorphism, 394

- genus
 - of a number field, 199
- group action
 - co-invariants, 295
 - invariants, 294
- group algebra, 294
- group invariants, 95
- group ring, 294

- Hasse index, 125
- Hasse's Principle, 355
- Hausdorff topological space, 507
- herbrand quotient, 299
- Hilbert class field, 344, 399
- Hilbert symbol, 417

- tame, 422
- wild, 422
- Hilbert's Reciprocity, 425
- Hilbert's Reciprocity Theorem, 425
 - First supplement, 426
 - Second supplement, 426
- Hilbert's Theorem 90, 302
- homology groups
 - of a group action, 296
- idèle
 - of a number field, 536
- idèle class group
 - modulo a modulus of a number field, 540
 - of a number field, 537
- idèle class group associated with a number field extension, 546
- ideal class
 - of a Dedekind domain, 41
- ideal class group
 - of a Dedekind domain, 41
 - of a number field, 59
- imaginary quadratic number field, 3
- induced Dirichlet character, 219, 330
- inductive limit, 511
- inductive system
 - in a category, 510
- inertia group, 161, 162
 - of an infinite prime, 268
- infinite continued fraction, 82
- infinite prime
 - of a number field, 266
- injective module, 215
- integer, 6
- integers
 - of a quadratic number field, 7
- integral basis, 20
- integral closure, 6
- integrally closed, 6
- irreducible
 - character, 493
 - representation, 493
- Jacobi symbol, 69
- Krasner
 - lemma, 279
- Kronecker-Weber
 - Theorem, 214
- Kronecker-Weber Theorem, 364
- Krull dimension
 - of a commutative ring, 35
- Kummer extension, 371
- Kummer-Dedekind Theorem, 51, 149
- L -series
 - of a Dirichlet character, 226, 337
- lattice
 - in a \mathbb{Q} - or \mathbb{R} -vector space, 4
- leading coefficient
 - of a rational function, 142
- Legendre symbol, 66, 218
- Lipschitz map, 185
- local Artin map, 389
- Local Classification Theorem, 412
- local conductor, 393
- Local Existence Theorem, 412
- local field, 279
- local norm, 415
- localization
 - at a prime ideal, 134
 - of a Dedekind domain, 137
- logarithm
 - on a local field, 287
- maximal abelian extension
 - of a field, 528
- mesh
 - of a lattice in \mathbb{R}^n , 106
- Minkowski bound, 111
- Minkowski's Lattice Point Theorem, 107, 108
- module
 - over a group, 293
- modulus
 - for an abelian number field extension, 341

- of a number field, 320
- Moore's Reciprocity Uniqueness Theorem, 423
- Mordell equation, 32
- morphism of arithmetic projective systems, 327
- multiplicative arithmetic function, 196
- multiplicative function
 - of ideals, 200
- multiplicative system, 133

- narrow ideal class group, 143
- Noetherian ring, 35
- norm
 - global, 276
 - local, 276
 - of a finite field extension, 9
 - of a modulus, 335
 - of an ideal, 57
 - of fractional ideal, 174
 - on $\mathbb{R}^r \times \mathbb{C}^s$, 12
- norm coefficient
 - of a subgroup of a finite group, 473
- norm element, 294
- norm map
 - for adèles, 546
 - for idèle classes, 546
- norm relation
 - of a finite group, 472
- norm residue symbol, 415
- norm-Euclidean, 27
- normalizer of a subgroup, 168
- null sequence, 262
- number field, 3
 - degree, 3
 - quadratic, 3
 - imaginary, 3
 - real, 3
 - ring of integers, 9
- number ring, 4

- Ostrowski
 - theorem, 261, 264

- p -adic expansion, 272
- p -adic numbers, 272
- \mathfrak{p} -adic valuation
 - of a fractional ideal, 43
 - on a field of fractions of a Dedekind domain, 43
- \mathfrak{p} -polynomial, 153
- \mathfrak{p} -valuation
 - of a ring element, 37
 - of an ideal, 37
- p -value
 - of an idèle, 538
- partial zeta function
 - of a ray class, 334
- Pell equation, 95
- place
 - of a field, 257
- primary element
 - in $\mathbb{Z}[\zeta_l]$, l an odd prime, 433
- prime
 - of a number field, 266
- principal character, 219, 493
- principal fractional ideal, 42
- principal norm relation
 - of a finite group, 474
- product
 - of characters, 215
 - of Dirichlet characters, 219
 - of fractional ideals, 42
 - of ideals, 33
 - of topological spaces, 506
- product formula
 - for absolute values of a number field, 266
 - for norm residue symbols, 415
- profinite group, 521
 - abelianization, 524
- projective limit, 514
- projective system
 - in a category, 514
- pure cubic number field, 31

- quadratic nonresidue, 53
- quadratic number, 71

- reduced real, 86
- quadratic number field, 3
- Quadratic Reciprocity Law, 67, 178
- quadratic residue, 53
- ramification
 - of infinite primes, 267
- ramification group, 169
 - of a Galois extension of local fields, 455
- ramification index, 50, 56, 146, 151
 - of an extension of complete discretely valued fields, 274
 - of infinite primes, 267
- ramify, 148
- ray, 321
- ray class group, 321
- real embedding, 4
- real infinite prime
 - of a number field, 266
- real quadratic number field, 3
- reduced real quadratic number, 86
- regular representation, 493
- regulator
 - of a group of units, 128
 - of a modulus, 335
 - of a number field, 128
- relative extension
 - of number fields, 145
- relatively prime
 - ideals of s Dedekind domain, 38
- remain prime, 50, 148
- representation
 - character, 493
 - degree, 293
 - induced, 495
 - irreducible character, 493
 - of a group, 293
 - principal character, 493
 - regular, 493
- residue class degree, 50, 56, 151
 - absolute, 205
 - of an extension of complete discretely valued fields, 274
 - of infinite primes, 267
- residue class index, 146
- restricted product
 - of completions of a number field, 534
- Riemann zeta function, 192
- ring of integers
 - of a number field, 9
- S -ideal class group, 376
- S -unit, 376
- saturated collection of primes, 376
- Second Fundamental Inequality, 354
- semi-local commutative ring, 40
- separable closure
 - of a field, 527
- separated points
 - of a topology, 508
- spectrum
 - of a ring, 35
- split completely, 50, 148
- Steinberg symbol, 419
- strongly exceptional group, 498
- subbase
 - of a topology, 506
- Subsidiary Law
 - for quadratic reciprocity, 68
- sum
 - of ideals, 33
- symmetric subset of \mathbb{R}^n , 107
- tail equivalence of numbers, 87
- tame kernel
 - of a number field, 422
- tame symbol, 421
- tamely ramified, 149
- Tate cohomology groups, 296
- The Fundamental Equality, 354
- topological group, 508
- topological space
 - Hausdorff, 507
- totally disconnected topology, 508
- totally positive
 - element of a number field, 143

- totally ramify, [50](#), [148](#)
- totally separated topology, [508](#)
- trace
 - global, [276](#)
 - local, [276](#)
 - of a finite field extension, [9](#)
- transfer
 - for ray class groups, [333](#)
 - of a Galois module, [308](#)
 - of an ideal class, [175](#)
 - of groups, [397](#)
- transition matrix, [15](#)
- Translation Theorem, [365](#)
- trivial absolute value, [256](#)
- trivial norm coefficient, [474](#)
- Tykhonov's Theorem, [507](#)
- uniformizer
 - of a complete discretely valued field, [270](#)
 - of a discrete valuation, [133](#)
- unique factorization into prime ideals, [36](#)
- unit index
 - of a CM-field, [125](#)
- valuation ring
 - of a nonarchimedean absolute value, [260](#)
- valued field, [255](#)
 - completion, [262](#)
- Vandiver's Conjecture, [112](#)
- wild inertia group, [172](#)
- wild kernel
 - of a number field, [423](#)
- Zariski topology, [35](#)
- zeta function
 - completed, [196](#)
 - of a ray class, [334](#)

Number Fields is a textbook for algebraic number theory. It grew out of lecture notes of master courses taught by the author at Radboud University, the Netherlands, over a period of more than four decades. It is self-contained in the sense that it uses only mathematics of a bachelor level, including some Galois theory.

Part I of the book contains topics in basic algebraic number theory as they may be presented in a beginning master course on algebraic number theory. It includes the classification of abelian number fields by groups of Dirichlet characters. Class field theory is treated in Part II: the more advanced theory of abelian extensions of number fields in general. Full proofs of its main theorems are given using a 'classical' approach to class field theory, which is in a sense a natural continuation of the basic theory as presented in Part I. The classification is formulated in terms of generalized Dirichlet characters. This 'ideal-theoretic' version of class field theory dates from the first half of the twentieth century. In this book, it is described in modern mathematical language. Another approach, the 'idèlic version', uses topological algebra and group cohomology and originated halfway the last century. The last two chapters provide the connection to this more advanced idèlic version of class field theory.

The book focuses on the abstract theory and contains many examples and exercises. For quadratic number fields algorithms are given for their class groups and, in the real case, for the fundamental unit. New concepts are introduced at the moment it makes a real difference to have them available.

ISBN 978-94-9329-603-9



9 789493 296039 >

Radboud University



www.radbouduniversitypress.nl