Cover Page

Universiteit Leiden

Author: Dalla Torre G.
Title: The unit residue group
Issue Date: 2019-12-18

The unit residue group

Proefschrift

ter verkrijging van
de graad van Doctor aan de Universiteit Leiden,
op gezag van Rector Magnificus prof. mr. C. J. J. M. Stolker,
volgens besluit van het College voor Promoties
te verdedigen op woensdag 18 december 2019
klokke 12:30 uur

door

Gabriele Dalla Torre,

geboren te Trento, Italië,
in 1983

Promotor
prof. dr. H. W. Lenstra

Promotiecommissie
prof. dr. P. Stevenhagen (*voorzitter*, Universiteit Leiden)
prof. dr. R. M. van Luijk (*secretaris*, Universiteit Leiden)
prof. dr. Roberto Dvornicich (Università di Pisa)
prof. dr. R. J. Schoof (Università degli Studi di Roma Tor Vergata)

The unit residue group

Gabriele Dalla Torre

Gabriele Dalla Torre, Leiden, 2019
gabrieledallatorre@gmail.com

The cover illustration shows the painting *A Windmill on a polder waterway*, known as *In the month of July*, by Paul Joseph Constantin Gabriël, c. 1889. The original painting is in the Rijksmuseum in Amsterdam.

Contents

1 Introduction **1**
1.1 Quadratic reciprocity . . . 2
1.2 The Jacobi symbol . . . 3
1.3 Orthogonal primes . . . 5
1.4 The norm-residue symbol . . . 7
1.5 Orthogonality . . . 10
1.6 Global formulation . . . 12
1.7 Overview . . . 15
1.8 Skew abelian groups . . . 16
1.9 The local norm-residue symbol . . . 17
1.10 The global norm-residue symbol . . . 18
1.11 The unit residue group . . . 19
1.12 Quadratic number fields . . . 20
1.13 Two-ranks of ideal class groups . . . 21
1.14 Biquadratic number fields . . . 22
1.15 Cyclic number fields . . . 22
1.16 A large norm group . . . 23
1.17 Quadratic characters . . . 24

2 Skew abelian groups **25**
2.1 Preliminaries . . . 25
2.2 The classification . . . 29
2.3 Examples . . . 32
2.4 Pairings . . . 36
2.5 Antisymmetric pairings . . . 37
2.6 Wall's results . . . 43

3 The local norm-residue symbol **45**
3.1 Topological algebra . . . 45
3.2 Local fields . . . 47
3.3 Abelian Kummer theory . . . 51
3.4 Local class field theory . . . 53
3.5 The norm-residue symbol . . . 57
3.6 A new elementary characterization . . . 61
3.7 Archimedean local fields . . . 63
3.8 Non-Archimedean local fields . . . 64
3.9 Functorial properties . . . 72
3.10 The field of two-adic rationals and its unramified extensions . . . 72

4 The global norm-residue symbol **77**
4.1 Global fields . . . 77
4.2 Adeles and ideles . . . 79
4.3 Locally compact abelian groups . . . 82
4.4 Self-duality . . . 85
4.5 Function fields . . . 88
4.6 The Tate pairing . . . 93
4.7 The Arakelov class group . . . 95
4.8 Number fields . . . 98

5 The unit residue group **103**
5.1 Definitions and general results . . . 104
5.2 The virtual group . . . 111
5.3 The field of rational numbers . . . 115

6 Quadratic number fields and a biquadratic example **117**
6.1 Introduction . . . 117
6.2 Discriminants of quadratic number fields . . . 119
6.3 Unramified extensions . . . 119
6.4 The two-adic component of the unit residue group . . . 122
6.5 Imaginary quadratic number fields . . . 125
6.6 Real quadratic number fields . . . 129
6.7 The number field $\mathbb{Q}(\mathrm{i}, \sqrt{30})$ . . . 134

7 Two-ranks of ideal class groups **137**
7.1 Results . . . 137
7.2 Armitage–Fröhlich's theorem . . . 139
7.3 Proof of the main theorem . . . 140

8 Three-ranks of ideal class groups of quadratic number fields 143
8.1 Introduction 143
8.2 Two results on modules 146
8.3 Galois group decompositions of modules 147
8.4 Scholz's theorem 151
8.5 Dutarte's probabilistic model 152
8.6 Some consequences 154

9 Cyclic number fields 161
9.1 Introduction 161
9.2 Group rings 164
9.3 Number fields unramified at two 168
9.4 Cubic and quintic number fields 171

10 A large norm group 175
10.1 Main results 175
10.2 Auxiliary results 177
10.3 Proofs of the main results 180

11 Quadratic characters 183
11.1 Main result 183
11.2 Introduction 184
11.3 L-series 185
11.4 Lemmas 186
11.5 Proof of the main theorem 190

Bibliography 195

Summary 201

Samenvatting 203

Curriculum vitae 205

CHAPTER 1

Introduction

The unit residue group, to which the present thesis is devoted, is defined using the *norm-residue symbol*, which Hilbert introduced into algebraic number theory in 1897. This symbol is a bimultiplicative map whose values are roots of unity. If we just work with the field of rational numbers, as we shall do for now, those roots of unity are only 1 and -1.

One of the most famous theorems in elementary number theory is the *quadratic reciprocity law*, proved by Gauss in 1801, which expresses an unexpected symmetry property of the *Legendre symbol*. The norm-residue symbol enables us to reformulate the quadratic reciprocity law, together with its two supplementary laws, in terms of bilinear forms on vector spaces over the field of two elements. This reformulation is not only concise and elegant, but it also places the quadratic reciprocity law in the context of linear algebra. In addition, it points the way to higher reciprocity laws in algebraic number fields.

In Sections 1.1 to 1.6, everything we just mentioned, including the unit residue group, will be explained for the field of rational numbers. Section 1.7 is an overview of the content of the thesis and in Sections 1.8 to 1.17 we outline the main results of each chapter.

1.1 Quadratic reciprocity

Gauss called the quadratic reciprocity law both "Theorema aureum" (golden theorem) and "Theorema fundamentale". In his Disquisitiones Arithmeticae [21, article 131] he explained the latter name as follows: "Quia omnia fere, quae de residuis quadraticis dici possunt, huic theoremati innituntur, denominatio *theorematis fundamentalis*, qua in sequentibus utemur, haud absona erit."[1] More than one hundred people published proofs of this law since Gauss proved it in 1801. The formulation chosen here uses the Legendre symbol, which was introduced by Legendre in 1798 in his Théorie des nombres [36].

Definition 1.1 (Legendre symbol)**.** Let p be an odd prime number. For every integer a, the *Legendre symbol* $\left(\frac{a}{p}\right)$ is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} -1 & \text{if the equation } x^2 \equiv a \bmod p \text{ has no solution in } \mathbb{Z}/p\mathbb{Z}, \\ 1 & \text{if the equation } x^2 \equiv a \bmod p \text{ has a nonzero solution in } \mathbb{Z}/p\mathbb{Z}, \\ 0 & \text{if } p \text{ divides } a. \end{cases}$$

Theorem 1.2 (Quadratic reciprocity law (Gauss 1801))**.** *Let p and q be two distinct odd prime numbers. Then one has*

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

In other words, the symbols $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$ are equal unless p and q are both congruent to 3 modulo 4, in which case they are different. At first glance, one may not expect any connection between the two symbols, because one is defined by a congruence modulo q and the other one by a congruence modulo p, and p and q are coprime. Many number theorists view the quadratic reciprocity law as a miracle that is not explained away by any of its many proofs.

The behaviour of -1 and 2 modulo an odd prime number is governed by two other laws, called first supplement to the quadratic reciprocity law and second supplement to the quadratic reciprocity law, respectively.

Theorem 1.3 (First supplement to the quadratic reciprocity law)**.** *Let p be an odd prime number. Then one has*

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

[1] "Since almost everything that can be said about quadratic residues depends on this theorem, the term *fundamental theorem* which we will use from now on should be acceptable." Translation into English by Clarke [20].

Theorem 1.4 (Second supplement to the quadratic reciprocity law)**.** *Let p be an odd prime number. Then one has*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

In other words, the symbol $\left(\frac{-1}{p}\right)$ equals 1 if and only if $p \equiv 1 \bmod 4$, and the symbol $\left(\frac{2}{p}\right)$ equals 1 if and only if $p \equiv \pm 1 \bmod 8$.

Some traces of these laws, in particular of the first supplement, can be found in Fermat's theorems about expressing a prime by a quadratic form around the mid 1600's [37, pp. 2–3]. During the 18th century Euler studied Fermat's work. He made conjectures equivalent to the quadratic reciprocity law in 1744 [37, p. 4] and proved that for each prime p congruent to 1 modulo 8 the equation $x^2 \equiv 2 \bmod p$ has a solution in $\mathbb{Z}/p\mathbb{Z}$ [27, p. 70]. In 1785 Legendre discovered the laws independently of Euler and gave an incomplete proof [35]. The first full proof was given by Gauss in the Disquisitiones Arithmeticae [21] in 1801.

For more details about the history of the quadratic reciprocity law we refer to the books by Lemmermeyer [37] and Weil [77].

1.2 The Jacobi symbol

A result closely related to the quadratic reciprocity law is Euler's criterion.

Theorem 1.5 (Euler's criterion (Euler 1748))**.** *Let p be an odd prime. Then for every integer a one has*

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

From Euler's criterion it follows immediately that the Legendre symbol is a *completely multiplicative* function of its top argument, that is for all $a, b \in \mathbb{Z}$ one has

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Formulated in group theory language, the Legendre symbol induces a group homomorphism

$$(\mathbb{Z}/p\mathbb{Z})^* \to \{\pm 1\}$$

with kernel the subgroup $(\mathbb{Z}/p\mathbb{Z})^{*2}$ of squares.

When computing Legendre symbols, the quadratic reciprocity law makes it possible to turn symbols upside down. Hence, it is natural to extend the symbol to a function in two arguments. In 1837 Jacobi introduced a generalization of the Legendre symbol.

Definition 1.6 (Jacobi symbol)**.** Let a be an integer and let n be an odd integer. When n is positive, the *Jacobi symbol* $\left(\frac{a}{n}\right)$ is defined by

$$\left(\frac{a}{n}\right) = \prod_i \left(\frac{a}{p_i}\right)^{e_i},$$

where $n = \prod_i p_i^{e_i}$ is the prime factorization of n. When n is negative, it is defined by

$$\left(\frac{a}{n}\right) = \begin{cases} -\left(\frac{a}{-n}\right) & \text{if } a < 0, \\ \left(\frac{a}{-n}\right) & \text{if } a \geq 0. \end{cases}$$

Not everybody agrees on our definition of the Jacobi symbol: it is often defined only for odd positive integers n and is sometimes defined for odd negative integers n by $\left(\frac{a}{n}\right) = \left(\frac{a}{|n|}\right)$. Our choice makes it a restriction of the Kronecker symbol and is motivated by Theorem 1.7. The supplements to the quadratic reciprocity law generalize to the Jacobi symbol without amendment.

The Jacobi symbol equals the Legendre symbol when the denominator is a prime number and provides an efficient algorithm to calculate all Legendre symbols without performing factorization along the way. The quadratic reciprocity law for the Jacobi symbol is slightly different from the one for the Legendre symbol, because it also needs to take into account the sign of the arguments of the symbol.

Theorem 1.7 (Quadratic reciprocity law and its supplements for the Jacobi symbol)**.** *Let a and b be two odd coprime integers. Then one has*

$$\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}}, \quad \left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}}, \quad \left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = \langle a, b\rangle_{-1} \cdot \langle a, b\rangle_2,$$

where

$$\langle a, b\rangle_{-1} = \begin{cases} -1 & \text{if both } a \text{ and } b \text{ are negative} \\ 1 & \text{if at least one of } a \text{ and } b \text{ is positive} \end{cases}$$

and

$$\langle a, b\rangle_2 = \begin{cases} -1 & \text{if both } a \text{ and } b \text{ are congruent to } 3 \text{ modulo } 4, \\ 1 & \text{if at least one of } a \text{ and } b \text{ is congruent to } 1 \text{ modulo } 4. \end{cases}$$

The Jacobi symbol is a *bimultiplicative* function of its two arguments, that is it is a completely multiplicative function of each of its arguments when the other one is fixed. The quadratic reciprocity law implies that it is not

symmetric. If we restrict the domain of the Jacobi symbol by requiring that a and n are coprime in Definition 1.6, then it takes values in the multiplicative group $\{\pm 1\}$, which is isomorphic to the additive group $\mathbb{Z}/2\mathbb{Z}$. Moreover, it is well-defined modulo squares. Since the quotient group $\mathbb{Q}^*/\mathbb{Q}^{*2}$ is a vector space over $\mathbb{Z}/2\mathbb{Z}$ with the addition modulo 2 defined as multiplication modulo squares, the Jacobi symbol is reminiscent of bilinear forms on vector spaces over the finite field of two elements.

1.3 Orthogonal primes

In this section we turn the quadratic reciprocity law and its supplements into linear algebra using the bilinear map called the norm-residue symbol. We rephrase the statements of the laws in terms of bilinear forms on vector spaces over the finite field of two elements. This formulation has the advantages of compactness, symmetry, and generality. It combines three messy identities into one beautiful mathematical structure. The role of the prime 2 is less exceptional than before and there are no coprimality constraints on the arguments of the norm-residue symbol. Moreover, since the norm-residue symbol is defined on every local field, and all completions of number fields are local fields, this way of expressing the quadratic reciprocity law can be extended to any number field. In order to make the section more broadly accessible, we postpone some technical details and proofs to later sections.

We start by defining some vector spaces. Instead of taking the multiplicative group of the field of rational numbers modulo squares, we mod out $\mathbb{Q}^*$ by each of the subgroups consisting of the elements that are locally squares, as explained in Remark 1.13 . We get finite groups of exponent 2. The vector space structure may cause confusion: the vector addition is the usual multiplication and the scalar multiplication is the exponentiation.

Notation 1.8. Let T be the set of integers consisting of -1 and all the primes. For each r in T we define the group J_r by

$$J_r = \begin{cases} \mathbb{Q}^*/\mathbb{Q}_{>0} & \text{if } r = -1, \\ \mathbb{Q}^*/(\mathbb{Q}^{*2} \cdot \langle 1 + 8\mathbb{Z} \rangle) & \text{if } r = 2, \\ \mathbb{Q}^*/(\mathbb{Q}^{*2} \cdot \langle 1 + r\mathbb{Z} \rangle) & \text{if } r > 2. \end{cases}$$

The group J_{-1} is canonically isomorphic to the multiplicative group $\{\pm 1\}$. Using this isomorphism, the natural group homomorphism $\mathbb{Q}^* \to J_{-1}$ is given by the sign function.

In Section 1.4 for each r in T we show that the group J_r is a vector space

over the finite field $\mathbb{F}_2$ of 2 elements of dimension

$$\dim_{\mathbb{F}_2} J_r = \begin{cases} 1 & \text{if } r = -1, \\ 3 & \text{if } r = 2, \\ 2 & \text{if } r > 2. \end{cases}$$

In addition, we shall define the *norm-residue symbol at r*

$$\langle \cdot, \cdot \rangle_r : J_r \times J_r \to \{\pm 1\},$$

which is a nondegenerate symmetric bilinear map by Remark 1.15. In the case $r > 2$, this symbol does not carry much more information than the Legendre symbol $\left(\frac{\cdot}{r}\right)$.

Let S be a finite subset of T containing -1 and 2. Let J_S be the group $\prod_{r \in S} J_r$. Note that we have $\dim_{\mathbb{F}_2} J_S = 2 \cdot |S|$. By taking the product componentwise we get the nondegenerate symmetric bilinear map

$$\begin{aligned} \langle \cdot, \cdot \rangle_S : J_S \times J_S &\to \{\pm 1\}, \\ (x, y) &\mapsto \prod_{r \in S} \langle x_r, y_r \rangle_r, \end{aligned}$$

where $x = (x_r)_{r \in S}$ and $y = (y_r)_{r \in S}$. We call this bilinear map the *norm-residue symbol at S*.

We rephrase the quadratic reciprocity laws in terms of orthogonality with respect to the norm-residue symbol. See Remark 1.16 for more details.

Theorem 1.9. *Let T be the set of integers consisting of -1 and all the primes. Let p and q be two elements in T and let S be a finite subset of T containing -1, 2, p, and q. Then p and q are orthogonal with respect to the norm-residue symbol at S.*

Proof. This follows from Lemma 1.17. □

Let $\langle S \rangle$ be the subgroup of $\mathbb{Q}^*$ generated by the elements of S. It has dimension $|S|$ over $\mathbb{F}_2$. By Lemma 1.19 the natural group homomorphism $\mathbb{Q}^* \to J_S$ restricts to a group homomorphism $\langle S \rangle \to J_S$ with kernel $\langle S \rangle^2$. Hence, the induced group homomorphism $\langle S \rangle / \langle S \rangle^2 \to J_S$ is injective. We will denote the group generated by the image of S in J_S by $\langle \overline{S} \rangle$.

Using the common notation for the orthogonal complement of a vector space with respect to an inner product, we denote the annihilator in J_S of $\langle \overline{S} \rangle$ with respect to the norm-residue symbol at S by $\langle \overline{S} \rangle^\perp$. Note that Theorem 1.9 implies the inclusion $\langle \overline{S} \rangle \subseteq \langle \overline{S} \rangle^\perp$. Theorem 1.10 states that this inclusion is actually an equality.

Theorem 1.10. *Let the notation be as in* Notation 1.8 *and let S be a finite subset of T containing -1 and 2. Then the group generated by the image of S in J_S is its own annihilator with respect to the norm-residue symbol at S.*

Proof. Note that we have

$$\dim_{\mathbb{F}_2} J_S = 2 \cdot |S| = 2 \dim_{\mathbb{F}_2} \langle S \rangle.$$

Since the norm-residue symbol at S is nondegenerate, it follows that the annihilator $\langle \overline{S} \rangle^\perp$ of $\langle \overline{S} \rangle$ with respect to the norm-residue symbol at S has also dimension $|S|$ over $\mathbb{F}_2$. Theorem 1.9 implies that $\langle \overline{S} \rangle^\perp$ contains $\langle \overline{S} \rangle$. Since both $\langle \overline{S} \rangle$ and its annihilator have dimension $|S|$ over $\mathbb{F}_2$, the equality $\langle \overline{S} \rangle = \langle \overline{S} \rangle^\perp$ follows. □

Remark 1.11. The equality $\langle \overline{S} \rangle = \langle \overline{S} \rangle^\perp$ stated in Theorem 1.10 implies that the group homomorphism

$$\begin{aligned} J_S &\to \mathrm{Hom}(\langle \overline{S} \rangle, \{\pm 1\}), \\ x &\mapsto (r \mapsto \langle x, r \rangle_S), \end{aligned}$$

induces a group isomorphism $J_S / \langle \overline{S} \rangle \xrightarrow{\sim} \mathrm{Hom}(\langle \overline{S} \rangle, \{\pm 1\})$ and the norm-residue symbol at S induces a nondegenerate bilinear map $J_S / \langle \overline{S} \rangle \times \langle \overline{S} \rangle \to \{\pm 1\}$.

Remark 1.12. The group $J_S / \langle \overline{S} \rangle$ can be viewed as a Galois group. Let K_S be the number field $\mathbb{Q}(\sqrt{r} : r \in S)$ and let G_S be the Galois group $\mathrm{Gal}(K_S / \mathbb{Q})$. We have the well-known Kummer pairing

$$\begin{aligned} G_S \times \langle S \rangle / \langle S \rangle^2 &\to \{\pm 1\}, \\ (\sigma, r) &\mapsto \frac{\sigma(\sqrt{r})}{\sqrt{r}}. \end{aligned}$$

It is a nondegenerate bilinear map and therefore we have a group isomorphism $G_S \xrightarrow{\sim} \mathrm{Hom}(\langle S \rangle / \langle S \rangle^2, \{\pm 1\})$. See Theorem 3.47 for a more general statement in abelian Kummer theory. Since the groups $J_S / \langle \overline{S} \rangle$ and G_S are isomorphic to $\mathrm{Hom}(\langle \overline{S} \rangle, \{\pm 1\})$ and $\mathrm{Hom}(\langle S \rangle / \langle S \rangle^2, \{\pm 1\})$, respectively, we obtain a group isomorphism $J_S / \langle \overline{S} \rangle \xrightarrow{\sim} G_S$. This is a group isomorphism we also get from class field theory.

1.4 The norm-residue symbol

The natural definition of the norm-residue symbol uses class field theory. In the present section we give a more concrete and accordingly more artificial definition.

Let r be a prime. Every nonzero rational number x can be written in the form $r^n \frac{a}{b}$, where n, a, and b are integers with $ab \not\equiv 0 \bmod r$. The integer n is unique, is called the *valuation of x at r*, and is denoted by $\mathrm{v}_r(x)$.

For any odd prime r the map

$$\begin{aligned} \mathbb{Q}^* &\to (\mathbb{Z}/2\mathbb{Z}) \oplus ((\mathbb{Z}/r\mathbb{Z})^*/(\mathbb{Z}/r\mathbb{Z})^{*2}), \\ x = r^n \frac{a}{b} &\mapsto (\mathrm{v}_r(x) \bmod 2, ab \bmod r), \end{aligned}$$

where n is the valuation of x at r and a and b are integers that are not divisible by r, is a surjective group homomorphism with kernel $\mathbb{Q}^{*2} \cdot \langle 1 + r\mathbb{Z} \rangle$. This proves that the group J_r is generated by the images of r and any integer that is not a square modulo r.

For $r = 2$ the map

$$\begin{aligned} \mathbb{Q}^* &\to \mathbb{Z}/2\mathbb{Z} \oplus (\mathbb{Z}/8\mathbb{Z})^*, \\ x = 2^n \frac{a}{b} &\mapsto (\mathrm{v}_2(x) \bmod 2, ab \bmod 8), \end{aligned}$$

where n is the valuation of x at 2 and a and b are odd integers, is well-defined. It is a surjective group homomorphism with kernel $\mathbb{Q}^{*2} \cdot \langle 1 + 8\mathbb{Z} \rangle$. So J_2 is isomorphic to the group on the right-hand side, which is generated by the images of 2, -1, and 5. Therefore, we can write J_2 as $\langle \overline{2} \rangle \times \langle \overline{-1} \rangle \times \langle \overline{5} \rangle$.

It follows from the definition that for each $r \in T$ the group J_r has exponent 2 and we have just shown that it is a vector space over the finite field $\mathbb{F}_2$ of 2 elements of dimension

$$\dim_{\mathbb{F}_2} J_r = \begin{cases} 1 & \text{if } r = -1, \\ 3 & \text{if } r = 2, \\ 2 & \text{if } r > 2. \end{cases}$$

Remark 1.13 explains the origin of these groups to the reader who knows about completions of $\mathbb{Q}$.

Remark 1.13. The set T can be thought of as the set of places [Definition 4.10] of $\mathbb{Q}$. For each $r \in T$ the group J_r is $\mathbb{Q}^*$ modulo the subgroup of the elements that are locally squares at the place corresponding to r. The group J_{-1} is isomorphic to $\mathbb{R}^*/\mathbb{R}^{*2}$ and for each positive $r \in T$ the group J_r is isomorphic to $\mathbb{Q}_r^*/\mathbb{Q}_r^{*2}$, where $\mathbb{Q}_r$ is the field of r-adic rationals.

In 1897 Hilbert introduced his symbol, which we present in our setting. For each r in T we define the *norm-residue symbol at r*, which is a bilinear map

$$\langle \cdot, \cdot \rangle_r : J_r \times J_r \to \{\pm 1\}.$$

We proceed in the following way: we define a bilinear map

$$\langle \cdot, \cdot \rangle_r : \mathbb{Q}^* \times \mathbb{Q}^* \to \{\pm 1\}$$

and the norm-residue symbol at r is the map induced by the natural group homomorphism $\mathbb{Q}^* \to J_r$. We distinguish three cases: $r > 2$ and the two special cases $r = -1$ and $r = 2$. The first one has a clear connection to the Legendre symbol, while the other two appear in the quadratic reciprocity law for the Jacobi symbol and take into account the sign and the congruence modulo 4 of the arguments of the symbol.

Case $r > 2$. For each $(x, y) \in \mathbb{Q}^* \times \mathbb{Q}^*$ we set

$$\langle x, y \rangle_r \equiv \left((-1)^{\mathrm{v}_r(x)\,\mathrm{v}_r(y)} \frac{x^{\mathrm{v}_r(y)}}{y^{\mathrm{v}_r(x)}} \right)^{\frac{r-1}{2}} \mod r.$$

This formula may look quite involved, but it defines the same map, linear in each argument and with values in $\{\pm 1\}$, as the following: $\langle r, r \rangle_r = (-1)^{\frac{r-1}{2}}$ and for each integer a that is not a square modulo r one has $\langle a, a \rangle_r = 1$ and $\langle a, r \rangle_r = \langle r, a \rangle_r = -1$. The formula is also similar to the congruence in Euler's criterion. In fact, using the Legendre symbol, for any integer b that is not multiple of r we get

$$\langle b, r \rangle_r = \langle r, b \rangle_r = \left(\frac{b}{r} \right).$$

Moreover, for all integers c and d that are not multiple of r we have $\langle c, d \rangle_r = 1$.

Case $r = -1$. For each $(x, y) \in \mathbb{Q}^* \times \mathbb{Q}^*$ we set

$$\langle x, y \rangle_{-1} = \begin{cases} -1 & \text{if both } x \text{ and } y \text{ are negative,} \\ 1 & \text{if at least one of } x \text{ and } y \text{ is positive.} \end{cases}$$

Case $r = 2$. For each $(x, y) \in \mathbb{Q}^* \times \mathbb{Q}^*$ we set

$$\langle x, y \rangle_2 = (-1)^{\frac{a_1 b_1 - 1}{2} \cdot \frac{a_2 b_2 - 1}{2} + \mathrm{v}_2(x) \cdot \frac{(a_2 b_2)^2 - 1}{8} + \mathrm{v}_2(y) \cdot \frac{(a_1 b_1)^2 - 1}{8}}$$

where $x = 2^{\mathrm{v}_2(x)} \frac{a_1}{b_1}$ and $y = 2^{\mathrm{v}_2(y)} \frac{a_2}{b_2}$ with a_1, b_1, a_2 and b_2 odd integers. Writing J_2 as $\langle \overline{2} \rangle \times \langle \overline{-1} \rangle \times \langle \overline{5} \rangle$, an explicit description of the norm-residue symbol at 2 is given by the following table.

$\langle \cdot, \cdot \rangle_2$	$\overline{2}$	$\overline{-1}$	$\overline{5}$
$\overline{2}$	1	1	-1
$\overline{-1}$	1	-1	1
$\overline{5}$	-1	1	1

The table is equivalent to the following formula: for all integers a_{-1}, a_2, a_5, b_{-1}, b_2, and b_5 one has

$$\langle (-1)^{a_{-1}} \cdot 2^{a_2} \cdot 5^{a_5}, (-1)^{b_{-1}} \cdot 2^{b_2} \cdot 5^{b_5} \rangle_2 = (-1)^{a_{-1}b_{-1}+a_2b_5+a_5b_2}.$$

The definition of the norm-residue symbol is convoluted, in particular for $r = 2$, but Remark 1.14 shows that the symbol also has an interpretation in terms of the existence of a nonzero solution of a certain equation.

Remark 1.14. Let $r \in T$ and let F be the corresponding local field in Remark 1.13. Then one has

$$\langle a, b \rangle_r = \begin{cases} -1 & \text{if } z^2 = ax^2 + by^2 \text{ has no nonzero solution } (x, y, z) \in F^3, \\ 1 & \text{if } z^2 = ax^2 + by^2 \text{ has a nonzero solution } (x, y, z) \in F^3. \end{cases}$$

Remark 1.15. It follows from the definition that for each $r \in T$ the norm-residue symbol at r

$$\langle \cdot, \cdot \rangle_r : J_r \times J_r \to \{\pm 1\}$$

is a nondegenerate symmetric bilinear map.

1.5 Orthogonality

We explain why we say that Theorem 1.9 rephrases the quadratic reciprocity law in terms of orthogonality.

Remark 1.16. Theorem 1.9 states that if p and q are two elements in S, then they are orthogonal with respect to the norm-residue symbol at S. Firstly, suppose that p and q are two distinct odd primes in S. Since for each odd prime r different from p and q we have $\langle p, q \rangle_r = 1$, we get the equality

$$\langle p, q \rangle_S = \langle p, q \rangle_{-1} \langle p, q \rangle_2 \langle p, q \rangle_p \langle p, q \rangle_q,$$

which can be written, using the Legendre symbol, as

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

Hence, the quadratic reciprocity law is equivalent to the equality $\langle p, q \rangle_S = 1$. Similarly, for each odd prime p, the equalities $\langle -1, p \rangle_S = 1$ and $\langle 2, p \rangle_S = 1$ are equivalent to the two supplements to the quadratic reciprocity law.

Lemma 1.17. *Let the notation be as in* Notation 1.8 *and let S be a finite subset of T containing -1 and 2. Then the group generated by the image of S in J_S is contained in its own annihilator with respect to the norm-residue symbol at S.*

Proof. A straightforward computation shows the equality $\langle -1,-1\rangle_S = 1$:

$$\langle -1,-1\rangle_S = \langle -1,-1\rangle_{-1}\langle -1,-1\rangle_2 \prod_{p\in S\setminus\{-1,2\}} \langle -1,-1\rangle_p = (-1)(-1)\cdot 1 = 1.$$

In a similar way, we can prove the equalities

$$\langle -1,2\rangle_S = \langle 2,-1\rangle_S = \langle 2,2\rangle_S = 1$$

and for all odd primes p in S the equality $\langle p,p\rangle_S = 1$. These equalities cover all cases where both entries of the norm-residue symbol at S are in the set $\{-1,2\}$ or equal. Hence, using also the symmetry of the norm-residue symbol at S, we may assume that the second entry is an odd prime in S and the first entry is different from the second one. By Remark 1.16 for distinct elements $r \in S$ and $r' \in S \setminus \{-1,2\}$ we have $\langle r,r'\rangle_S = 1$. □

Let the notation be as in Notation 1.8. For each r in T we define a group homomorphism $J_r \to \mathbb{Z}/2\mathbb{Z}$. For $r = -1$ the map is the zero map. If r is positive, the map is given by $x \mapsto \mathrm{v}_r(x) \bmod 2$. For each $r \in T$ we denote the kernel of this homomorphism by U_r. We have $U_{-1} = J_{-1}$ and for each positive $r \in T$ we get a short exact sequence

$$1 \longrightarrow U_r \longrightarrow J_r \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0. \tag{1.18}$$

Let S be a finite subset of T containing -1 and 2. As before, we denote the group $\prod_{r\in S} J_r$ by J_S. Moreover, we define the group

$$U_S = \prod_{r\in S} U_r = \{(x_r)_r \in J_S : \forall r \in S\setminus\{-1\} : \mathrm{v}_r(x_r) \equiv 0 \bmod 2\}.$$

Now it is straightforward to prove Lemma 1.19.

Lemma 1.19. *The natural group homomorphism $\mathbb{Q}^* \to J_S$ restricts to a group homomorphism $\langle S\rangle \to J_S$ with kernel $\langle S\rangle^2$.*

Proof. It follows from the definition of the components of J_S that $\langle S\rangle^2$ is contained in the kernel of the group homomorphism $\langle S\rangle \to J_S$. On the other hand, any element in the kernel has to be contained in U_S, that is it has even valuation at each prime number in S, and has to be positive. This implies that it is an element of $\langle S\rangle^2$. Hence, the kernel of the group homomorphism $\langle S\rangle \to J_S$ is $\langle S\rangle^2$. □

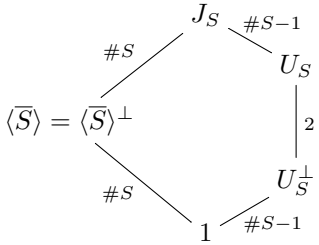
We focus our attention on the norm-residue symbol at S. It follows from its definition that for each $r \in T$ the annihilator $U_r^\perp$ of U_r with respect to the norm-residue symbol at r is contained in U_r. As before, we distinguish three cases.

Case $r > 2$. We have the equality $U_r = U_r^\perp$. It follows that the dimension over $\mathbb{F}_2$ of $U_r/U_r^\perp$ is 0.

Case $r = -1$. The group U_{-1} is equal to J_{-1}. Since the norm-residue symbol is a nondegenerate bilinear map, the annihilator $U_{-1}^\perp$ of U_{-1} is trivial. Hence, the dimension over $\mathbb{F}_2$ of $U_{-1}/U_{-1}^\perp$ is 1.

Case $r = 2$. Writing J_2 as $\langle\overline{2}\rangle \times \langle\overline{-1}\rangle \times \langle\overline{5}\rangle$ the group U_2 is the subgroup $\langle\overline{-1}\rangle \times \langle\overline{5}\rangle$ of J_2. Its annihilator is the subgroup $\langle\overline{5}\rangle$ and therefore the dimension over $\mathbb{F}_2$ of $U_2/U_2^\perp$ is 1.

Summarizing, the dimension over $\mathbb{F}_2$ of $U_r/U_r^\perp$ is 0 if r is greater than 2 and 1 if r is equal to -1 or 2. Hence, the annihilator $U_S^\perp$ of U_S with respect to the norm-residue symbol at S is contained in U_S and the dimension over $\mathbb{F}_2$ of $U_S/U_S^\perp$ is 2. We present the situation in the following diagram, which is reflected upside down by taking the annihilators. Each segment connects two groups, of which the lower one is a subgroup of the higher one, and is labelled by the dimension over $\mathbb{F}_2$ of their quotient group.



The diagram shows two ways to break up J_S. On the right-hand side we find the quotient group $U_S/U_S^\perp$. Note that it is independent of S and has order 4. Up to a natural isomorphism, this group is the 2-*nd unit residue group* of the field of rational numbers [Theorem 5.32]. In Section 1.6 we see how S can be replaced by T.

1.6 Global formulation

Many results will become more interesting as soon as we are able to define the group J_T for the infinite set T, which consists of -1 and all the primes. An obvious choice would be the direct product $\prod_{r\in T} J_r$. Unfortunately, in this case it is not clear how to extend the norm-residue symbol to $J_T \times J_T$. The product componentwise does not work, because there can be infinitely many nontrivial components. It works if we take the direct sum $\bigoplus_{r\in T} J_r$, but then we do not have anymore a natural group homomorphism $\mathbb{Q}^* \to J_T$. It seems that the direct product is too 'big' and the direct sum too 'small' for our purposes. We are going to define a topological group $\overline{J}$ in between that does not present these problems.

We define the group

$$\overline{J} = \{(x_r)_r \in \prod_{r \in T} J_r : \text{ for all but finitely many } r \in T : x_r \in U_r\}.$$

We endow the groups J_r with the discrete topology, consider them as topological groups, and endow $\overline{J}$ with the topology that makes $\overline{J}$ the restricted topological product of the J_r with respect to the U_r. Here we do not give the general definition, which can be found in Definition 4.15, but we remark that a standard notation is

$$\overline{J} = \prod_{r \in T}{}' J_r.$$

Let $\overline{U} = \prod_{r \in T} U_r$ be the topological product of the compact groups U_r. It is a compact topological group and is a subgroup of $\overline{J}$.

Remark 1.20. The reader who knows about ideles may think of $\overline{J}$ as the group of ideles of $\mathbb{Q}$ modulo squares and of $\overline{U}$ as the group of unit ideles of $\mathbb{Q}$ modulo squares.

We have a short exact sequence

$$1 \longrightarrow \overline{U} \longrightarrow \overline{J} \longrightarrow \bigoplus_{r \in T} J_r/U_r \longrightarrow 1.$$

We extend the norm-residue symbol to a bilinear map $\overline{J} \times \overline{J} \to \{\pm 1\}$. By taking the product componentwise, we define the norm-residue symbol

$$\begin{aligned} \langle \cdot, \cdot \rangle : \overline{J} \times \overline{J} &\to \{\pm 1\}, \\ (x, y) &\mapsto \prod_{r \in T} \langle x_r, y_r \rangle_r, \end{aligned}$$

where $x = (x_r)_{r \in T}$ and $y = (y_r)_{r \in T}$. It is well-defined, because for all but finitely many $r \in T$ we have $\langle x_r, y_r \rangle_r = 1$. This follows from the fact that for all but finitely many odd primes $r \in T$ we have $\mathrm{v}_r(x_r) = \mathrm{v}_r(y_r) = 0$.

We have a natural group homomorphism $\mathbb{Q}^* \to \overline{J}$, because, given a nonzero rational number, for all but finitely many $r \in T$ its image in J_r is contained in U_r. Moreover, this natural group homomorphism has kernel $\mathbb{Q}^{*2}$ and induces an injective group homomorphism $\mathbb{Q}^*/\mathbb{Q}^{*2} \hookrightarrow \overline{J}$. We will denote the group generated by the image of $\mathbb{Q}^*$ in $\overline{J}$ by $\overline{\mathbb{Q}^*}$. We see that the role played by S in the previous sections is played by $\mathbb{Q}^*$ here. This observation suggests the statement of the following theorem, which collects the main results we have presented so far.

Theorem 1.21. *The image of $\mathbb{Q}^*$ in $\overline{J}$ is its own annihilator with respect to the norm-residue symbol $\overline{J} \times \overline{J} \to \{\pm 1\}$.*

Proof. The inclusion $\overline{\mathbb{Q}^*} \subseteq \overline{\mathbb{Q}^*}^{\perp}$ follows from Lemma 1.17. Let $y \in \overline{\mathbb{Q}^*}^{\perp}$. Multiplying y by an element in $\mathbb{Q}^*$, we may assume $y_{-1} = 1$ and for each positive $r \in T$ the equality $\mathrm{v}_r(y_r) = 0$. We cannot have $y_2 \neq 1$, because in this case $\langle -1, y\rangle = \langle -1, y_2\rangle_2$ and $\langle 2, y\rangle = \langle 2, y_2\rangle_2$ are not both equal to 1. Suppose there is $s \in T \setminus \{-1, 2\}$ with $y_s \neq 1$. Then we have

$$\langle s, y\rangle = \langle s, 1\rangle_2 \cdot \langle s, y_s\rangle_s = -1,$$

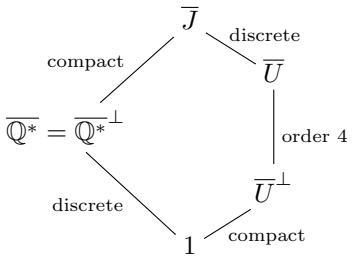
which contradicts $y \in \overline{\mathbb{Q}^*}^{\perp}$. Hence, we get the inclusion $\overline{\mathbb{Q}^*}^{\perp} \subseteq \overline{\mathbb{Q}^*}$. □

Remark 1.22. The image of $\mathbb{Q}^*$ in $\overline{J}$ is a discrete subgroup of $\overline{J}$.

Remark 1.23. Theorem 1.21 and Remark 1.22 can be extended to global fields [Definition 4.3] containing a primitive m-th root of unity. See Theorem 4.52 and Theorem 4.53.

We look at the annihilator $\overline{U}^{\perp}$ of $\overline{U}$ in $\overline{J}$ with respect to the norm-residue symbol. The inclusion $\overline{U}^{\perp} \subseteq \overline{U}$ follows from the definition of the norm-residue symbol. We remark that the inclusion is strict and therefore we get the non-trivial quotient group $\overline{U}/\overline{U}^{\perp}$. This is the group substituting for $U_S/U_S^{\perp}$ in Section 1.5 when we replace the set S by T. Since $U_S/U_S^{\perp}$ is independent of S, it is not surprising that $\overline{U}/\overline{U}^{\perp}$ is a finite group of order 4 and, up to a natural isomorphism, is the 2-*nd unit residue group* of the field of rational numbers [Theorem 5.32]. The behaviour of the group $\overline{U}$ with respect to the norm-residue symbol can be considered as a possible starting point of our research. For instance, what happens if we replace $\mathbb{Q}$ by a number field or a function field?

The situation for the field of rational numbers is summarized in the following diagram. Each segment connects two groups, of which the lower one is a subgroup of the higher one, and its label refers to their quotient group.



We say that the subgroup $\overline{\mathbb{Q}^*}$ of $\overline{J}$ lies halfway in $\overline{J}$, because it is its own annihilator with respect to the norm-residue symbol. Do we have a similar subgroup on the right-hand side? The answer is affirmative and it gives rise to the virtual group [Definition 5.15].

1.7 Overview

We will now replace $\mathbb{Q}$ by a *global field* K, i.e. either an algebraic number field or the function field of a curve over a finite field. The fields $\mathbb{R}$ and $\mathbb{Q}_r$ will be replaced by the completions K_v of K at the places v of K; these completions are *local fields*. We also fix a positive integer m such that K contains a primitive m-th root of unity; for $K = \mathbb{Q}$ we took $m = 2$. We denote by μ_m the group of m-th roots of unity in K.

The role of the groups J_r will be played by the groups K_v^*/K_v^{*m}, which are finite abelian groups, "most" of which have order m^2. For each v there is a norm-residue symbol, which is a nondegenerate antisymmetric pairing $K_v^*/K_v^{*m} \times K_v^*/K_v^{*m} \to \mu_m$. As before, we write $\overline{J}$ for the restricted direct product of the groups K_v^*/K_v^{*m}, with v ranging over all places of K; it is a topological group, which one may identify with J/J^m, where J is the so-called group of ideles of K. The product of all norm-residue symbols defines a nondegenerate antisymmetric pairing $\overline{J} \times \overline{J} \to \mu_m$. Just as for the field of rational numbers, the image $\overline{K^*}$ of K^* in $\overline{J}$ equals its own annihilator with respect to this pairing.

Let it now first be assumed that K is a function field. In this case *each* group K_v^*/K_v^{*m} has order m^2, and it has a subgroup $\overline{U}_v$ that plays the role of the groups U_r in the rational case; $\overline{U}_v$ has order m and is its own annihilator with the respect to the norm-residue symbol. The product $\overline{U}$ of all $\overline{U}_v$ is a subgroup of $\overline{J}$ and equals its own annihilator with respect to the pairing defined on $\overline{J}$. The latter equality leads to a construction of the so-called the Tate pairing, which is important both in arithmetic geometry and in cryptography.

Not everything we just wrote carries over to the case of number fields, where the situation is more complicated. Investigating it is one of the main purposes of the present thesis.

Let K be a number field. The first difficulty is the existence of *infinite places*, which are places v for which K_v is isomorphic to $\mathbb{R}$ or $\mathbb{C}$. For $K = \mathbb{Q}$ there is just one infinite place, corresponding to $r = -1$. For general K the set of infinite places is finite and nonempty. When v is infinite, then it is not obvious how to define $\overline{U}_v$, and we choose $\overline{U}_v = K_v^*/K_v^{*m}$; this group is trivial unless $m = 2$ and $K_v \cong \mathbb{R}$, in which case it has order 2. As for $K = \mathbb{Q}$, we now define $\overline{U}$ to be the product of all $\overline{U}_v$ as v ranges over all places of K. The second difficulty is that, while almost all of the groups K_v^*/K_v^{*m} have order m^2, there are exceptions when $m > 1$. These exceptions are exactly those v for which $\overline{U}_v$ is not its own annihilator with respect to the norm-residue symbol. However, our definition ensures that the annihilator $\overline{U}^\perp$ of $\overline{U}$ with respect to the pairing defined on $\overline{J}$ satisfies $\overline{U}^\perp \subseteq \overline{U}$.

Thus, the quotient group $\overline{U}/\overline{U}^\perp$, which is trivial in the function field case, measures the complication of the number field situation. One of our results

is that it is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^{2s}$, where s is the number of infinite places of K. Also, $\overline{U}/\overline{U}^{\perp}$ carries again a nondegenerate antisymmetric μ_m-valued pairing. This group, together with its pairing, is called the *unit residue group*.

By its definition, the unit residue group is a direct sum of local contributions. It also has a subgroup of a global nature, called the *virtual group*, which is the image of $\overline{K^*} \cap \overline{U}$ in the unit residue group. The virtual group equals its own annihilator with respect to the pairing, and has order m^s, but it is not generally isomorphic to $(\mathbb{Z}/m\mathbb{Z})^s$.

In the present thesis we give a precise description of the unit residue groups and their virtual subgroups for some classes of number fields, including all quadratic fields. In addition we point out connections to two classical theorems on ideal class groups, namely the theorem of Armitage and Fröhlich on 2-ranks and Scholz's theorem on 3-ranks.

In Chapter 10 we study certain subgroups of the multiplicative group of a local field that play an important role in an algorithm for computing norm-residue symbols. Chapter 11 is independent of the rest of the thesis. We describe its contents in Section 1.17.

1.8 Skew abelian groups

In Chapter 2, which is purely auxiliary, we collect some results about finite abelian groups equipped with an antisymmetric pairing, rephrasing them in terms of the *skew element*.

The norm-residue symbol defined in Section 1.4 is a nondegenerate symmetric bilinear map. Since it is defined on groups of exponent 2, it is also antisymmetric. For general exponents the norm-residue symbol is antisymmetric.

Definition 1.24 (Skew abelian group)**.** A *skew abelian group* is a triple (A, C, β), where A is a finite abelian group, C is an abelian group, and $\beta : A \times A \to C$ is an antisymmetric perfect pairing [Definition 2.3].

Remark 2.24 shows that not much generality is lost in Definition 1.24 by assuming $C = \mathbb{Q}/\mathbb{Z}$.

Every skew abelian group has a special element called its *skew element*, which has order dividing 2. In the skew abelian groups we study, the skew element is usually the residue class of -1.

Definition 1.25 (Skew element)**.** Let (A, C, β) be a skew abelian group. The *skew element* of (A, C, β) is the element $g \in A$ such that $\beta(g, a) = \beta(a, a)$ for all $a \in A$.

An alternating pairing is a well-known example of an antisymmetric pairing. We call a skew abelian group *symplectic* if its pairing is alternating. Theo-

rem 2.15 states this occurs if and only if the skew element is the identity element of A.

Definition 1.26 (Isomorphism of skew abelian groups)**.** Let (A, C, β) and (B, C, γ) be skew abelian groups. An *isomorphism of skew abelian groups* is a group isomorphism $\varphi : A \to B$ such that for all $x, y \in A$ one has $\beta(x, y) = \gamma(\varphi(x), \varphi(y))$.

The classification of symplectic abelian groups up to isomorphism [Theorem 2.25] is well-known: every symplectic abelian group is isomorphic to the direct sum of a finite abelian group and its dual group. The classification of skew abelian groups up to isomorphism [Theorem 2.28] distinguishes two cases, according to the parity of the 2-rank; this 2-rank is even if and only if the skew element is orthogonal to itself [Remark 2.31]. The odd case is reminiscent of the classification of symplectic abelian groups, which is itself a special case of the more complicated even case; the skew element still plays a decisive role here.

1.9 The local norm-residue symbol

In Chapter 3 we review local class field theory and the norm-residue symbol.

For a positive integer m and a local field F that contains a primitive m-th root of unity, the norm-residue symbol is a pairing $F^* \times F^* \to \mu_m$ that is characterized by a few easily stated properties [Theorem 3.80]; while the uniqueness of the norm-residue symbol allows a perfectly elementary proof, its existence proof uses local class field theory.

In Section 3.7 we show that for an Archimedean local field the norm-residue symbol is the trivial map, unless the field is the field of real numbers and m is equal to 2. In this case, the second power norm-residue symbol is the pairing

$$(\cdot, \cdot) : \mathbb{R}^* \times \mathbb{R}^* \to \langle -1 \rangle$$

defined for all $a, b \in \mathbb{R}^*$ by

$$(a, b) = \begin{cases} -1 & \text{if both } a \text{ and } b \text{ are negative,} \\ 1 & \text{if at least one of } a \text{ and } b \text{ is positive.} \end{cases}$$

It gives rise to the skew abelian group $(U_{\mathbb{R}}/U_{\mathbb{R}}^{\perp}, \langle -1 \rangle, (\cdot, \cdot))$, where $U_{\mathbb{R}} = \mathbb{R}^*$, $U_{\mathbb{R}}^{\perp} = \mathbb{R}_{>0}$, and the pairing is the map induced by the norm-residue symbol. This skew abelian group has order 2 and its skew element is $-1 \cdot U_{\mathbb{R}}^{\perp}$.

Also in the case of a non-Archimedean local field does the norm-residue symbol give rise to a skew abelian group. When F is a non-Archimedean local field containing a primitive m-th root of unity, the map

$$(\cdot, \cdot)_{F,m} : F^*/F^{*m} \times F^*/F^{*m} \to \mu_m$$

induced by the m-th power norm-residue symbol is an antisymmetric perfect pairing. Since the group F^*/F^{*m} is finite, the triple $(F^*/F^{*m}, \mu_m, (\cdot,\cdot)_{F,m})$ is a skew abelian group. Theorem 3.82 shows that its skew element is $-1 \cdot F^{*m}$ and describes how this triple fits into the classification of skew abelian groups. When the characteristic of the residue field of F does not divide m, we have a group isomorphism $F^*/F^{*m} \cong (\mathbb{Z}/m\mathbb{Z})^2$.

Narrowing our focus on the group U_F of units of the ring of integers of F produces a result of the same nature [Corollary 3.92]. In particular, if $U_F^{\perp}$ is the annihilator in U_F of U_F with respect to the norm-residue symbol, then the triple $(U_F/U_F^{\perp}, \mu_m, (\cdot,\cdot)_{F,m})$ is a skew abelian group with skew element $-1 \cdot U_F^{\perp}$, and $U_F/U_F^{\perp}$ is trivial if and only if m is not a multiple of the characteristic of the residue field of F.

When F ranges over completions of a global field K, the skew abelian groups $U_F/U_F^{\perp}$ are the local components of the m-th unit residue group of K.

1.10 The global norm-residue symbol

The local norm-residue symbols induce a pairing on the group of ideles of any global field. This pairing is studied in Chapter 4.

Let m be a positive integer, let K be a global field containing a primitive m-th root of unity, and denote by J the group of ideles of K [Definition 4.19]. Taking the product of the local norm-residue symbols over all completions of K, we obtain a nondegenerate antisymmetric pairing $\overline{J} \times \overline{J} \to \mu_m$, where $\overline{J} = J/J^m$ and μ_m is the group of m-th roots of unity in K. We refer to this pairing as the *global norm-residue symbol*.

Two important subgroups of J are the multiplicative group K^* of K and the group of unit ideles U of K. The former is a discrete subgroup of J and its image $\overline{K^*}$ in $\overline{J}$ equals its own annihilator in $\overline{J}$ with respect the global norm-residue symbol. The latter is a compact subgroup of J and its image $\overline{U}$ in $\overline{J}$ contains its own annihilator $\overline{U}^{\perp}$ in $\overline{J}$ with respect to the same pairing. The global norm-residue symbol induces a perfect pairing of finite abelian groups

$$(\overline{K^*} \cap \overline{U}) \times \overline{J}/(\overline{K^*} \cdot \overline{U}^{\perp}) \to \mu_m.$$

When K is a function field, Remark 4.70 shows that this pairing is an extension to larger groups of the inverse of the Tate pairing [Definition 4.68], which has found several applications in cryptography. As a corollary we obtain a new proof of the fact that the Tate pairing is a perfect pairing.

The existence of the Tate pairing relies on the equality $\overline{U} = \overline{U}^{\perp}$. The unit residue group naturally arises when one tries to extend the Tate pairing to number fields and can be also viewed as an obstruction to the existence of a similar pairing. Indeed, in the case of number fields and for m greater than 1,

the group $\overline{U}$ strictly contains its own annihilator $\overline{U}^{\perp}$. In Chapter 5 the *m-th unit residue group* of K is defined to be the quotient group $\overline{U}/\overline{U}^{\perp}$ together with the antisymmetric perfect pairing induced by the global norm-residue symbol.

When K is a number field, the global norm-residue symbol does not give a clean duality between $\mathrm{Cl}[m]$ and $\mathrm{Cl}\,/\,\mathrm{Cl}^m$, where Cl is the ideal class group of K, but it induces pairings that do not deviate much from a naturally defined perfect pairing $\mathrm{Cl}[m] \times \mathrm{Cl}\,/\,\mathrm{Cl}^m \to \mu_m$ [Theorem 4.84 and Theorem 4.86]. We show that an upper bound for these deviations is provided by the m-th virtual group of K [Definition 5.15], which is a subgroup of the m-th unit residue group of K.

In the function field case, the groups $\overline{K^*} \cap \overline{U}$ and $\overline{J}/(\overline{K^*} \cdot \overline{U})$ are very familiar to algebraic geometers. Indeed, they have an interpretation in terms of étale cohomology. For more details about this subject we refer to the books by Milne [46], [47]. If C is the projective nonsingular absolutely irreducible curve over a finite field of which K is the function field, then we have natural group isomorphisms

$$\overline{K^*} \cap \overline{U} \xrightarrow{\sim} H^1(C, \mu_m) \quad \text{and} \quad \overline{J}/(\overline{K^*} \cdot \overline{U}) \xrightarrow{\sim} H^2(C, \mu_m).$$

A duality theorem from algebraic geometry implies that there is also a bilinear cup product

$$H^1(C, \mu_m) \times H^2(C, \mu_m) \to H^3(C, \mu_m \otimes \mu_m),$$

which is a perfect pairing of finite abelian groups. Since the abelian group $H^3(C, \mu_m \otimes \mu_m)$ is canonically isomorphic to μ_m, one may expect that, modulo the isomorphisms just mentioned and with suitable sign conventions, the pairing induced by the global norm-residue symbol coincides with the cup product.

1.11 The unit residue group

Chapter 5 is devoted to introducing the unit residue group and the virtual group, and presenting general results on them.

In Section 1.5 we introduced the 2-nd unit residue group of the field of rational numbers, which is described in detail in Section 5.3. It has only two nontrivial local components, at 2 and at infinity, and as an abelian group it is a Klein four-group. Equipped with the pairing given by the second power norm-residue symbol of $\mathbb{Q}$ it is a skew abelian group. This pairing is essentially a combination of the two pairings in the quadratic reciprocity law for the Jacobi symbol.

Given a positive integer m and a global field K containing a primitive m-th root of unity, we define in Chapter 5 the m-th unit residue group of K. It is a finite abelian group equipped with a pairing induced by the m-th power norm-residue symbol. This pairing makes it into a skew abelian group. When K is a function field, the m-th unit residue group of K is the trivial group. In general, as an abelian group, the m-th unit residue group of a global field K is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^{2s}$, where s is the number of infinite places of K [Theorem 5.10].

The m-th unit residue group of K is isomorphic to an orthogonal sum of skew abelian groups that are defined locally at the places of K dividing m and at the real Archimedean places of K. It has a subgroup that is defined globally: the m-th virtual group of K. It is a maximal self-annihilating subgroup of the m-th unit residue group, of order m^s [Theorem 5.17] and its order equals its index in the m-th unit residue group. We remark that the m-th virtual group is not necessarily isomorphic, as an abelian group, to $(\mathbb{Z}/m\mathbb{Z})^s$. In fact, in Chapter 6 we give an example of a number field whose 4-th virtual group is not a free module over $\mathbb{Z}/4\mathbb{Z}$ [Theorem 6.31].

The m-th virtual group of K is also the image of a natural surjective group homomorphism [Remark 5.28] from the group of *m-virtual units* of K, which are the elements in K that have normalized valuation divisible by m at every non-Archimedean place of K. This group homomorphism enables us to compute the m-th virtual group by explicitly specifying a set of m-virtual units of K of which the image generates the m-th virtual group, as well as the relations among those generators. The field extensions of K that are obtained by adjoining m-th roots of m-virtual units of K can ramify only at the places of K dividing m and at the real Archimedean places of K.

1.12 Quadratic number fields

In Chapter 6 we explicitly describe all unit residue groups and virtual groups of quadratic number fields, including their Galois module structure.

Let K be a quadratic number field, $\mathcal{O}_K$ be its ring of integers, Δ be its discriminant, and G be the Galois group $\mathrm{Gal}(K/\mathbb{Q})$. By the 2-adic component of the 2-nd unit residue group of K we mean the product of its local components at the places of K dividing 2, and by its component at infinity we mean the product of its components at the real places. The 2-nd unit residue group is the orthogonal sum of its 2-adic component and its component at infinity.

The component at infinity of the 2-nd unit residue group of K is trivial if K is imaginary, and is a free $(\mathbb{Z}/2\mathbb{Z})[G]$-module of rank 1 if K is real. In the latter case the skew element is the unique nontrivial Galois invariant element, which is the image of -1.

We next discuss the 2-adic component. The group

$$(\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2}$$

is a Klein four-group and there is a unique perfect pairing

$$\beta : (\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2} \times (\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2} \to \{\pm 1\}$$

that makes $((\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2}, \{\pm 1\}, \beta)$ into a skew abelian group with skew element the residue class of -1. This skew abelian group is naturally isomorphic to the 2-adic component of the 2-nd unit residue group of K. Its structures as a Galois module and as a skew abelian group are intimately linked: they are both determined by the skew element. In fact, the Galois action is trivial if and only if the skew element is the identity element, and if and only if the skew abelian group is symplectic [Definition 2.6]. Also, this occurs if and only if Δ is congruent to 4 modulo 8 [Corollary 6.13]. For $\Delta \not\equiv 4 \bmod 8$ the 2-adic component of the 2-nd unit residue group of K is a free $(\mathbb{Z}/2\mathbb{Z})[G]$-module of rank 1. In order to write down an explicit $(\mathbb{Z}/2\mathbb{Z})[G]$-module isomorphism, we will distinguish the cases $\Delta \equiv 1 \bmod 4$ and $\Delta \equiv 0 \bmod 8$ [Theorem 6.12].

To describe the 2-nd virtual group V, we first assume that K is imaginary quadratic. Then V has order 2, and is therefore trivially acted upon by G. Since for $\Delta \not\equiv 4 \bmod 8$ the 2-nd unit residue group of K is a free $(\mathbb{Z}/2\mathbb{Z})[G]$-module of rank 1, it has only one nontrivial Galois invariant element; this is the residue class of -1, which is therefore a generator of V. For $\Delta \equiv 4 \bmod 8$ the residue class of -1 is trivial; in this case it turns out that V is generated by the image of 2 under the surjective group homomorphism $\{\text{2-virtual units of } K\} \twoheadrightarrow V$ in Remark 5.28. These results are proved in Section 6.5.

Now let K be real quadratic. Then the 2-nd virtual group V of K is a Klein four-group. For $\Delta \equiv 4 \bmod 8$, we shall prove that it is generated by the images of -1 and 2 under the map $\{\text{2-virtual units of } K\} \twoheadrightarrow V$ and is therefore trivially acted upon by G. Next suppose $\Delta \not\equiv 4 \bmod 8$. If Δ has a prime divisor p that is congruent to 3 modulo 4, then V is, for any such p, generated by the images of -1 and p, and again trivially acted upon by G. If no such p exists, then there is an integer a for which $\Delta - 4a^2$ is a square, and V is, for any such a, generated by the images of -1 and $2a - \sqrt{\Delta}$. Also, in the latter case V is a free $(\mathbb{Z}/2\mathbb{Z})[G]$-module of rank 1. These results are proved in Section 6.6.

1.13 Two-ranks of ideal class groups

Chapter 7 places the 2-nd virtual group of a number field K in the classical context of inequalities involving 2-ranks of ideal class groups.

What is the difference between the 2-ranks of the ideal class groups of K in the strict sense [Definition 7.1] and in the usual sense? We show how this

difference is measured by the projection of the 2-nd virtual group of K on the product of local components of the 2-nd unit residue group of K at the places dividing 2 [Theorem 7.2].

Using a lower bound on the 2-rank of the projection just mentioned [Corollary 5.22] we get the inequality in Oriat's theorem [Theorem 7.6]. This theorem is a strengthening of the theorem of Armitage–Fröhlich [Theorem 7.8], which gives a lower bound on the 2-rank of the ideal class group of a number field.

1.14 Biquadratic number fields

Using unit residue groups we rephrase and prove Scholz's theorem in Chapter 8. Moreover, we present and employ a probabilistic model on 3-ranks of ideal class groups of quadratic number fields.

Let $d \in \mathbb{Z}_{>1}$ be squarefree and let K be the number field $\mathbb{Q}(\sqrt{d},\sqrt{-3})$. The number field $K/\mathbb{Q}$ is normal with Galois group G a Klein four-group. The 3-rd unit residue of K is a free $(\mathbb{Z}/3\mathbb{Z})[G]$-module of rank 1 [Theorem 8.1]. There are two different Galois module structures of the 3-rd virtual group of K and they correspond to the two cases in Scholz's theorem on the 3-rank of the ideal class group of the quadratic subfields of K [Theorem 8.2]. As a byproduct we get a proof of Scholz's theorem in this setting.

In Section 8.5 we present Dutarte's probabilistic model on 3-ranks of ideal class groups of quadratic number fields, which he used to study the compatibility of the Cohen–Lenstra heuristics with Scholz's theorem. We show that the basic assumptions in his model and a further, much more natural assumption are sufficient to compute the probability that a real quadratic number field has prescribed 3-rank [Theorem 8.6]. The value of this probability is exactly the one predicted by the Cohen–Lenstra heuristics. We get a similar result for imaginary quadratic number fields [Theorem 8.31].

1.15 Cyclic number fields

In Chapter 9 we describe the 2-nd unit residue group and the 2-nd virtual group of a number field that is Galois over $\mathbb{Q}$ and unramified at 2. In the case of a cyclic number field $K/\mathbb{Q}$ of degree either 3 or 5 these descriptions give rise to an unexpected bijection involving the set of real Archimedean places of K.

Let K be a number field that is Galois over $\mathbb{Q}$ with Galois group G and unramified at 2. The 2-nd unit residue group of K is a free $(\mathbb{Z}/2\mathbb{Z})[G]$-module of rank either 1 or 2 according as the extension $K/\mathbb{Q}$ is complex or real [Remark 9.22]. The latter case includes all abelian extensions of $\mathbb{Q}$ of odd degree [Lemma 9.24]. When G is abelian and its exponent divides at least one of the integers in the set $\{2^n + 1 \mid n \in \mathbb{Z}_{>0}\}$, the 2-nd virtual group of K is the graph

of a $(\mathbb{Z}/2\mathbb{Z})[G]$-module isomorphism between two free $(\mathbb{Z}/2\mathbb{Z})[G]$-modules of rank 1 that is also an isomorphism of skew abelian groups [Theorem 9.25]. In the case of a cyclic number field extension of $\mathbb{Q}$ of degree either 3 or 5 we give a more precise description of this isomorphism [Theorem 9.27, Theorem 9.30, and Theorem 9.33]. These results are connected with the fact that both the finite field extension of degree 3 over $\mathbb{Z}/2\mathbb{Z}$ and the finite field extension of degree 5 have a unique self-dual normal basis over $\mathbb{Z}/2\mathbb{Z}$.

In a real quadratic number field K of discriminant congruent to 1 modulo 8, the rational prime 2 splits completely in the ring of integers of K. There are two prime ideals of the ring of integers of K dividing 2 and K has two real places. Using the two square roots of the discriminant of K, which are conjugate under the action of the Galois group $\mathrm{Gal}(K/\mathbb{Q})$, there is a way of defining a natural bijection between the set of primes above 2 and the set of real places of K [Theorem 9.1]. Both this bijection and a similar bijection in the case of a quadratic number field for which the rational prime 2 is inert in the ring of integers of the number field are suggested by the descriptions of 2-nd unit residue groups and 2-nd virtual groups of quadratic number fields. We extend this result to cyclic number field extensions of $\mathbb{Q}$ of degree either 3 or 5 [Theorem 9.3, Theorem 9.4, and Theorem 9.5].

1.16 A large norm group

In Chapter 10 we study a certain group that occurs in algorithms for computing the norm-residue symbol by Daberkow [13] and Bouw [7].

Let p be a prime number and let F be a finite extension of the field $\mathbb{Q}_p$ of p-adic rationals. Let $\mathfrak{P}$ be the maximal ideal of the ring of integers of F, and write $U^{(1)}$ for the multiplicative group $1+\mathfrak{P}$, which is a $\mathbb{Z}_p$-module. The cardinality of the residue field of F is denoted by q.

Let π be a prime element of F, and write H_π for the sub-$\mathbb{Z}_p$-module of $U^{(1)}$ generated by the set of all elements of the form $1-\zeta\pi^i$, where ζ ranges over all $q-1$-st roots of unity in F and i over all positive integers not divisible by p.

We are interested in the $\mathbb{Z}_p$-module $U^{(1)}/H_\pi$. It is not difficult to exhibit an element $\delta \in U^{(1)}$ with the property $U^{(1)} = \delta^{\mathbb{Z}_p} \cdot H_\pi$ [Lemma 10.11], so $U^{(1)}/H_\pi$ is cyclic as a $\mathbb{Z}_p$-module. For each $u \in U^{(1)}$ there exists $k \in \mathbb{Z}_p$ with $u \in \delta^k \cdot H_\pi$; also, such a value for k is typically easy to compute when u is given, but it is only uniquely determined modulo the annihilator of the module $U^{(1)}/H_\pi$.

The relevance of H_π in the context of norm-residue symbols is as follows. Suppose that n is such that F contains a primitive p^n-th root of unity. Then one checks that the p^n-th power norm-residue symbol (π,δ) is a primitive p^n-th root of unity [Lemma 10.10], and that one has $(\pi,h)=1$ for all $h \in H_\pi$

[Lemma 10.4]. Hence if $u \in \delta^k \cdot H_\pi$ is as above, then we have $(\pi, u) = (\pi, \delta)^k$, so that for given u the number k is at least uniquely determined modulo p^n. It follows that the annihilator of the $\mathbb{Z}_p$-module $U^{(1)}/H_\pi$ is divisible by p^n.

It is natural to ask whether the number k gives us any additional information about u, in other words whether it has any significance independently of the norm-residue symbol. Theorem 10.1 shows that the answer is negative: if we take n maximal, then $U^{(1)}/H_\pi$ is cyclic of order p^n, its annihilator is generated by p^n, and k is really only well-defined modulo p^n. This state of affairs can also be expressed by the existence of a short exact sequence

$$1 \to H_\pi \to U^{(1)} \to \mu_{p^n} \to 1,$$

where the second map is the inclusion map and the third sends u to (π, u) [Theorem 10.2].

The proofs in Chapter 10 make use of local class field theory.

1.17 Quadratic characters

In Chapter 11 we study group isomorphisms between the groups of quadratic characters of two number fields that preserve L-series.

To every number field one can associate many mathematical objects, such as the ring of integers, the unit group, the ideal class group, the adele ring, the absolute Galois group, and the Dedekind zeta function. A very natural question is determining to which extent these objects characterize the number field up to isomorphism. For instance, in 1926 Gaßmann showed that the Dedekind zeta function of a number field does in general not determine the number field up to isomorphism [19], whereas in 1976 Uchida proved that the absolute Galois group does [71].

More recently, Cornelissen and Marcolli proved that two number fields are isomorphic if there is a group isomorphism between the groups of abelian characters of their absolute Galois groups that preserves L-series [12]. Generalizing a result by de Smit, Pintonello proved that it is enough to consider only two elements in the group of quadratic characters [Theorem 11.3].

We prove that the natural map from the set of field isomorphisms between two number fields to the set of group isomorphisms between their groups of quadratic characters that preserve L-series is bijective [Theorem 11.1]. As a corollary we get the known result that the existence of a group isomorphism that preserves L-series between the groups of quadratic characters of two number fields implies that the two number fields are isomorphic [Corollary 11.2].

CHAPTER 2

Skew abelian groups

We classify up to isomorphism triples (A, C, β), where A is a finite abelian group, C is an abelian group, and $\beta : A \times A \to C$ is an antisymmetric perfect pairing. We call these triples *skew abelian groups* and their classification is Theorem 2.28. The main reference, which we summarize and link to our theorems in Section 2.6, is [73] by Wall. Similar results are given in [57] by Poonen and Stoll for the nondivisible part of the Shafarevich–Tate group of an abelian variety over a global field.

2.1 Preliminaries

We state definitions and theorems that are useful for understanding the classification in Section 2.2. Abelian groups are considered with additive notation. As a reference for some definitions and basic results see [32] by Lang.

Definition 2.1 (Pairing or bilinear map)**.** Let A, B, and C be abelian groups. A *pairing* or *bilinear map* from $A \times B$ to C is a map

$$\beta : A \times B \to C,$$

such that for each $a \in A$ the function $B \to C$, $x \mapsto \beta(a, x)$, is a group homomorphism and, similarly, for each $b \in B$ the function $A \to C$, $x \mapsto \beta(x, b)$, is a group homomorphism.

Theorem 2.2. *Let A, B, and C be abelian groups and let $\beta : A \times B \to C$ be a map. Then the following are equivalent.*

(i) *The map $\beta : A \times B \to C$ is a pairing.*
(ii) *There is a group homomorphism $A \to \mathrm{Hom}(B, C)$ given by $a \mapsto \beta(a, \cdot)$.*
(iii) *There is a group homomorphism $B \to \mathrm{Hom}(A, C)$ given by $b \mapsto \beta(\cdot, b)$.*

Proof. See Proposition 5.1 of Chapter XI in [22] by Grillet. □

Definition 2.3 (Perfect pairing)**.** Let A, B, and C be abelian groups. A pairing $\beta : A \times B \to C$ is a *perfect pairing* if the group homomorphisms $A \to \mathrm{Hom}(B, C)$, $a \mapsto \beta(a, \cdot)$, and $B \to \mathrm{Hom}(A, C)$, $b \mapsto \beta(\cdot, b)$, are group isomorphisms.

Definition 2.4 (Alternating pairing, antisymmetric pairing)**.** Let A and C be abelian groups. A pairing $\beta : A \times A \to C$ is

(a) *alternating* if $\beta(a, a) = 0$ for all $a \in A$,
(b) *antisymmetric* if $\beta(a, b) = -\beta(b, a)$ for all $a, b \in A$.

Theorem 2.5. *If a pairing is alternating, then it is antisymmetric.*

Proof. Let $\beta : A \times A \to C$ be an alternating pairing. For all $a, b \in A$ we have

$$0 = \beta(a + b, a + b) = \beta(a, a) + \beta(a, b) + \beta(b, a) + \beta(b, b) = \beta(a, b) + \beta(b, a).$$

Hence, the pairing is also antisymmetric. □

Definition 2.6 (Symplectic abelian group)**.** A *symplectic abelian group* is a triple (A, C, β), where A is a finite abelian group, C is an abelian group, and $\beta : A \times A \to C$ is an alternating perfect pairing.

Definition 2.7 (Skew abelian group)**.** A *skew abelian group* is a triple (A, C, β), where A is a finite abelian group, C is an abelian group, and $\beta : A \times A \to C$ is an antisymmetric perfect pairing.

Remark 2.8. By Theorem 2.5 every symplectic abelian group is a skew abelian group.

Definition 2.9 (Similarity of skew abelian groups)**.** Let the triples (A, C, β) and (B, D, γ) be skew abelian groups. Let C' and D' be the groups generated by the images of β in C and of γ in D, respectively. A *similarity of skew abelian groups* is a pair (φ, ψ) of group isomorphisms $\varphi : A \to B$ and $\psi : C' \to D'$ such that for all $x, y \in A$ one has $\psi(\beta(x, y)) = \gamma(\varphi(x), \varphi(y))$.

The diagram

$$\begin{array}{ccc} A \times A & \xrightarrow{\beta} & C' \\ {\scriptstyle\varphi}\downarrow \quad {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\psi} \\ B \times B & \xrightarrow{\gamma} & D' \end{array}$$

visualizes Definition 2.9.

Definition 2.10 (Isomorphism of skew abelian groups)**.** Let (A, C, β) and (B, C, γ) be skew abelian groups. An *isomorphism of skew abelian groups* is a group isomorphism $\varphi : A \to B$ such that for all $x, y \in A$ one has $\beta(x, y) = \gamma(\varphi(x), \varphi(y))$.

Using Remark 2.8 we give similar definitions for symplectic abelian groups. We say that two symplectic abelian groups are *similar* (*isomorphic*) if they are similar (isomorphic) as skew abelian groups.

Theorem 2.11. *Let (A, C, β) be a skew abelian group. Then there exists a unique $g \in A$ such that $\beta(g, a) = \beta(a, a)$ for all $a \in A$.*

Proof. See Theorem 2.42. □

Definition 2.12 (Skew element)**.** Let (A, C, β) be a skew abelian group. The *skew element* of (A, C, β) is the element $g \in A$ such that $\beta(g, a) = \beta(a, a)$ for all $a \in A$.

Theorem 2.13. *Let (A, C, β) be a skew abelian group. Then the skew element of (A, C, β) has order dividing 2.*

Proof. Let $g \in A$ be the skew element of (A, C, β). For all $a \in A$ we have

$$\beta(2g, a) = \beta(g, a) + \beta(g, a) = \beta(a, a) + \beta(a, a) = 0,$$

because $\beta(g, a) = \beta(a, a)$. Since the group homomorphism $\beta(2g, \cdot) : A \to C$ is trivial and by definition of perfect pairing the map $A \to \mathrm{Hom}(B, C)$, $a \mapsto \beta(a, \cdot)$, is a group isomorphism, we get $2g = 0$. □

Corollary 2.14. *Let $(A, \mathbb{Q}/\mathbb{Z}, \beta)$ be a skew abelian group and let g be its skew element. Then one has either $\beta(g, g) = 1/2 + \mathbb{Z}$ or $\beta(g, g) = 0$.*

Proof. The result follows from Theorem 2.13. □

Theorem 2.15. *Let (A, C, β) be a skew abelian group. Then the following are equivalent.*

(i) *The pairing $\beta : A \times A \to C$ is alternating, that is, the triple (A, C, β) is a symplectic abelian group.*

(ii) *The skew element of (A, C, β) is the zero element of A.*

Proof. Let g be the skew element of (A, C, β). Since $\beta : A \times A \to C$ is a perfect pairing, we have $g = 0$ if and only if the group homomorphism $\beta(g, \cdot) : A \to C$, $a \mapsto \beta(g, a)$, is trivial. This is equivalent to the pairing $\beta : A \times A \to C$ being alternating, because for all $a \in A$ we have $\beta(a, a) = \beta(g, a)$. □

Definition 2.16 (Dual group)**.** Let A be a finite abelian group. The *dual group* $\widehat{A}$ of A is the group $\mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z})$ of homomorphisms from A to $\mathbb{Q}/\mathbb{Z}$.

Theorem 2.17. *A finite abelian group is isomorphic to its own dual group.*

Proof. See Theorem 9.1 of Chapter I in [32] by Lang. □

Corollary 2.18. *Let A be a finite abelian group. Then the natural map $A \to \mathrm{Hom}(\widehat{A}, \mathbb{Q}/\mathbb{Z})$, $a \mapsto (f \mapsto f(a))$, is a group isomorphism.*

Proof. See Corollary 3.2 of Chapter 3 in [74]. □

Corollary 2.19. *Let A be a finite abelian group and let $\widehat{A}$ be the dual group of A. Then the pairing $A \times \widehat{A} \to \mathbb{Q}/\mathbb{Z}$, $(a, b) \mapsto b(a)$, is a perfect pairing.*

Proof. The result follows from Corollary 2.18. □

Corollary 2.20. *Let A be an abelian group, let B be a finite abelian group, and let $\beta : A \times B \to \mathbb{Q}/\mathbb{Z}$ be a map. If there is a group isomorphism $A \to \widehat{B}$ given by $a \mapsto \beta(a, \cdot)$, then β is a perfect pairing.*

Proof. Suppose there is a group isomorphism $A \to \widehat{B}$ given by $a \mapsto \beta(a, \cdot)$. By Theorem 2.2 the map β is a pairing. By Corollary 2.18 the map $B \to \mathrm{Hom}(\widehat{B}, \mathbb{Q}/\mathbb{Z})$, $b \mapsto (f \mapsto f(b))$, is a group isomorphism. Using the group isomorphism $A \to \widehat{B}$, $a \mapsto \beta(a, \cdot)$, we get the group isomorphism $B \to \mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z})$, $b \mapsto \beta(\cdot, b)$. Hence β is a perfect pairing. □

Definition 2.21 (Exponent of a group)**.** Let G be a group and let e_G be its identity element. The *exponent* of G is the smallest positive integer m, if there exists one, such that for every g in G one has $g^m = e_G$. Otherwise, the *exponent* of G is zero.

The following theorem was proved by Prüfer [3] for countable groups. The general case is due to Baer [3].

Theorem 2.22 (Prüfer [58], Baer [3])**.** *Let A be an abelian group of positive exponent. Then A is isomorphic to a direct sum of cyclic groups.*

Proof. See Corollary 10.37 of Chapter 10 in [60] by Rotman. □

Given a positive integer n and an abelian group A, the subset $\{a \in A : na = 0\}$ forms a subgroup of A. We denote it by $A[n]$.

Theorem 2.23. *Let A be a finite abelian group, let e be the exponent of A, and let C be an abelian group. Then the following are equivalent.*

(i) *There exist an abelian group B and a perfect pairing $\beta : A \times B \to C$.*

(ii) *The subgroup $C[e]$ of C is a cyclic group of order e.*

Proof. (ii) $\Longrightarrow$ (i) Let B be the dual $\widehat{A}$ of A. By Corollary 2.19 we have the perfect pairing $A \times B \to \mathbb{Q}/\mathbb{Z}$, $(a, b) \mapsto b(a)$. Since A has exponent e, the image of this pairing is contained in $\frac{1}{e}\mathbb{Z}/\mathbb{Z}$. Composing with an isomorphism $\frac{1}{e}\mathbb{Z}/\mathbb{Z} \xrightarrow{\sim} C[e]$ gives a perfect pairing $A \times B \to C$.

(i) $\Longrightarrow$ (ii) By definition of perfect pairing the group homomorphism $B \to \mathrm{Hom}(A, C)$, $b \mapsto \beta(\cdot, b)$ is a group isomorphism. Since for all $b \in B$ we have $e\beta(\cdot, b) = 0$, the exponent of B divides e and the image of β is contained in $C[e]$. A similar argument shows that e divides the exponent of B. Hence, they are equal. The group C contains an element c of order e, because $\mathrm{Hom}(A, C)$ has exponent e. By Theorem 2.22 the group B is isomorphic to a direct sum of cyclic groups. Since $\mathrm{Hom}(B, C)$ is finite, the group B is also finite. We have

$$B \cong \mathrm{Hom}(A, C) \supseteq \mathrm{Hom}(A, \langle c \rangle) \cong \widehat{A}$$

and

$$A \cong \mathrm{Hom}(B, C) \supseteq \mathrm{Hom}(B, \langle c \rangle) \cong \widehat{B}.$$

Theorem 2.17 implies that the inclusions are equalities. Since every element in $C[e]$ is in the image of at least one homomorphism $B \to C$, the equality $\mathrm{Hom}(B, C) = \mathrm{Hom}(B, \langle c \rangle)$ implies that all elements in $C[e]$ are in the group $\langle c \rangle$. □

Remark 2.24. Since for every finite cyclic group C' there is an injective group homomorphism $C' \hookrightarrow \mathbb{Q}/\mathbb{Z}$, by Theorem 2.23 every skew (symplectic) abelian group is similar to a skew (symplectic) abelian group of the form $(A, \mathbb{Q}/\mathbb{Z}, \beta)$, where A is a finite abelian group and β is an antisymmetric (alternating) perfect pairing. Hence, we will give results for skew (symplectic) abelian groups of the form $(A, \mathbb{Q}/\mathbb{Z}, \beta)$. By abuse of notation an element in $\mathbb{Q}/\mathbb{Z}$ will be often denoted only by a rational number.

2.2 The classification

We want to classify skew abelian groups up to similarity. By Remark 2.24 we will consider only skew abelian group of the form $(A, \mathbb{Q}/\mathbb{Z}, \beta)$, where A is a finite abelian group and β is an antisymmetric perfect pairing. Moreover, since the results do not change and isomorphism is a stronger notion than similarity, we will only classify skew abelian groups of the form $(A, \mathbb{Q}/\mathbb{Z}, \beta)$ up to isomorphism.

Theorem 2.25 (Classification of symplectic abelian groups)**.** *There is a bijection*

$$\{\text{finite abelian groups}\}/\cong \to \{\text{symplectic abelian groups } (A, \mathbb{Q}/\mathbb{Z}, \beta)\}/\cong,$$
$$[B] \mapsto [(B \oplus \widehat{B}, \mathbb{Q}/\mathbb{Z}, \gamma)],$$

where γ is the map

$$\gamma : (B \oplus \widehat{B}) \times (B \oplus \widehat{B}) \to \mathbb{Q}/\mathbb{Z},$$
$$((b_1, f_1), (b_2, f_2)) \mapsto f_2(b_1) - f_1(b_2).$$

Proof. Theorem 2.34 implies that the map is well-defined. By Theorem 2.60 it is surjective. The injectivity follows from Theorem 2.17 and the structure theorem for finite abelian groups. □

Definition 2.26 (p-rank)**.** Let p be a prime and let A be an abelian group. The *p-rank* $\mathrm{rk}_p(A)$ of A is the dimension of A/pA as a vector space over $\mathbb{Z}/p\mathbb{Z}$.

Remark 2.27. In order to simplify the exposition, Theorem 2.28 contains the following abuses of notation. The map

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathbb{Q}/\mathbb{Z},$$
$$(g_1, g_2) \mapsto \begin{cases} 0 & \text{if } g_1 = 0 \text{ or } g_2 = 0, \\ \frac{1}{2} & \text{if } g_1 = g_2 = 1 \bmod 2, \end{cases}$$

is denoted by $(g_1, g_2) \mapsto g_1 g_2/2$. In a similar way the map

$$\frac{1}{2}\mathbb{Z}/\mathbb{Z} \times \frac{1}{2}\mathbb{Z}/\mathbb{Z} \to \mathbb{Q}/\mathbb{Z},$$
$$(c_1, c_2) \mapsto \begin{cases} 0 & \text{if } c_1 = 0 \text{ or } c_2 = 0, \\ \frac{1}{2} & \text{if } c_1 = c_2 = \frac{1}{2}, \end{cases}$$

is denoted by $(c_1, c_2) \mapsto 2c_1c_2$.

Theorem 2.28 (Classification of skew abelian groups)**.**

(a) *Odd 2-rank: there is a bijection*

$$\{\text{finite abelian groups}\}/\cong \to \left\{ \begin{array}{l} \textit{skew abelian groups } (A, \mathbb{Q}/\mathbb{Z}, \beta) \\ \textit{of odd 2-rank} \end{array} \right\} /\cong,$$
$$[B] \mapsto [(\mathbb{Z}/2\mathbb{Z} \oplus B \oplus \widehat{B}, \mathbb{Q}/\mathbb{Z}, \gamma)],$$

where γ is the map

$$\gamma : (\mathbb{Z}/2\mathbb{Z} \oplus B \oplus \widehat{B}) \times (\mathbb{Z}/2\mathbb{Z} \oplus B \oplus \widehat{B}) \to \mathbb{Q}/\mathbb{Z},$$
$$((g_1, b_1, f_1), (g_2, b_2, f_2)) \mapsto \frac{g_1 g_2}{2} + f_2(b_1) - f_1(b_2).$$

(b) *Even 2-rank: there is a bijection*

$$\left\{ \begin{array}{l} (B, g)\textit{: } B \textit{ is a finite abelian} \\ \textit{group and } g \in B[2] \end{array} \right\} /\cong \to \left\{ \begin{array}{l} \textit{skew abelian groups } (A, \mathbb{Q}/\mathbb{Z}, \beta) \\ \textit{of even 2-rank} \end{array} \right\} /\cong,$$
$$[(B, g)] \mapsto [(B \oplus \widehat{B}, \mathbb{Q}/\mathbb{Z}, \gamma)],$$

where two pairs (B_1, g_1) and (B_2, g_2) on the left are defined to be isomorphic if there is a group isomorphism $\varphi : B_1 \to B_2$ with $\varphi(g_1) = g_2$ and where γ is the map

$$\gamma : (B \oplus \widehat{B}) \times (B \oplus \widehat{B}) \to \mathbb{Q}/\mathbb{Z},$$
$$((b_1, f_1), (b_2, f_2)) \mapsto f_2(b_1) - f_1(b_2) + 2f_1(g)f_2(g).$$

Proof. Theorem 2.36 and Theorem 2.38 imply that the maps are well-defined and the skew elements of $(\mathbb{Z}/2\mathbb{Z} \oplus B \oplus \widehat{B}, \mathbb{Q}/\mathbb{Z}, \gamma)$ in (a) and of $(B \oplus \widehat{B}, \mathbb{Q}/\mathbb{Z}, \gamma)$ in (b) are $(1, 0, 0)$ and $(g, 0)$, respectively. By Remark 2.31, Theorem 2.61, and Theorem 2.62 they are surjective. The injectivity in (a) follows from Theorem 2.17 and the structure theorem for finite abelian groups. Since isomorphisms of skew abelian groups map skew elements to skew elements, the injectivity in (b) follows from Lemma 2.30. □

Definition 2.29 (Heights)**.** Let A be an abelian group and let $a \in A$. The *height* of a is the largest positive integer n, if there exists one, such that the equation $nx = a$ has a solution $x \in A$. Otherwise, the *height* of a is infinite. Let p be a prime number. The *p-height* of a is the largest positive integer n, if there exists one, such that the equation $p^n x = a$ has a solution $x \in A$. Otherwise, the *p-height* of a is infinite.

Lemma 2.30. *Let B_1 and B_2 be finite abelian groups and let $g_1 \in B_1[2]$ and $g_2 \in B_2[2]$. Let t_1 and t_2 be the 2-heights of g_1 and g_2, respectively. Then the following are equivalent.*

(i) *There exists a group isomorphism $\varphi : B_1 \to B_2$ with $\varphi(g_1) = g_2$.*
(ii) *There exists a group isomorphism $B_1 \xrightarrow{\sim} B_2$ and $t_1 = t_2$.*

Proof. (i) $\implies$ (ii) Obvious.

(ii) $\implies$ (i) If g_1 is the zero element, then the implication is obvious. Hence, we may assume that g_1 is not the zero element. Since the order 2 of g_1 is prime, there exists $b_1 \in B_1$ such that $2^{t_1} b_1 = g_1$ and the subgroup $\langle b_1 \rangle$ is a direct summand of B_1. Similarly, there exists $b_2 \in B_2$ such that $2^{t_2} b_2 = g_2$ and the subgroup $\langle b_2 \rangle$ is a direct summand of B_2. From the equality $t_1 = t_2$ we get the group isomorphism $\langle b_1 \rangle \xrightarrow{\sim} \langle b_2 \rangle$, $b_1 \mapsto b_2$. Let H_1 and H_2 be finite abelian groups such that $B_1 \cong \langle b_1 \rangle \oplus H_1$ and $B_2 \cong \langle b_2 \rangle \oplus H_2$. The structure theorem for finite abelian groups implies the existence of a group isomorphism $H_1 \xrightarrow{\sim} H_2$. Now the result follows by extending the group isomorphism $\langle b_1 \rangle \xrightarrow{\sim} \langle b_2 \rangle$, $b_1 \mapsto b_2$, to a group isomorphism $B_1 \xrightarrow{\sim} B_2$. □

Remark 2.31. Theorem 2.61 and Theorem 2.62 imply that the case distinction in Theorem 2.28 is the same as the one in Corollary 2.14. Given a skew abelian group $(A, \mathbb{Q}/\mathbb{Z}, \beta)$ with skew element g, we have the following facts.

(a) The 2-rank $\mathrm{rk}_2(A)$ is odd if and only if one has $\beta(g, g) = 1/2$.

(b) The 2-rank $\mathrm{rk}_2(A)$ is even if and only if one has $\beta(g,g)=0$.

Remark 2.32. Since every symplectic abelian group is a skew abelian group, one may wonder where symplectic abelian groups occur in Theorem 2.28. They are the skew abelian groups given by the pairs (B,g) in (b) with $g=0$, because $(g,0)$ is the skew element of the skew abelian group $(B\oplus\widehat{B},\mathbb{Q}/\mathbb{Z},\gamma)$.

2.3 Examples

We show how to construct antisymmetric perfect pairings on finite abelian groups.

Example 2.33. Let p be a prime, let $r\in\mathbb{Z}_{\geq 0}$, and let $A=\mathbb{Z}/p^r\mathbb{Z}\oplus\mathbb{Z}/p^r\mathbb{Z}$. We denote by x and y the elements $(1,0)\in A$ and $(0,1)\in A$, respectively. The map $\langle x\rangle\times\langle y\rangle\to A$, $(x_1,x_2)\mapsto x_1+x_2$, is a group isomorphism. We construct a map $\beta:A\times A\to\mathbb{Q}/\mathbb{Z}$ by setting

$$\beta(x,x)=\beta(y,y)=0,\quad \beta(x,y)=-\beta(y,x)=\frac{1}{p^r},$$

and extending by bilinearity, that is, for all $i,j,k,l\in\mathbb{Z}$ we set

$$\beta(ix+jy,kx+ly)=ik\beta(x,x)+il\beta(x,y)+jk\beta(y,x)+jl\beta(y,y)=\frac{il-jk}{p^r}.$$

It is immediate to get $\beta(ix+jy,ix+jy)=0$ for all $i,j\in\mathbb{Z}$. Hence β is an alternating pairing. Moreover, for each $a\in A\setminus\{(0,0)\}$ we cannot have both $\beta(a,x)=0$ and $\beta(a,y)=0$. Hence, the group homomorphism $A\to\mathrm{Hom}(A,\mathbb{Q}/\mathbb{Z})$, $a\mapsto\beta(a,\cdot)$ is injective. Theorem 2.17 implies it is a group isomorphism. By Corollary 2.20 the map β is a perfect pairing. Hence $(A,\mathbb{Q}/\mathbb{Z},\beta)$ is a symplectic abelian group. The skew element of $(A,\mathbb{Q}/\mathbb{Z},\beta)$ is the zero element, because β is alternating.

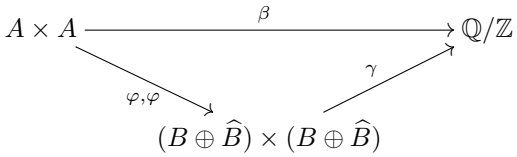
Let $B=\mathbb{Z}/p^r\mathbb{Z}$, let b be a generator of B, and let f be the element in $\widehat{B}$ such that $f(b)=1/p^r$. Consider the group isomorphism $\varphi:A\to B\oplus\widehat{B}$ defined by setting the images $\varphi(x)=(b,0)$ and $\varphi(y)=(0,f)$ of the generators x and y of A and extending to the whole group by the homomorphism property. Let γ be the map

$$\begin{aligned}\gamma:(B\oplus\widehat{B})\times(B\oplus\widehat{B})&\to\mathbb{Q}/\mathbb{Z},\\ ((b_1,f_1),(b_2,f_2))&\mapsto f_2(b_1)-f_1(b_2).\end{aligned}$$

By definition it is a pairing and we have

$$\gamma((b,0),(b,0))=\gamma((0,f),(0,f))=0,$$
$$\gamma((b,0),(0,f))=-\gamma((0,f),(b,0))=\frac{1}{p^r}.$$

Hence, we get the following commutative diagram.



The situation described in Example 2.33 is very general, as we can see in Theorem 2.34 and in Theorem 2.60.

Theorem 2.34. *Let B be a finite abelian group and γ be the map*

$$\begin{aligned}\gamma : (B \oplus \widehat{B}) \times (B \oplus \widehat{B}) &\to \mathbb{Q}/\mathbb{Z},\\ ((b_1, f_1), (b_2, f_2)) &\mapsto f_2(b_1) - f_1(b_2).\end{aligned}$$

Then the triple $(B \oplus \widehat{B}, \mathbb{Q}/\mathbb{Z}, \gamma)$ is a symplectic abelian group.

Proof. Corollary 2.19 implies that there are group homomorphisms

$$\begin{aligned} B \oplus \widehat{B} &\to \mathrm{Hom}(B, \mathbb{Q}/\mathbb{Z}), & B \oplus \widehat{B} &\to \mathrm{Hom}(\widehat{B}, \mathbb{Q}/\mathbb{Z})\\ (b_1, f_1) &\mapsto (b_2 \mapsto -f_1(b_2)), & (b_1, f_1) &\mapsto (f_2 \mapsto f_2(b_1)), \end{aligned}$$

and their kernels are the groups $B \oplus \{0\}$ and $\{0\} \oplus \widehat{B}$, respectively. Using the natural group isomorphism

$$\mathrm{Hom}(B \oplus \widehat{B}, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\sim} \mathrm{Hom}(B, \mathbb{Q}/\mathbb{Z}) \times \mathrm{Hom}(\widehat{B}, \mathbb{Q}/\mathbb{Z}),$$

we get an injective group homomorphism $B \oplus \widehat{B} \to \mathrm{Hom}(B \oplus \widehat{B}, \mathbb{Q}/\mathbb{Z})$, $(b_1, f_1) \mapsto ((b_2, f_2) \mapsto f_2(b_1) - f_1(b_2))$. Since by Theorem 2.17 the group $B \oplus \widehat{B}$ and its dual group are finite groups of the same cardinality, it is a group isomorphism. Corollary 2.20 implies that the map γ is a perfect pairing. A direct computation shows that it is also alternating. □

Example 2.35. Let $A = \mathbb{Z}/2\mathbb{Z}$ and let $\beta : A \times A \to \mathbb{Q}/\mathbb{Z}$ be the map defined by setting $\beta(1,1) = 1/2$ and $\beta(0,1) = \beta(1,0) = \beta(0,0) = 0$. We see that β is an antisymmetric perfect pairing and the skew element of the skew abelian group $(A, \mathbb{Q}/\mathbb{Z}, \beta)$ is 1. The perfect pairing β is not alternating, because we have $\beta(1,1) = 1/2$.

Example 2.35 describes the case of a skew abelian group $(A, \mathbb{Q}/\mathbb{Z}, \beta)$ with skew element g such that $\beta(g,g) = 1/2$. More generally, we have Theorem 2.36 and Theorem 2.61.

Theorem 2.36. *Let B be a finite abelian group and γ be the map*

$$\gamma : (\mathbb{Z}/2\mathbb{Z} \oplus B \oplus \widehat{B}) \times (\mathbb{Z}/2\mathbb{Z} \oplus B \oplus \widehat{B}) \to \mathbb{Q}/\mathbb{Z},$$
$$((g_1, b_1, f_1), (g_2, b_2, f_2)) \mapsto \frac{g_1 g_2}{2} + f_2(b_1) - f_1(b_2).$$

Then the triple $(\mathbb{Z}/2\mathbb{Z} \oplus B \oplus \widehat{B}, \mathbb{Q}/\mathbb{Z}, \gamma)$ is a skew abelian group of odd 2-rank and its skew element is $(1, 0, 0)$.

Proof. Since the pairing $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$, $(g_1, g_2) \mapsto 2g_1 g_2$, is perfect and by Corollary 2.19 the map $B \times \widehat{B} \to \mathbb{Q}/\mathbb{Z}$, $(b, f) \mapsto f(b)$, is also a perfect pairing, as in the proof of Theorem 2.34 we get an injective group homomorphism

$$\mathbb{Z}/2\mathbb{Z} \oplus B \oplus \widehat{B} \to \mathrm{Hom}(\mathbb{Z}/2\mathbb{Z} \oplus B \oplus \widehat{B}, \mathbb{Q}/\mathbb{Z}),$$
$$(g_1, b_1, f_1) \mapsto ((g_2, b_2, f_2) \mapsto 2g_1 g_2 + f_2(b_1) - f_1(b_2)).$$

It is also surjective, because by Theorem 2.17 it is an injective group homomorphism between two finite groups of the same cardinality. Corollary 2.20 implies that the map γ is a perfect pairing. A direct computation shows that γ is also antisymmetric and the skew element of $(\mathbb{Z}/2\mathbb{Z} \oplus B \oplus \widehat{B}, \mathbb{Q}/\mathbb{Z}, \gamma)$ is $(1, 0, 0)$. Hence $(\mathbb{Z}/2\mathbb{Z} \oplus B \oplus \widehat{B}, \mathbb{Q}/\mathbb{Z}, \gamma)$ is a skew abelian group and by Theorem 2.17 its 2-rank is odd. □

Example 2.37. Let $s \in \mathbb{Z}_{>0}$, and let $A = \mathbb{Z}/2^s\mathbb{Z} \oplus \mathbb{Z}/2^s\mathbb{Z}$. We denote by x and y the elements $(1, 0) \in A$ and $(0, 1) \in A$, respectively. The map $\langle x \rangle \times \langle y \rangle \to A$, $(x_1, x_2) \mapsto x_1 + x_2$, is a group isomorphism. We construct a map $\beta : A \times A \to \mathbb{Q}/\mathbb{Z}$ by setting

$$\beta(x, x) = 0, \quad \beta(x, y) = -\beta(y, x) = \frac{1}{2^s}, \quad \beta(y, y) = \frac{1}{2},$$

and extending by bilinearity as in Example 2.33. For all $i, j, k, l \in \mathbb{Z}$ we set

$$\beta(ix + jy, kx + ly) = \frac{il - jk}{2^s} + \frac{jl}{2}.$$

For all $i, j, k, l \in \mathbb{Z}$ we get

$$\beta(ix+jy, kx+ly) = \frac{il - jk}{2^s} + \frac{jl}{2} = -\left(\frac{kj - li}{2^s} + \frac{lj}{2}\right) = -\beta(kx+ly, ix+jy),$$

because we have $1/2 \equiv -1/2 \bmod \mathbb{Z}$. Hence β is an antisymmetric pairing. Moreover, for each $a \in A \setminus \{(0, 0)\}$ we cannot have both $\beta(a, x) = 0$ and $\beta(a, y) = 0$. Hence, the group homomorphism $A \to \mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z})$, $a \mapsto \beta(a, \cdot)$, is injective. Theorem 2.17 implies it is a group isomorphism. By Corollary 2.20

the map β is a perfect pairing. Hence $(A, \mathbb{Q}/\mathbb{Z}, \beta)$ is a skew abelian group. The skew element of $(A, \mathbb{Q}/\mathbb{Z}, \beta)$ is the element $2^{s-1}x$, because for all $i, j \in \mathbb{Z}$ we have

$$\beta(2^{s-1}x, ix + jy) = 2^{s-1}j\beta(x, y) = \frac{j}{2} = j\beta(y, y) = \beta(ix + jy, ix + jy).$$

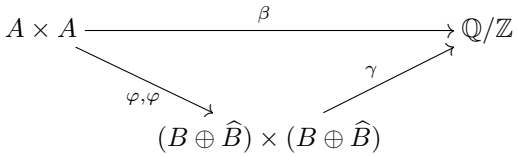
Let $B = \langle x \rangle$ be the subgroup of A generated by x and let f be the element in $\widehat{B}$ such that $f(x) = 1/2^s$. Note that we have $f(2^{s-1}x) = 1/2$. Consider the group isomorphism $\varphi : A \to B \oplus \widehat{B}$ defined by setting the images $\varphi(x) = (x, 0)$ and $\varphi(y) = (0, f)$ of the generators x and y of A and extending to the whole group by the homomorphism property. Let γ be the map

$$\gamma : (B \oplus \widehat{B}) \times (B \oplus \widehat{B}) \to \mathbb{Q}/\mathbb{Z},$$
$$((b_1, f_1), (b_2, f_2)) \mapsto f_2(b_1) - f_1(b_2) + \begin{cases} 0 & \text{if } f_1(g) = 0 \text{ or } f_2(g) = 0, \\ \frac{1}{2} & \text{if } f_1(g) = f_2(g) = \frac{1}{2}. \end{cases}$$

A straightforward computation shows that it is a pairing and we have

$$\gamma((x, 0), (x, 0)) = 0, \quad \gamma((0, f), (0, f)) = \frac{1}{2},$$
$$\gamma((b, 0), (0, f)) = -\gamma((0, f), (b, 0)) = \frac{1}{2^s}.$$

Hence, we get the following commutative diagram.



Example 2.37 describes the case of a skew abelian group $(A, \mathbb{Q}/\mathbb{Z}, \beta)$ with nontrivial skew element g such that $\beta(g, g) = 0$. More generally, we have Theorem 2.38 and Theorem 2.62.

Theorem 2.38. *Let B be a finite abelian group and let $g \in B[2]$. Then the triple $(B \oplus \widehat{B}, \mathbb{Q}/\mathbb{Z}, \gamma)$, where γ is the map*

$$\gamma : (B \oplus \widehat{B}) \times (B \oplus \widehat{B}) \to \mathbb{Q}/\mathbb{Z},$$
$$((b_1, f_1), (b_2, f_2)) \mapsto f_2(b_1) - f_1(b_2) + 2f_1(g)f_2(g),$$

is a skew abelian group of even 2-rank and its skew element is $(g, 0)$.

Proof. We claim that there are group homomorphisms

$$B \oplus \widehat{B} \to \mathrm{Hom}(B, \mathbb{Q}/\mathbb{Z}), \qquad B \oplus \widehat{B} \to \mathrm{Hom}(\widehat{B}, \mathbb{Q}/\mathbb{Z}),$$
$$(b_1, f_1) \mapsto (b_2 \mapsto -f_1(b_2)), \qquad (b_1, f_1) \mapsto (f_2 \mapsto f_2(b_1) + 2f_1(g)f_2(g)),$$

and the intersection of their kernels is $\{0\}$. A straightforward computation shows that there is a group homomorphism $B \oplus \widehat{B} \to \mathrm{Hom}(\widehat{B}, \mathbb{Q}/\mathbb{Z})$, $(b_1, f_1) \mapsto (f_2 \mapsto 2f_1(g)f_2(g))$. Now the claim follows from Corollary 2.19. As in the proof of Theorem 2.34, from the group homomorphisms of the claim we get an injective group homomorphism

$$B \oplus \widehat{B} \to \mathrm{Hom}(B \oplus \widehat{B}, \mathbb{Q}/\mathbb{Z}),$$
$$((b_1, f_1), (b_2, f_2)) \mapsto ((b_2, f_2) \mapsto f_2(b_1) - f_1(b_2) + 2f_1(g)f_2(g)).$$

Since by Theorem 2.17 the group $B \oplus \widehat{B}$ and its dual group are finite groups of the same cardinality, it is a group isomorphism. Corollary 2.20 implies that the map γ is a perfect pairing. A direct computation shows that γ is also antisymmetric and the skew element of $(B \oplus \widehat{B}, \mathbb{Q}/\mathbb{Z}, \gamma)$ is $(g, 0)$. Hence $(B \oplus \widehat{B}, \mathbb{Q}/\mathbb{Z}, \gamma)$ is a skew abelian group and by Theorem 2.17 its 2-rank is even. □

2.4 Pairings

We recall common definitions we have not used yet.

Definition 2.39 (Orthogonal or perpendicular)**.** Let A, B, and C be abelian groups and let $\beta : A \times B \to C$ be a pairing. An element $a \in A$ is *orthogonal* or *perpendicular* to a subset B' of B with respect to β if one has $\beta(a, b') = 0$ for all $b' \in B'$.

The set of elements of A orthogonal to a subset B' of B is a subgroup of A and is denoted by ${}^{\perp}B'$. If B' is a set with exactly one element b', then by abuse of notation we write ${}^{\perp}b'$ for ${}^{\perp}B'$. We make similar definitions for elements of B. If A' is a subset of A, then we denote by $A'^{\perp}$ the set of element of B orthogonal to A'. Note that we have ${}^{\perp}B = 0$ if and only if the group homomorphisms $A \to \mathrm{Hom}(B, C)$, $a \mapsto \beta(a, \cdot)$, is injective. Similarly, we have $A^{\perp} = 0$ if and only if the group homomorphism $B \to \mathrm{Hom}(A, C)$, $b \mapsto \beta(\cdot, b)$, is injective.

Remark 2.40. If a pairing $\beta : A \times A \to C$ is antisymmetric, then for each subset A' of A we have ${}^{\perp}A' = A'^{\perp}$. Hence, in this case we will use only the notation $A'^{\perp}$.

Definition 2.41 (Nondegenerate pairing)**.** Let A, B, and C be abelian groups. A pairing $\beta : A \times B \to C$ is a *nondegenerate pairing* if one has both ${}^{\perp}B = 0$ and $A^{\perp} = 0$.

2.5 Antisymmetric pairings

Theorem 2.42. *Let A be a finite abelian group, let C be an abelian group, and let $\beta : A \times A \to C$ be a perfect pairing. Then the following are equivalent.*

(i) *The map $Q : A \to C$, $a \mapsto \beta(a, a)$, is a group homomorphism.*

(ii) *The pairing $\beta : A \times A \to C$ is antisymmetric, that is, the triple (A, C, β) is a skew abelian group.*

(iii) *There exists $g \in A$ such that $\beta(g, a) = \beta(a, a)$ for all $a \in A$.*

(iv) *There exists a unique $g \in A$ such that $\beta(g, a) = \beta(a, a)$ for all $a \in A$.*

Proof. (i) $\implies$ (iv) Since the pairing $\beta : A \times A \to C$ is perfect, the group homomorphism $A \to \mathrm{Hom}(A, C)$, $a \mapsto \beta(a, \cdot)$, is a group isomorphism. Since we have $Q \in \mathrm{Hom}(A, C)$, there exists a unique $g \in A$ such that Q is the map $\beta(g, \cdot) : A \to C$.

(iv) $\implies$ (iii) Obvious.

(iii) $\implies$ (ii) For all $a, b \in A$ we have

$$\begin{aligned}\beta(a, b) + \beta(b, a) &= \beta(a + b, a + b) - \beta(a, a) - \beta(b, b) = \\ &= \beta(g, a + b) - \beta(g, a) - \beta(g, b) = \beta(g, 0) = 0.\end{aligned}$$

(ii) $\implies$ (i) For all $a, b \in A$ we see that

$$Q(a+b) = \beta(a, a)+\beta(a, b)+\beta(b, a)+\beta(b, b) = \beta(a, a)+\beta(b, b) = Q(a)+Q(b).$$

Hence, the map $Q : A \to C$, $a \mapsto \beta(a, a)$, is a group homomorphism. □

Definition 2.43 (Orthogonal sum)**.** Let I be an index set. For each $i \in I$ let A_i be a finite abelian group, let C_i be an abelian group, and let $\beta_i : A_i \times A_i \to C_i$ be an antisymmetric pairing. Suppose that for all but finitely many $i \in I$ the group A_i is trivial and that for each $i \in I$ there exists a positive integer e_i such that the group C_i' generated by the image of β_i in C_i is a cyclic group of exponent e_i. Let C be an abelian group such that for each $i \in I$ the subgroup $C[e_i]$ of C is cyclic of order e_i. For each $i \in I$ let $\psi_i : C_i' \to C$ be an injective group homomorphism. The *orthogonal sum*

$$\beta = \bigperp_{i \in I} \beta_i$$

of the sequence $(\beta_i)_{i \in I}$ of pairings is the pairing

$$\begin{aligned}\beta : \bigoplus_{i \in I} A_i \times \bigoplus_{i \in I} A_i &\to C, \\ ((a_i)_i, (b_i)_i) &\mapsto \sum_{i \in I} \psi_i(\beta_i(a_i, b_i)).\end{aligned}$$

Remark 2.44. Each map $\psi_i : C_i' \to C$ in Definition 2.43 is part of the structure of the orthogonal sum. The orthogonal sum depends on the choice of these maps.

Remark 2.45. In Definition 2.43 the group generated by the image of β in C is a cyclic subgroup of C and can be mapped injectively to $\mathbb{Q}/\mathbb{Z}$. In order to simplify the notation, now we restrict our attention to antisymmetric pairings with image contained in $\mathbb{Q}/\mathbb{Z}$ and to orthogonal sums where the maps $\psi_i : \frac{1}{e_i}\mathbb{Z}/\mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$ in Definition 2.43 are the inclusion maps.

Definition 2.46 (Skew pair)**.** A *skew pair* is a pair (A, β), where A is a finite abelian group and $\beta : A \times A \to \mathbb{Q}/\mathbb{Z}$ is an antisymmetric pairing.

Remark 2.47. Let (A, β) be a skew pair. If β is a perfect pairing, then $(A, \mathbb{Q}/\mathbb{Z}, \beta)$ is a skew abelian group.

Definition 2.48 (Isomorphism of skew pairs)**.** Let (A, β) and (B, γ) be skew pairs. An *isomorphism of skew pairs* is a group isomorphism $\varphi : A \to B$ such that for all $x, y \in A$ one has $\beta(x, y) = \gamma(\varphi(x), \varphi(y))$.

Remark 2.49. Let $(A, \mathbb{Q}/\mathbb{Z}, \beta)$ and $(B, \mathbb{Q}/\mathbb{Z}, \gamma)$ be skew abelian groups. They are isomorphic as skew pairs if and only if they are isomorphic as skew abelian groups.

Let A be an abelian group and let H_1 and H_2 be subgroups of A. If the map $H_1 \times H_2 \to A$, $(h_1, h_2) \mapsto h_1 + h_2$, is a group isomorphism, then we write $A = H_1 \times H_2$.

Let (A, β) be a skew pair and let H be a subgroup of A. Then $(H, \beta|_H)$ is also a skew pair, where $\beta|_H : H \times H \to \mathbb{Q}/\mathbb{Z}$ is the restriction of β to $H \times H$. Let H_1 and H_2 be subgroups of A. Then we write $(A, \beta) = (H_1, \beta|_{H_1}) \perp (H_2, \beta|_{H_2})$, if the map $H_1 \times H_2 \to A$, $(h_1, h_2) \mapsto h_1 + h_2$, is an isomorphism of skew pairs. In order to simplify the notation we will often write only $A = H_1 \perp H_2$ if there is no ambiguity on the pairing β.

Lemma 2.50. *Let (A, β) be a skew pair and let H_1 and H_2 be subgroups of A such that $A = H_1 \times H_2$. Then one has $A = H_1 \perp H_2$ if and only if H_1 and H_2 are orthogonal to each other.*

Proof. Let $a \in A$ and let $h_1 \in H_1$ and $h_2 \in H_2$ with $a = h_1 + h_2$. If we have $A = H_1 \perp H_2$, then $\beta(h_1, h_2) = \beta|_{H_1}(h_1, 0) + \beta|_{H_2}(0, h_2) = 0$. Hence H_1 and H_2 are orthogonal to each other.

Now suppose that H_1 and H_2 are orthogonal to each other. For all $g, h \in A$, $g_1, h_1 \in H_1$, $g_2, h_2 \in H_2$, with $g = g_1 + g_2$ and $h = h_1 + h_2$, we have

$$\begin{aligned}\beta(g, h) &= \beta(g_1 + g_2, h_1 + h_2) = \beta(g_1, h_1) + \beta(g_1, h_2) + \beta(g_2, h_1) + \beta(g_2, h_2) \\ &= \beta(g_1, h_1) + \beta(g_2, h_2) = \beta|_{H_1}(g_1, h_1) + \beta|_{H_2}(g_2, h_2).\end{aligned}$$

Hence, we get $A = H_1 \perp H_2$. □

Lemma 2.51. *Let (A, β) be a skew pair and let H_1 and H_2 be subgroups of A such that $A = H_1 \perp H_2$. Then β is a perfect pairing if and only if $\beta|_{H_1}$ and $\beta|_{H_2}$ are perfect pairings.*

Proof. The map $\varphi : A \to \mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z})$ may be written as

$$\varphi : H_1 \perp H_2 \to \mathrm{Hom}(H_1, \mathbb{Q}/\mathbb{Z}) \oplus \mathrm{Hom}(H_2, \mathbb{Q}/\mathbb{Z}).$$

Since H_1 and H_2 are orthogonal to each other, this map preserves the components. The map β is a perfect pairing, which is equivalent to φ being an isomorphism, if and only if φ induces group isomorphisms $H_1 \xrightarrow{\sim} \mathrm{Hom}(H_1, \mathbb{Q}/\mathbb{Z})$ and $H_2 \xrightarrow{\sim} \mathrm{Hom}(H_2, \mathbb{Q}/\mathbb{Z})$, that is, the maps $\beta|_{H_1}$ and $\beta|_{H_2}$ are perfect pairings. □

Lemma 2.52. *Let (A, β) be a skew pair and let H be a subgroup of A such that $(H, \mathbb{Q}/\mathbb{Z}, \beta|_H)$ is a skew abelian group. Then one has $A = H \perp H^\perp$. Moreover β is a perfect pairing if and only if $\beta|_{H^\perp}$ is a perfect pairing.*

Proof. By definition the kernel of the map $\varphi : A \to \mathrm{Hom}(H, \mathbb{Q}/\mathbb{Z})$, $a \mapsto (h \mapsto \beta(a, h))$, is $H^\perp$. Since $(H, \mathbb{Q}/\mathbb{Z}, \beta_H)$ is a skew abelian group, which is equivalent to $\varphi|_H$ being an isomorphism, we have $H \cap H^\perp = \{0\}$ and the natural map $H \to A/H^\perp$ is a group isomorphism. Hence, the subgroups H and $H^\perp$ span A. By Lemma 2.50 we get the decomposition $A = H \perp H^\perp$. The last statement follows from Lemma 2.51. □

Lemma 2.53. *Let $(A, \mathbb{Q}/\mathbb{Z}, \beta)$ and $(B, \mathbb{Q}/\mathbb{Z}, \gamma)$ be skew abelian groups. Then the orthogonal sum $(A, \mathbb{Q}/\mathbb{Z}, \beta) \perp (B, \mathbb{Q}/\mathbb{Z}, \gamma)$ is a skew abelian group.*

Proof. Apply Lemma 2.51 to the orthogonal sum. □

Lemma 2.54. *Let (A, β) be a skew pair and let H_1 and H_2 be subgroups of A such that $A = H_1 \times H_2$. If the exponents of H_1 and H_2 are coprime, then $A = H_1 \perp H_2$.*

Proof. Let e_1 and e_2 be the exponents of H_1 and H_2, respectively. Then for all $h_1 \in H_1$ and $h_2 \in H_2$ we have

$$e_1\beta(h_1, h_2) = e_2\beta(h_1, h_2) = 0.$$

Since e_1 and e_2 are coprime, we get $\beta(h_1, h_2) = 0$ for all $h_1 \in H_1$ and $h_2 \in H_2$. Hence H_1 and H_2 are orthogonal to each other and by Lemma 2.50 we have $A = H_1 \perp H_2$. □

Definition 2.55 (p-primary component of an abelian group)**.** Let p be a prime and let A be an abelian group. The *p-primary component* $A[p^\infty]$ of A is the subgroup

$$A[p^\infty] = \bigcup_{i \in \mathbb{Z}_{\geq 0}} A[p^i]$$

of A.

Theorem 2.56. *Let A be a torsion abelian group and for each prime p let $A[p^\infty]$ be its p-primary component. Then the map*

$$\bigoplus_{p \text{ prime}} A[p^\infty] \to A,$$
$$(a_p)_p \mapsto \sum_{p \text{ prime}} a_p,$$

is an isomorphism of abelian groups.

Proof. See Theorem 4.1.1 in Section 4.1 of Chapter 4 in [59] by Robinson. □

Theorem 2.57. *Let p be a prime, let (A, C, β) be a skew abelian group, and let $A[p^\infty]$ be the p-primary component of A. Then $(A[p^\infty], C, \beta|_{A[p^\infty]})$ is a skew abelian group.*

Proof. By Theorem 2.56 there is a subgroup H of A such that $A = A[p^\infty] \times H$ and the exponents of H and $A[p^\infty]$ are coprime. By Lemma 2.54 we get $A = A[p^\infty] \perp H$. The result follows from Lemma 2.51 . □

Definition 2.58 (p-primary component of a skew abelian group)**.** Let p be a prime, let (A, C, β) be a skew abelian group, and let $A[p^\infty]$ be the p-primary component of A. The *p-primary component* of (A, C, β) is the skew abelian group $(A[p^\infty], C, \beta|_{A[p^\infty]})$.

Theorem 2.59. *Let (A, C, β) be a skew abelian group and for each prime p let $(A[p^\infty], C, \beta|_{A[p^\infty]})$ be its p-primary component. Then the group isomorphism*

$$\varphi : \bigoplus_{p \text{ prime}} A[p^\infty] \to A,$$
$$(a_p)_p \mapsto \sum_{p \text{ prime}} a_p,$$

is an isomorphism

$$\bigperp_{p \text{ prime}} (A[p^\infty], C, \beta|_{A[p^\infty]}) = (A, C, \beta)$$

of skew abelian groups.

Proof. Since A is a finite abelian group, for all but finitely many primes p the group $A[p^\infty]$ is trivial. Hence, the orthogonal sum in the statement of the theorem is well-defined. The result follows from Theorem 2.56 and Lemma 2.54. □

Theorem 2.60. *Let $(A, \mathbb{Q}/\mathbb{Z}, \beta)$ be a symplectic abelian group. Then there exist a finite abelian group B and a group isomorphism $\varphi : A \xrightarrow{\sim} B \oplus \widehat{B}$ such that the diagram*

$$\begin{array}{ccc} A \times A & \xrightarrow{\quad\beta\quad} & \mathbb{Q}/\mathbb{Z} \\ & {\scriptstyle \varphi,\varphi} \searrow \quad \nearrow {\scriptstyle \gamma} & \\ & (B \oplus \widehat{B}) \times (B \oplus \widehat{B}) & \end{array}$$

commutes, where γ is the map

$$\begin{aligned} \gamma : (B \oplus \widehat{B}) \times (B \oplus \widehat{B}) &\to \mathbb{Q}/\mathbb{Z}, \\ ((b_1, f_1), (b_2, f_2)) &\mapsto f_2(b_1) - f_1(b_2). \end{aligned}$$

Proof. We pick an element $a \in A$ of maximal order e. Let $\langle a \rangle$ be the subgroup generated by a. Then the short exact sequence $0 \to \langle a \rangle \to A \to A/\langle a \rangle \to 0$ splits. We choose a splitting of the sequence. Composing the projection of A onto $\langle a \rangle$ with the isomorphism $\langle a \rangle \xrightarrow{\sim} \frac{1}{e}\mathbb{Z}/\mathbb{Z}$ that maps a to $\frac{1}{e}$ mod $\mathbb{Z}$ as in the diagram

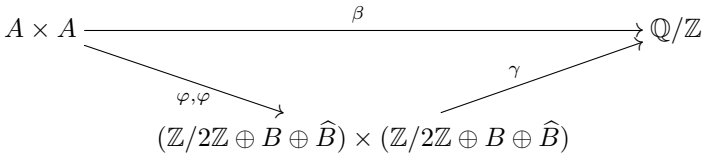
$$\begin{array}{ccc} A = \langle a \rangle \oplus A/\langle a \rangle & \twoheadrightarrow & \langle a \rangle \\ & \chi \searrow & \Big\downarrow {\scriptstyle \sim} \; {\scriptstyle a \mapsto \frac{1}{e} \bmod \mathbb{Z}} \\ & & \frac{1}{e}\mathbb{Z}/\mathbb{Z} \end{array}$$

gives a homomorphism $\chi : A \to \mathbb{Q}/\mathbb{Z}$. Since the pairing β is perfect, by duality there is an element $b \in A$ such that for all $x \in A$ one has $\chi(x) = \beta(x, b)$. Hence, we have $\beta(a, b) = \frac{1}{e}$ and the order of b is e. Since we have $\langle a \rangle \subset \langle a \rangle^{\perp}$ and $\langle b \rangle \cap \langle a \rangle^{\perp} = \{0\}$, the subgroups $\langle a \rangle$ and $\langle b \rangle$ form a direct sum $H = \langle a \rangle \oplus \langle b \rangle$ in A and the pairing $\beta|_H$ is perfect. By Lemma 2.52 we get the decomposition $A = H \perp H^{\perp}$ and the pairing $\beta|_{H^{\perp}}$ is perfect.

The pairing satisfies $\beta(a, a) = \beta(b, b) = 0$ and $\beta(a, b) = -\beta(b, a) = 1/e$. If we identify the group $\langle b \rangle$ with the dual group of $\langle a \rangle$ as above, the restriction of our pairing to $(\langle a \rangle \oplus \widehat{\langle a \rangle}) \times (\langle a \rangle \oplus \widehat{\langle a \rangle})$ becomes $((a_1, f_1), (a_2, f_2)) \mapsto f_2(a_1) - f_1(a_2)$. By induction on the order of the group A we conclude the proof. □

Theorem 2.61. *Let $(A, \mathbb{Q}/\mathbb{Z}, \beta)$ be a skew abelian group, let g be its skew element, and suppose $\beta(g, g) = 1/2$. Then there exist a finite abelian group B and a group isomorphism $\varphi : A \xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z} \oplus B \oplus \widehat{B}$ such that $\varphi(g) = (1, 0, 0)$*

and the diagram

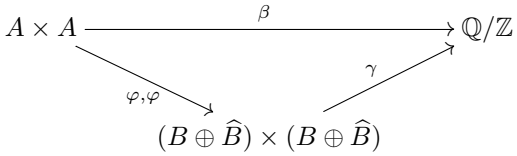


commutes, where γ is the map

$$\gamma : (\mathbb{Z}/2\mathbb{Z} \oplus B \oplus \widehat{B}) \times (\mathbb{Z}/2\mathbb{Z} \oplus B \oplus \widehat{B}) \to \mathbb{Q}/\mathbb{Z},$$
$$((g_1, b_1, f_1), (g_2, b_2, f_2)) \mapsto \frac{g_1 g_2}{2} + f_2(b_1) - f_1(b_2).$$

Proof. We have $g \notin \langle g \rangle^\perp$. Hence, the pairing $\beta|_{\langle g \rangle}$ is perfect. By Lemma 2.52 we get the decomposition $A = \langle g \rangle \perp \langle g \rangle^\perp$ and the pairing $\beta|_{\langle g \rangle^\perp}$ is perfect. It is also alternating, because $a \in \langle g \rangle^\perp$ implies $\beta(a, a) = \beta(g, a) = 0$. Hence $(\langle g \rangle^\perp, \mathbb{Q}/\mathbb{Z}, \beta|_{\langle g \rangle^\perp})$ is a symplectic abelian group. We conclude by combining Theorem 2.60 applied to $(\langle g \rangle^\perp, \mathbb{Q}/\mathbb{Z}, \beta|_{\langle g \rangle^\perp})$ and the skew abelian group isomorphism $\langle g \rangle \xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z}$, $g \mapsto 1 \bmod 2$, from $(\langle g \rangle, \mathbb{Q}/\mathbb{Z}, \beta|_{\langle g \rangle})$ to $(\mathbb{Z}/2\mathbb{Z}, \mathbb{Q}/\mathbb{Z}, (g_1, g_2) \mapsto g_1 g_2/2)$. □

Theorem 2.62. *Let $(A, \mathbb{Q}/\mathbb{Z}, \beta)$ be a skew abelian group, let g_A be its skew element, and suppose $\beta(g_A, g_A) = 0$. Then there exist a finite abelian group B, an element $g \in B[2]$, and a group isomorphism $\varphi : A \xrightarrow{\sim} B \oplus \widehat{B}$ such that $\phi(g_A) = (g, 0)$ and the diagram*



commutes, where γ is the map

$$\gamma : (B \oplus \widehat{B}) \times (B \oplus \widehat{B}) \to \mathbb{Q}/\mathbb{Z},$$
$$((b_1, f_1), (b_2, f_2)) \mapsto f_2(b_1) - f_1(b_2) + 2 f_1(g) f_2(g).$$

Moreover, for $g_A \neq 0$ there exists a subgroup H of A such that $A = H \perp H^\perp$, the triple $(H^\perp, \mathbb{Q}/\mathbb{Z}, \beta|_{H^\perp})$ is a symplectic abelian group, and $(H, \mathbb{Q}/\mathbb{Z}, \beta|_H)$ is a skew abelian group isomorphic to $(\mathbb{Z}/2^s\mathbb{Z} \oplus \mathbb{Z}/2^s\mathbb{Z}, \mathbb{Q}/\mathbb{Z}, \delta)$, where s is the largest positive integer such that the equation $2^{s-1}x = g_A$ has a solution $x \in A$ and δ is the map $\delta : \mathbb{Z}/2^s\mathbb{Z} \oplus \mathbb{Z}/2^s\mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$, $\delta((i, j), (k, l)) = (il - jk)/2^s + jl/2$.

Proof. The case $g_A = 0$ is Theorem 2.60. By Theorem 2.13 we are left with the case when g_A has order 2. By Lemma 2.54 we can assume that A is a 2-group. Let s be the largest positive integer such that the equation $2^{s-1}x = g_A$ has a solution $x \in A$. Since the order 2 of g_A is prime, there exists $a \in A$ such that $g_A = 2^{s-1}a$ and the subgroup $\langle a \rangle$ is a direct summand of A. We have $\beta(a,a) = \beta(a, g_A) = 2^{s-1}\beta(a,a) = 0$, because either $s = 1$ and $a = g_A$ or $s > 1$ and an odd multiple of $\beta(a,a)$ equals 0. Now, as in the proof of Theorem 2.60, there is $b \in A$ of order 2^s such that $\beta(a,b) = 1/2^s$, the subgroups $\langle a \rangle$ and $\langle b \rangle$ form a direct sum $H = \langle a \rangle \oplus \langle b \rangle$ in A, and the pairing $\beta|_H$ is perfect. By Lemma 2.52 we get the decomposition $A = H \perp H^\perp$ and the pairing $\beta|_{H^\perp}$ is perfect. It is also alternating, because $c \in H^\perp$ implies $c \in g_A^\perp$ and therefore $\beta(c,c) = \beta(g_A, c) = 0$. Hence, the triple $(H^\perp, \mathbb{Q}/\mathbb{Z}, \beta|_{H^\perp})$ is a symplectic abelian group.

The pairing satisfies $\beta(a,a) = 0$, $\beta(b,b) = 1/2$ and $\beta(a,b) = -\beta(b,a) = 1/2^s$. Hence, the group isomorphism $H \xrightarrow{\sim} \mathbb{Z}/2^s\mathbb{Z} \oplus \mathbb{Z}/2^s\mathbb{Z}$ given by $a \mapsto (1,0)$ and $b \mapsto (0,1)$ is an isomorphism between the skew abelian groups $(H, \mathbb{Q}/\mathbb{Z}, \beta|_H)$ and $(\mathbb{Z}/2^s\mathbb{Z} \oplus \mathbb{Z}/2^s\mathbb{Z}, \mathbb{Q}/\mathbb{Z}, \delta)$, where δ is the map $\delta : \mathbb{Z}/2^s\mathbb{Z} \oplus \mathbb{Z}/2^s\mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$, $\delta((i,j),(k,l)) = (il - jk)/2^s + jl/2$. If we identify the group $\langle b \rangle$ with the dual group $\widehat{\langle a \rangle}$ of $\langle a \rangle$ as in the proof of Theorem 2.60, the restriction of our pairing to $(\langle a \rangle \oplus \widehat{\langle a \rangle}) \times (\langle a \rangle \oplus \widehat{\langle a \rangle})$ becomes

$$((a_1, f_1), (a_2, f_2)) \mapsto f_2(a_1) - f_1(a_2) + 2f_1(g_A)f_2(g_A).$$

If we have $H^\perp = \{0\}$, then the result follows by taking $B = \mathbb{Z}/2^s\mathbb{Z}$, $g = 2^{s-1} \bmod 2^s\mathbb{Z} \in B$, and $\varphi : A \to B \oplus \widehat{B}$ such that $\phi(a) = (1,0)$ and $\varphi(b) = (0,1)$. Otherwise, the result follows by combining this particular case and Theorem 2.60 applied to the symplectic abelian group $(H^\perp, \mathbb{Q}/\mathbb{Z}, \beta|_{H^\perp})$. □

2.6 Wall's results

We summarize the results about isomorphism classes of skew abelian groups of the form $(A, \mathbb{Q}/\mathbb{Z}, \beta)$, where A is a finite abelian group and β is an antisymmetric perfect pairing, in [73] by Wall. We link his notation to our examples and proofs.

Let $\mathfrak{M}$ be the set of isomorphism classes of skew abelian groups of the form $(A, \mathbb{Q}/\mathbb{Z}, \beta)$. By Lemma 2.53 the orthogonal sum induces a commutative and associative operation on $\mathfrak{M}$. The class e of the trivial group is an identity element of this operation. Hence $\mathfrak{M}$ is an abelian monoid. We want to give generators and relations for $\mathfrak{M}$.

For p prime and $r \in \mathbb{Z}_{>0}$ define W_{p^r} as the isomorphism class in $\mathfrak{M}$ of $(A, \mathbb{Q}/\mathbb{Z}, \beta)$, where $A = \langle x \rangle \times \langle y \rangle$, the subgroups $\langle x \rangle$ and $\langle y \rangle$ of A have both

order p^r, and $\beta(x,x) = \beta(y,y) = 0$, $\beta(x,y) = -\beta(y,x) = 1/p^r$. This is the isomorphism class given by a cyclic group B of order p^r in Theorem 2.25. It is also the isomorphism class of the skew abelian group $(A, \mathbb{Q}/\mathbb{Z}, \beta)$ in Example 2.33 and of the skew abelian group $(H, \mathbb{Q}/\mathbb{Z}, \beta|_H)$ used in the proof of Theorem 2.60 when H has order p^{2r}.

Define Y_2 as the isomorphism class of the skew abelian group $(A, \mathbb{Q}/\mathbb{Z}, \beta)$, where $A = \langle g \rangle$ has order 2 and $\beta(g,g) = 1/2$. This is the isomorphism class given by the trivial group B in (a) of Theorem 2.28. It is also the isomorphism class of the skew abelian group $(A, \mathbb{Q}/\mathbb{Z}, \beta)$ in Example 2.35 and of the skew abelian group $(\langle g \rangle, \mathbb{Q}/\mathbb{Z}, \beta|_{\langle g \rangle})$ used in the proof of Theorem 2.61.

For $s \in \mathbb{Z}_{>0}$ define X_{2^s} as the isomorphism class of the skew abelian group $(A, \mathbb{Q}/\mathbb{Z}, \beta)$, where $A = \langle x \rangle \times \langle y \rangle$, the subgroups $\langle x \rangle$ and $\langle y \rangle$ of A have both order 2^s, and $\beta(x,x) = 0$, $\beta(x,y) = -\beta(y,x) = 1/2^s$, $\beta(y,y) = 1/2$. This is the isomorphism class given by a cyclic group B of order 2^s with $g \neq 0$ in (b) of Theorem 2.28. It is also the isomorphism class of the skew abelian group $(A, \mathbb{Q}/\mathbb{Z}, \beta)$ in Example 2.37 and of the skew abelian group $(H, \mathbb{Q}/\mathbb{Z}, \beta|_H)$ used in the proof of Theorem 2.62 when H has order 2^{2s}.

Theorem 2.63 (Wall [73])**.** *Let $(A, \mathbb{Q}/\mathbb{Z}, \beta)$ be a skew abelian group, let g be its skew element, and let W be the set $W = \{W_{p^r} : r \in \mathbb{Z}_{>0},\ p \text{ prime}\}$. Then the isomorphism class of $(A, \mathbb{Q}/\mathbb{Z}, \beta)$ in $\mathfrak{M}$ can be written*

(a) *uniquely as a finite sum of elements in W if β is alternating,*

(b) *as a sum of Y_2 and a finite sum of elements in W if $\beta(g,g) = 1/2$,*

(c) *as a sum of X_{2^s} and a finite sum of elements in W if $g \neq 0$, $\beta(g,g) = 0$, and s is the largest positive integer such that the equation $2^{s-1}x = g$ has a solution $x \in A$.*

Proof. Theorem 2.25 and (a) of Theorem 2.28 give (a) and (b), respectively. Combining (b) of Theorem 2.28, Lemma 2.30, and the orthogonal sum decomposition in Theorem 2.62 gives (c). □

Theorem 2.64 (Wall [73])**.** *The monoid $\mathfrak{M}$ is generated by the elements in the set*

$$M = \{W_{p^r}, Y_2, X_{2^s} : r \in \mathbb{Z}_{>0}, s \in \mathbb{Z}_{>0}, p \text{ prime}\}$$

with relations $Y_2 + Y_2 = X_2$, $Y_2 + X_{2^r} = Y_2 + W_{2^r}$, and $X_{2^r} + X_{2^s} = X_{2^r} + W_{2^s}$, where $r, s \in \mathbb{Z}_{>0}$ and $s \geq r$.

Proof. The result follows from Theorem 2.63. □

CHAPTER 3

The local norm-residue symbol

We introduce the concept of norm-residue symbol in the case of local fields. Most of the statements in this chapter are well-known. Our main new contribution is Theorem 3.80, which characterizes the norm-residue symbol in an elementary way.

3.1 Topological algebra

We consider groups, rings, and fields endowed with a topology and recall some properties when they are locally compact Hausdorff spaces.

Definition 3.1 (Topological group)**.** A *topological group* is a group $(G, \cdot)$ together with a topology on G such that the group operations

(a) $G \times G \to G,\ (x, y) \mapsto x \cdot y$,

(b) $G \to G,\ x \mapsto x^{-1}$,

are continuous, where $G \times G$ has the product topology.

Remark 3.2. We consider finite groups as topological groups by endowing them with the discrete topology.

Definition 3.3 (Locally compact)**.** A topological space X is *locally compact* if every point of X has a compact neighbourhood.

Definition 3.4 (σ-algebra)**.** A *σ-algebra* on a set X is a non empty collection Σ of subsets of X closed under the formation of complements and countable unions.

Definition 3.5 (Measure)**.** Let X be a set and let Σ be a σ-algebra on X. A *measure* μ on Σ is a function $\mu : \Sigma \to \mathbb{R}_{\geq 0} \cup \{+\infty\}$ such that $\mu(\emptyset) = 0$ and for any sequence $(X_i)_{i \in \mathbb{Z}_{>0}}$ of pairwise disjoint sets in Σ one has

$$\mu\left(\bigcup_{i=1}^{\infty} X_i\right) = \sum_{i=1}^{\infty} \mu(X_i).$$

Definition 3.6 (Left Haar measure)**.** Let G be a locally compact topological group and let $\mathcal{B}$ be the σ-algebra generated by the compact subsets of G. A *left Haar measure* on G is a measure $\mu : \mathcal{B} \to \mathbb{R}_{\geq 0} \cup \{+\infty\}$ with the following properties.

(a) It is not the zero measure.

(b) It is finite on all compact sets $C \in \mathcal{B}$.

(c) It is outer regular on all sets $B \in \mathcal{B}$:

$$\mu(B) = \inf\{\mu(U) : B \subseteq U, \text{ open } U \in \mathcal{B}\}.$$

(d) It is inner regular on all sets $B \in \mathcal{B}$:

$$\mu(U) = \sup\{\mu(C) : C \subseteq B, \text{ compact } C \in \mathcal{B}\}.$$

(e) It is invariant under left translation: for every $g \in G$ and every set $B \in \mathcal{B}$ one has $\mu(gB) = \mu(B)$.

Theorem 3.7 (Weil [75])**.** *Let G be a locally compact Hausdorff group. Then there exists a left Haar measure on G. If μ and ν are two left Haar measures on G, then there is $C \in \mathbb{R}_{>0}$ such that $\nu = C\mu$.*

Proof. We refer to Chapter XI in [23] by Halmos. See Theorem B in Section 58 for the existence and Theorem C in Section 60 for the uniqueness up to a positive constant. □

Remark 3.8. A ring $(R, +, \cdot)$ is assumed to have a multiplicative identity, which we denote by 1.

Definition 3.9 (Topological ring)**.** A *topological ring* is a ring $(R, +, \cdot)$ together with a topology on R such that the ring operations

(a) $R \times R \to R,\ (x, y) \mapsto x + y$,

(b) $R \times R \to R,\ (x, y) \mapsto x \cdot y$

are continuous, where $R \times R$ has the product topology.

Theorem 3.10. *Let R be a ring. Then the set of all invertible elements of R forms a group under multiplication.*

Proof. See Section 1 of Chapter II in [32] by Lang. □

Definition 3.11 (Group of units)**.** Let R be a ring. The *group of units* R^* of R is the group of all invertible elements of R.

Remark 3.12. The topology of a topological ring R, which is often called 'additive topology', induces a topology on the group R^*. This topology does not always render R^* a topological group, because the operation $R^* \to R^*$, $x \mapsto x^{-1}$, is not necessarily continuous with respect to the additive topology. A canonical way to repair this is to give R^* the subset topology coming from the injection

$$R^* \to R \times R,\ x \mapsto (x, x^{-1}),$$

of R^* into the topological product $R \times R$. This topology renders R^* a topological group and the inclusion map $R^* \hookrightarrow R$ is continuous.

The previous remark suggests the following definition of topological field.

Definition 3.13 (Topological field)**.** A *topological field* is a field F that is a topological ring such that the operation

$$F^* \to F^*,\ x \mapsto x^{-1},$$

is continuous with respect to the induced topology on F^*.

Theorem 3.14. *Let F be a locally compact Hausdorff topological ring that is a field. Then F is a topological field.*

Proof. See Section 2.3 of Chapter III in [28] by Iyanaga. □

3.2 Local fields

We recall some basic facts and terminology relative to local fields. We refer to [65] by Serre, to [9] by Cassels and Fröhlich, to [6] by Bourbaki, to [50] and [51] by Neukirch. Since the definitions of some concepts are not uniform, we provide a reference for our reader.

Definition 3.15 (Local field)**.** A *local field* is a non-discrete locally compact Hausdorff topological field.

Local fields have been completely classified by van Dantzig [72] and Pontryagin [55].

Theorem 3.16 (van Dantzig [72], Pontryagin [55])**.** *All of the following are local fields and every local field is isomorphic, as a topological field, to one of the following:*

(a) *the field $\mathbb{R}$ of real numbers;*

(b) *the field $\mathbb{C}$ of complex numbers;*
(c) *a finite field extension of $\mathbb{Q}_p$, the field of p-adic rationals, where p is a prime;*
(d) *the field $\mathbb{F}_q((t))$ of formal Laurent series in one variable t with coefficients in a finite field $\mathbb{F}_q$ of q elements.*

Proof. See Theorem 22 in Section 27 of Chapter 4 in [56] by Pontryagin. □

Definition 3.17 (Normalized absolute value)**.** Let F be a local field. The *normalized absolute value* $|\cdot|_F$ on F is the function

$$|\cdot|_F : F \to \mathbb{R}_{\geq 0}$$

such that for every $\alpha \in F$ the normalized absolute value $|\alpha|_F$ of α is given by the formula

$$|\alpha|_F = \frac{\mu(\alpha X)}{\mu(X)},$$

where μ is a Haar measure on the additive group F and X is any subset of F with $0 < \mu(X) < \infty$.

We will often use only the symbol $|\cdot|$ for the normalized absolute value when the field is understood.

Theorem 3.18. *Let F be a local field and let $|\cdot|_F : F \to \mathbb{R}_{\geq 0}$ be the normalized absolute value on F. Then for all $\alpha, \beta \in F$ one has*

$$|\alpha\beta|_F = |\alpha|_F \cdot |\beta|_F.$$

Proof. The formula follows from Definition 3.17. □

Definition 3.19 (Non-Archimedean and Archimedean local fields)**.** A local field F is *non-Archimedean* if for all $\alpha, \beta \in F$ one has

$$|\alpha + \beta| \leq \max\{|\alpha|, |\beta|\}.$$

Otherwise, it is *Archimedean*.

The fields of real and complex numbers are Archimedean fields. All local fields that are not isomorphic to any of those two fields are non-Archimedean.

Definition 3.20 (Extension of local fields)**.** An *extension of local fields* is a field extension F/E such that E and F are local fields and the inclusion $E \hookrightarrow F$ is continuous.

Theorem 3.21. *Let F/E be an extension of local fields. Then F/E is a finite field extension.*

Proof. See Theorem 3 in Section 2.4 of Chapter I in [6] by Bourbaki. □

Theorem 3.22. *Let F/E be an extension of local fields and let $|\cdot|_F : F \to \mathbb{R}_{\geq 0}$ and $|\cdot|_E : E \to \mathbb{R}_{\geq 0}$ be the normalized absolute values on F and E, respectively. Then for all $\alpha \in F$ one has*

$$|\alpha|_F = |\,\mathrm{N}_{F/E}\,\alpha|_E.$$

Proof. See Lemma in Section 11 of Chapter II in [9] by Cassels and Fröhlich. □

Theorem 3.23. *Let F be a non-Archimedean local field. Then the set of all elements of F whose normalized absolute value is less than or equal to* 1 *forms a ring under addition and multiplication.*

Proof. The result follows from Theorem 3.18 and Definition 3.19. □

Definition 3.24 (Ring of integers)**.** Let F be a non-Archimedean local field. The *ring of integers* $\mathcal{O}_F$ of F is the ring of all elements of F whose normalized absolute value is less than or equal to 1.

Theorem 3.25. *Let F be a non-Archimedean local field and let $\mathcal{O}_F$ be its ring of integers. Then the set of all elements of F whose normalized absolute value is equal to* 1 *forms the group $\mathcal{O}_F^*$ of invertible elements of $\mathcal{O}_F$ under multiplication.*

Proof. The result follows from Theorem 3.18. □

Definition 3.26 (Group of units)**.** Let F be a non-Archimedean local field and let $\mathcal{O}_F$ be its ring of integers. The *group of units* U_F of $\mathcal{O}_F$ is the group of elements of F whose normalized absolute value is equal to 1.

Remark 3.27. Note the equality $\mathcal{O}_F^* = U_F$. We introduce a different notation in analogy to Definition 3.36.

Theorem 3.28. *Let F be a non-Archimedean local field and let $\mathcal{O}_F$ be its ring of integers. Then $\mathcal{O}_F$ is a local ring with maximal ideal formed by the set of all elements of F whose normalized absolute value is less than* 1*.*

Proof. Theorem 3.18 and Definition 3.19 imply that the set of all elements of F whose normalized absolute value is less than 1 forms an ideal of $\mathcal{O}_F$. Theorem 3.25 shows that this ideal is the unique maximal ideal of $\mathcal{O}_F$. □

Definition 3.29 (Maximal ideal)**.** Let F be a non-Archimedean local field. The *maximal ideal* $\mathfrak{P}_F$ of the ring of integers of F is the additive group of all elements of F whose normalized absolute value is less than 1.

Definition 3.30 (Residue field)**.** Let F be a non-Archimedean local field, let $\mathcal{O}_F$ be the ring of integers of F, and let $\mathfrak{P}_F$ be the maximal ideal of $\mathcal{O}_F$. The *residue field* of F is the quotient $\mathcal{O}_F/\mathfrak{P}_F$.

Theorem 3.31. *Let F be a non-Archimedean local field. Then there exist a unique real number $C \in \mathbb{R}_{>1}$ and a unique surjective group homomorphism $\mathrm{v}_F : F^* \to \mathbb{Z}$ such that for all $\alpha \in F^*$ one has*

$$|\alpha| = C^{-\mathrm{v}_F(\alpha)}.$$

Proof. See Theorem 6 in Section 4 of Chapter I in [76] by Weil. □

Definition 3.32 (Normalized valuation)**.** Let F be a non-Archimedean local field. The *normalized valuation* on F is the function $\mathrm{v}_F : F \to \mathbb{Z} \cup \{+\infty\}$ such that $\mathrm{v}_F(0) = +\infty$ and $\mathrm{v}_F\,|_{F^*}$ equals the surjective group homomorphism $F^* \to \mathbb{Z}$ of Theorem 3.31.

We will often use only the symbol v for the normalized valuation when the field is understood and the symbol v_p for the normalized valuation on the field $\mathbb{Q}_p$ of p-adic rationals.

Definition 3.33 (Prime element)**.** Let F be a non-Archimedean local field. A *prime element* of F is an element in F whose normalized valuation is 1.

Theorem 3.34. *Let F be a non-Archimedean local field. Then the cardinality of its residue field is finite and equals the constant C of* Theorem 3.31.

Proof. See Theorem 6 in Section 4 of Chapter I in [76] by Weil. □

Theorem 3.35. *Let F be a non-Archimedean local field, let $\mathcal{O}_F$ be its ring of integers, and let $\mathfrak{P}_F$ be the maximal ideal of $\mathcal{O}_F$. Then for each $n \in \mathbb{Z}_{>0}$ the $\mathcal{O}_F$-ideal $\mathfrak{P}_F^n$ consists of all elements of F whose normalized valuation is greater than or equal to n.*

Proof. The result follows from Theorem 3.31. □

Definition 3.36 (Higher unit groups)**.** Let F be a non-Archimedean local field and let $\mathfrak{P}_F$ be the maximal ideal of its ring of integers. For each $n \in \mathbb{Z}_{>0}$ the *n-th higher unit group* $U_F^{(n)}$ of the ring of integers of F is the group $1+\mathfrak{P}_F^n$. The *0-th higher unit group* $U_F^{(0)}$ of the ring of integers of F is the group of units U_F.

Theorem 3.37. *Let F be a non-Archimedean local field, let q be the cardinality of its residue field, let U_F be the group of units of the ring of integers of F, and let μ_{q-1} be the group of $q-1$-th roots of unity in F. Then the short sequence*

$$1 \longrightarrow U_F \longrightarrow F^* \xrightarrow{\mathrm{v}} \mathbb{Z} \longrightarrow 1$$

is exact and split, the group μ_{q-1} is cyclic of order $q-1$, and the group U_F has the direct decomposition

$$U_F = \mu_{q-1} \times U_F^{(1)},$$

where $U_F^{(1)}$ is the first higher unit group of the ring of integers of F.

Proof. See Proposition 1.1 of Chapter III in [50] by Neukirch. □

Theorem 3.38. *Let F be a non-Archimedean local field of characteristic 0, let p and q be the characteristic and the cardinality of its residue field, respectively, let U_F be the group of units of the ring of integers of F, let d the degree of the extension $F/\mathbb{Q}_p$, where $\mathbb{Q}_p$ is the field of p-adic rationals, and let $\mathbb{Z}_p$ be the ring of integers of $\mathbb{Q}_p$. Then there exists $a \in \mathbb{Z}_{\geq 0}$ such that there is an isomorphism of topological groups*

$$U_F \cong \mathbb{Z}/(q-1)\mathbb{Z} \oplus \mathbb{Z}/p^a\mathbb{Z} \oplus \mathbb{Z}_p^d.$$

Proof. See Proposition 5.7 of Chapter II in [51] by Neukirch. □

Theorem 3.39. *Let p be a prime, let F be a non-Archimedean local field of characteristic p, let q be the cardinality of its residue field, and let U_F be the group of units of the ring of integers of F. Then there is an isomorphism of topological groups*

$$U_F \cong \mathbb{Z}/(q-1)\mathbb{Z} \oplus \mathbb{Z}_p^{\mathbb{Z}},$$

where $\mathbb{Z}_p^{\mathbb{Z}}$ is endowed with the product topology.

Proof. See Proposition 5.7 of Chapter II in [51] by Neukirch. □

3.3 Abelian Kummer theory

Definition 3.40 (Exponent of a Galois field extension)**.** The *exponent of a Galois field extension L/K* is the exponent of the Galois group $\mathrm{Gal}(L/K)$.

Definition 3.41 (Abelian field extension)**.** An *abelian field extension* is a Galois field extension L/K such that the Galois group $\mathrm{Gal}(L/K)$ is abelian.

Definition 3.42 (Cyclic field extension)**.** A *cyclic field extension* is a Galois field extension L/K such that the Galois group $\mathrm{Gal}(L/K)$ is cyclic.

Definition 3.43 (Kummer m-extension)**.** Let m be a positive integer. A *Kummer m-extension* is an abelian field extension L/K of exponent dividing m such that the field K contains a primitive m-th root of unity.

Theorem 3.44. *Let m be a positive integer and let K be a field containing a primitive m-th root of unity. Then there is an inclusion preserving bijection*

$$\begin{aligned}\{\textit{Kummer } m\textit{-extensions of } K\}/{\cong_K} &\leftrightarrow \{\textit{subgroups of } K^*/{K^*}^m\},\\ L &\mapsto (L^{*m} \cap K^*)/K^{*m},\\ K(\sqrt[m]{\Delta}) &\hookleftarrow \Delta\end{aligned}$$

Proof. See Theorem 8.2 in Section 8 of Chapter VI in [32] by Lang. □

Remark 3.45. On the Galois group $\mathrm{Gal}(L/K)$ of a Galois field extension L/K we consider the Krull topology. If G is a topological group and H is an abelian topological group, then the set of continuous group homomorphisms $G \to H$ forms an abelian group under pointwise addition. We denote the group of continuous group homomorphisms from G to H by $\mathrm{Hom}(G, H)$.

Definition 3.46 (Compact-open topology)**.** Let X and Y be topological spaces and let $\mathrm{C}(X, Y)$ be the set of continuous functions $X \to Y$. The *compact-open topology* on the set $\mathrm{C}(X, Y)$ is the topology generated by the sets of the form

$$V(K, U) = \{f \in \mathrm{C}(X, Y) : f(K) \subseteq U\},$$

where K ranges over the compact subsets of X and U ranges over the open subsets of Y.

Theorem 3.47. *Let m be a positive integer, let K be a field containing a primitive m-th root of unity, let μ_m be the group of m-th roots of unity in K, let L be a Kummer m-extension of K, and let Δ be the discrete group $(L^{*m} \cap K^*)/K^{*m}$. Then there is a perfect pairing*

$$\begin{aligned}\mathrm{Gal}(L/K) \times \Delta &\to \mu_m,\\ (\sigma, a) &\mapsto \frac{\sigma(\sqrt[m]{a})}{\sqrt[m]{a}},\end{aligned}$$

that is, the map that sends an element $a \in \Delta$ to the character $\sigma \mapsto \frac{\sigma(\sqrt[m]{a})}{\sqrt[m]{a}}$ is a canonical isomorphism of topological groups

$$\Delta \cong \mathrm{Hom}(\mathrm{Gal}(L/K), \mu_m)$$

and the map that sends an automorphism $\sigma \in \mathrm{Gal}(L/K)$ to the character $a \mapsto \frac{\sigma(\sqrt[m]{a})}{\sqrt[m]{a}}$ is a canonical isomorphism of topological groups

$$\mathrm{Gal}(L/K) \cong \mathrm{Hom}(\Delta, \mu_m),$$

where the groups $\mathrm{Hom}(\mathrm{Gal}(L/K), \mu_m)$ and $\mathrm{Hom}(\Delta, \mu_m)$ are endowed with the compact-open topology.

Proof. See Theorem 5.3 of Chapter I in [50] by Neukirch. □

Remark 3.48. Let m be a positive integer and let K be a field containing a primitive m-th root of unity. Within a fixed algebraic closure of K there exists a unique maximal Kummer m-extension $L = K(\sqrt[m]{K^*})$, because L is a Kummer m-extension and all Kummer m-extensions of K are contained in L. By Theorem 3.47 we have a canonical isomorphism of topological groups

$$K^*/K^{*m} \cong \mathrm{Hom}(\mathrm{Gal}(L/K), \mu_m).$$

3.4 Local class field theory

We state the main theorem of local class field theory about the local reciprocity map and some related results. See [50] by Neukirch and Chapter VI in [9] by Cassels and Fröhlich as references.

Theorem 3.49. *Let l/k be an extension of finite fields. The map $\varphi : l \to l$, $x \mapsto x^{\#k}$, is an automorphism of l over k.*

Proof. See Theorem 5.5 in Section 5 of Chapter V in [32] by Lang. □

Definition 3.50 (Frobenius automorphism)**.** Let l/k be an extension of finite fields. The *Frobenius automorphism* of l over k is the automorphism of l that maps any element x in l to $x^{\#k}$.

Theorem 3.51. *Let l/k be an extension of finite fields. Then the extension l/k is Galois and its Galois group* $\mathrm{Gal}(l/k)$ *is cyclic and generated by the Frobenius automorphism of l over k.*

Proof. See Theorem 5.5 in Section 5 of Chapter V in [32] by Lang. □

Definition 3.52 (Unramified extension of non-Archimedean local fields)**.** Let F/E be an extension of non-Archimedean local fields and let $\mathcal{O}_F/\mathfrak{P}_F$ and $\mathcal{O}_E/\mathfrak{P}_E$ be the residue fields of F and E, respectively. The extension F/E is *unramified* if one has

$$[F : E] = [\mathcal{O}_F/\mathfrak{P}_F : \mathcal{O}_E/\mathfrak{P}_E].$$

Theorem 3.53. *Let F/E be an unramified extension of non-Archimedean local fields and let $\mathrm{v}_F : F^* \to \mathbb{Z}$ and $\mathrm{v}_E : E^* \to \mathbb{Z}$ be the normalized valuations on F and E, respectively. Then one has*

$$\mathrm{v}_F\,|_E = \mathrm{v}_E\,.$$

Proof. By definition $\mathrm{v}_F(0) = +\infty = \mathrm{v}_E(0)$. Let $\mathcal{O}_F/\mathfrak{P}_F$ and $\mathcal{O}_E/\mathfrak{P}_E$ be the residue fields of F and E, respectively. Since the extension F/E is unramified, we have

$$[F : E] = [\mathcal{O}_F/\mathfrak{P}_F : \mathcal{O}_E/\mathfrak{P}_E].$$

Using Theorem 3.22 and Theorem 3.34 we get for all $\alpha \in E^*$

$$|\mathcal{O}_F/\mathfrak{P}_F|^{-\mathrm{v}_F(\alpha)} = |\mathcal{O}_E/\mathfrak{P}_E|^{-\mathrm{v}_E(\mathrm{N}_{F/E}\,\alpha)}.$$

Taking the logarithm in base $|\mathcal{O}_E/\mathfrak{P}_E|$ of both sides gives

$$-[F : E]\,\mathrm{v}_F(\alpha) = -\,\mathrm{v}_E(\mathrm{N}_{F/E}\,\alpha).$$

The result follows from the equality $\mathrm{N}_{F/E}\,\alpha = \alpha^{[F:E]}$ for all $\alpha \in E$. □

Theorem 3.54. *Let F/E be an unramified extension of non-Archimedean local fields and let $\mathcal{O}_F/\mathfrak{P}_F$ and $\mathcal{O}_E/\mathfrak{P}_E$ be the residue fields of F and E, respectively. Then the extension F/E is Galois and the map that sends an automorphism in $\mathrm{Gal}(F/E)$ to its induced automorphism in $\mathrm{Gal}((\mathcal{O}_F/\mathfrak{P}_F)/(\mathcal{O}_E/\mathfrak{P}_E))$ by restriction to the rings of integers and reduction modulo the maximal ideals is a canonical isomorphism*

$$\mathrm{Gal}(F/E) \cong \mathrm{Gal}((\mathcal{O}_F/\mathfrak{P}_F)/(\mathcal{O}_E/\mathfrak{P}_E)).$$

Proof. See Corollary of Theorem 1 in Section 7 of Chapter 1 in [9] by Cassels and Fröhlich. □

Definition 3.55 (Frobenius element)**.** Let F/E be an unramified extension of non-Archimedean local fields. The *Frobenius element* $\mathrm{Fr}_{F/E}$ is the automorphism in the Galois group $\mathrm{Gal}(F/E)$ that induces the Frobenius automorphism on the corresponding extension of residue fields.

Theorem 3.56. *Let F/E be an unramified extension of non-Archimedean local fields. Then the Galois group $\mathrm{Gal}(F/E)$ is cyclic and generated by the Frobenius element $\mathrm{Fr}_{F/E}$.*

Proof. By Theorem 3.54 the Galois group $\mathrm{Gal}(F/E)$ is isomorphic to the Galois group of an extension of finite fields, which is, by Theorem 3.51, cyclic and generated by the Frobenius automorphism. □

Theorem 3.57. *Let $\mathcal{L}$ be the category whose objects are local fields and whose morphisms are continuous homomorphisms of fields, let $E \to F$ be a morphism of local fields, and let $\mathrm{N}_{F/E} : F \to E$ be the norm map from F to E. Then there is a unique system of group homomorphisms*

$$r_{F/E} : \mathrm{Gal}(F/E) \to E^*/\,\mathrm{N}_{F/E}\,F^*$$

indexed by all morphisms $E \to F$ in $\mathcal{L}$ with F/E Galois with the following properties.

(a) *For each commutative diagram in* $\mathcal{L}$

$$\begin{array}{ccc} E & \longrightarrow & F \\ \downarrow & & \downarrow \\ K & \longrightarrow & L \end{array}$$

with F/E *and* L/K *Galois, the diagram*

$$\begin{array}{ccc} \mathrm{Gal}(L/K) & \xrightarrow{r_{L/K}} & K^*/\,\mathrm{N}_{L/K}\,L^* \\ \Big\downarrow{\scriptstyle \mathrm{res}} & & \Big\downarrow{\scriptstyle \mathrm{N}_{K/E}} \\ \mathrm{Gal}(F/E) & \xrightarrow{r_{F/E}} & E^*/\,\mathrm{N}_{F/E}\,F^* \end{array}$$

commutes, where the map $\mathrm{res} : \mathrm{Gal}(L/K) \to \mathrm{Gal}(F/E)$ *is given by restricting to* F *the automorphisms of* L *over* K*.*

(b) *If* E *is Archimedean, then the group homomorphism*

$$r_{F/E} : \mathrm{Gal}(F/E) \to E^*/\,\mathrm{N}_{F/E}\,F^*$$

is surjective.

(c) *If* E *is non-Archimedean and the extension* F/E *is unramified, then there is a commutative diagram*

$$\begin{array}{ccc} \mathrm{Gal}(F/E) & \xrightarrow{r_{F/E}} & E^*/\,\mathrm{N}_{F/E}\,F^* \\ \Big\downarrow{\scriptstyle \sim} & & \Big\downarrow{\scriptstyle \mathrm{v}} \\ \mathrm{Gal}((\mathcal{O}_F/\mathfrak{P}_F)/(\mathcal{O}_E/\mathfrak{P}_E)) & \xrightarrow{\sim} & \mathbb{Z}/[F:E]\mathbb{Z} \end{array}$$

where the map

$$\mathrm{Gal}(F/E) \xrightarrow{\sim} \mathrm{Gal}((\mathcal{O}_F/\mathfrak{P}_F)/(\mathcal{O}_E/\mathfrak{P}_E))$$

is the isomorphism of Theorem 3.54*, the vertical map*

$$\mathrm{v} : E^*/\,\mathrm{N}_{F/E}\,F^* \longrightarrow \mathbb{Z}/[F:E]\mathbb{Z}$$

is the group homomorphism induced by the normalized valuation on E *modulo* $[F:E]$*, and the isomorphism*

$$\mathrm{Gal}((\mathcal{O}_F/\mathfrak{P}_F)/(\mathcal{O}_E/\mathfrak{P}_E)) \xrightarrow{\sim} \mathbb{Z}/[F:E]\mathbb{Z}$$

maps the Frobenius automorphism of $\mathcal{O}_F/\mathfrak{P}_F$ *over* $\mathcal{O}_E/\mathfrak{P}_E$ *to the residue class* $1 \bmod [F:E]$*.*

Proof. See Section 2 of Chapter III in [50] by Neukirch. □

Definition 3.58 (Local reciprocity maps)**.** The *local reciprocity maps* are the group homomorphisms $r_{F/E}$ in Theorem 3.57.

Theorem 3.59. *Let F/E be a Galois extension of local fields and let $\mathrm{Gal}(F/E)^{\mathrm{ab}}$ be the abelianization of the Galois group of F over E. Then each local reciprocity map $r_{F/E}$ induces a group isomorphism*

$$\mathrm{Gal}(F/E)^{\mathrm{ab}} \xrightarrow{\sim} E^*/\,\mathrm{N}_{F/E}\,F^*. \tag{3.60}$$

Proof. See Theorem 2.1 in Section 2 of Chapter III in [50] by Neukirch. □

Definition 3.61 (Norm-residue map)**.** Let F/E be a Galois extension of local fields and let $\mathrm{Gal}(F/E)^{\mathrm{ab}}$ be the abelianization of the Galois group of F over E. The *norm-residue map* $\psi_{F/E}$ of the extension F/E is the surjective homomorphism

$$\psi_{F/E} : E^* \to \mathrm{Gal}(F/E)^{\mathrm{ab}}$$

obtained by composing the inverse $E^*/\,\mathrm{N}_{F/E}\,F^* \to \mathrm{Gal}(F/E)^{\mathrm{ab}}$ of the group isomorphism 3.60 with the projection $E^* \to E^*/\,\mathrm{N}_{F/E}\,F^*$.

Remark 3.62. By taking projective limits the norm-residue map gives rise to a norm-residue map for any arbitrary Galois extension F/E of a given local field E. In the particular case of the maximal abelian extension of E we denote by

$$\psi_E : E^* \to G_E^{\mathrm{ab}}$$

the norm-residue map from E^* to the Galois group G_E^{ab} of the maximal abelian extension of E.

Theorem 3.63 (Local existence theorem)**.** *Let E be a local field. A subgroup of E^* is of the form $\mathrm{N}_{F/E}\,F^*$ for some abelian extension F/E of local fields if and only if it is of finite index and open.*

Proof. See Theorem 3 in Section 2.7 of Chapter VI in [9] by Cassels and Fröhlich. □

Theorem 3.64. *Let m be a positive integer, let E be a local field containing a primitive m-th root of unity, and let $F = E(\sqrt[m]{E^*})$ be the maximal Kummer m-extension of E within a fixed algebraic closure of E. Then the extension F/E is finite, one has*

$$\mathrm{N}_{F/E}\,F^* = E^{*m},$$

and the norm-residue map $\psi_{F/E}$ induces an isomorphism

$$E^*/E^{*m} \xrightarrow{\sim} \mathrm{Gal}(F/E).$$

Proof. By Theorem 3.37, Theorem 3.38, and Theorem 3.39 the subgroup E^{*m} of E is of finite index and open. Theorem 3.63 implies that there exists some abelian extension L/E of local fields such that $\mathrm{N}_{L/E}\, L^* = E^{*m}$. By Theorem 3.21 the extension L/E is finite. By Theorem 3.59 the local reciprocity map $r_{L/E}$ gives the isomorphism

$$\mathrm{Gal}(L/E) \xrightarrow{\sim} E^*/E^{*m}.$$

Hence, the norm-residue map $\psi_{F/E}$ induces an isomorphism

$$E^*/E^{*m} \xrightarrow{\sim} \mathrm{Gal}(F/E).$$

Since E^*/E^{*m} is the maximal quotient group of E^* of exponent dividing m, the extension L/E is the maximal Kummer m-extension of E. □

Theorem 3.65 (Norm limitation theorem)**.** *Let E/F be an extension of local fields and let L be the largest abelian extension of F contained in E. Then one has*

$$\mathrm{N}_{E/F}\, E^* = \mathrm{N}_{L/F}\, L^*.$$

Proof. See Proposition 4 in Section 2.6 of Chapter VI in [9] by Cassels and Fröhlich. □

Corollary 3.66. *Let E/F be an extension of local fields and let L be the largest abelian extension of F contained in E. Let $U_E^{(1)}$ and $U_L^{(1)}$ be the first higher unit groups of the rings of integers of E and of L, respectively. Then one has*

$$\mathrm{N}_{E/F}\, U_E^{(1)} = \mathrm{N}_{L/F}\, U_L^{(1)}$$

Proof. Let U_E, U_L, and U_F be the unit groups of the rings of integers of E, of L, and of F, respectively. Since we have $\mathrm{N}_{E/F}\, U_E = (\mathrm{N}_{E/F}\, E^*) \cap U_F$ and $\mathrm{N}_{L/F}\, U_L = (\mathrm{N}_{L/F}\, L^*) \cap U_F$, the result follows from Theorem 3.65 and the direct decompositions of Theorem 3.37. □

3.5 The norm-residue symbol

Given a positive integer m, we introduce the m-th power norm-residue symbol.

Definition 3.67 (m-th power norm-residue symbol)**.** Let m be a positive integer, let F be a local field containing a primitive m-th root of unity, let μ_m be the group of m-th roots of unity in F, and let $\psi_F : F^* \to G_F^{\mathrm{ab}}$ be the norm-residue map. The *m-th power norm-residue symbol* is the map

$$\begin{aligned}(\cdot,\cdot)_{F,m} : F^* \times F^* &\to \mu_m,\\ (a,b) &\mapsto (a,b)_{F,m},\end{aligned}$$

such that for all $a, b \in F^*$ one has

$$(a,b)_{F,m} = \psi_F(a)(\beta)/\beta,$$

where $\beta^m = b$ with β in an algebraic closure of F.

Remark 3.68. The m-th power norm-residue symbol is well-defined. The definition does not depend on the choice of β, because F contains the group of m-th roots of unity.

We will often write only '$(\cdot,\cdot)$' and 'norm-residue symbol' when m and F are understood.

Theorem 3.69. *Let m be a positive integer, let F be a local field containing a primitive m-th root of unity, and let μ_m be the group of m-th roots of unity in F. Then the norm-residue symbol is a pairing*

$$(\cdot,\cdot) : F^* \times F^* \to \mu_m.$$

Proof. Since by Definition 3.61 the norm-residue map is a homomorphism, for all $a, b, c \in F^*$ we get

$$(ac,b) = \frac{\psi(ac)(\beta)}{\beta} = \frac{\psi(a)(\psi(c)(\beta))}{\beta} = \frac{\psi(a)(\beta')}{\beta'}\frac{\psi(c)(\beta)}{\beta} = (a,b)\,(c,b)\,,$$

where $\beta^m = b$ and $\beta' = \psi(c)(\beta)$. Note that $(\beta')^m = b$, because $\psi(c)$ is a field automorphism that is the identity on F. Moreover, if $\gamma^m = c$, we have

$$(a,bc) = \frac{\psi(a)(\beta\gamma)}{\beta\gamma} = \frac{\psi(a)(\beta)}{\beta}\frac{\psi(a)(\gamma)}{\gamma} = (a,b)\,(a,c)\,.$$

Hence, the norm-residue symbol is a pairing. □

Let m be a positive integer and let F be a local field containing a primitive m-th root of unity. Now we want to apply both Kummer theory and local class field theory to the maximal abelian extension of F of exponent dividing m, that is, the field extension $L = F(\sqrt[m]{F^*})$, and to see how we can obtain the norm-residue symbol. By Theorem 3.64 of local class field theory the norm-residue map $\psi_{L/F}$ induces a canonical isomorphism

$$F^*/{F^*}^m \cong \mathrm{Gal}(L/F).$$

Combining this isomorphism and the perfect pairing

$$\begin{aligned} \mathrm{Gal}(L/F) \times F^*/{F^*}^m &\to \mu_m, \\ (\sigma, a) &\mapsto \frac{\sigma(\sqrt[m]{a})}{\sqrt[m]{a}}. \end{aligned}$$

of Theorem 3.47 yields the perfect pairing

$$(\cdot,\cdot) : F^*/F^{*m} \times F^*/F^{*m} \to \mu_m$$
$$(a,b)_m = \psi_{L/F}(a)(\beta)/\beta,$$

where $\beta^m = b$, which is equal to the pairing induced by the norm-residue symbol. We have proved the following theorem.

Theorem 3.70. *Let m be a positive integer, let F be a local field containing a primitive m-th root of unity, and let μ_m be the group of m-th roots of unity in F. Then the norm-residue symbol induces a perfect pairing*

$$(\cdot,\cdot) : F^*/F^{*m} \times F^*/F^{*m} \longrightarrow \mu_m.$$

We will often call the pairing in Theorem 3.70 'norm-residue symbol'.

Theorem 3.71. *Let m be a positive integer and let F be a local field containing a primitive m-th root of unity. Then*

$$[F^* : F^{*m}] = m[U_F : U_F^m] = m^2|m|^{-1} < \infty.$$

Proof. The first equality follows from the exact and split sequence of Theorem 3.37. If the characteristic of F is 0, then Theorem 3.38 gives

$$[U_F : U_F^m] = m|(\mathbb{Z}_p/m\mathbb{Z}_p)|^d = mp^{d\,\mathrm{v}_p(m)},$$

where p is the characteristic of the residue field of F and $d = [F : \mathbb{Q}_p]$. Using Theorem 3.22 we get

$$|m|^{-1} = |\,\mathrm{N}_{F/\mathbb{Q}_p}\, m|^{-1} = |m^d|^{-1} = p^{d\,\mathrm{v}_p(m)}.$$

Hence, we obtain the equality

$$[U_F : U_F^m] = m|m|^{-1}.$$

If the characteristic of F is a prime p, then we have $(m,p) = 1$. Hence, we obtain $|m| = 1$ and $m\mathbb{Z}_p = \mathbb{Z}_p$. The equality

$$[U_F : U_F^m] = m|m|^{-1}$$

follows from Theorem 3.39. □

Lemma 3.72. *Let m be a positive integer, let F be a local field containing a primitive m-th root of unity, and let a and b be elements in F^*. Then one has $(a,b) = 1$ if and only if a is a norm for the extension $F(\beta)/F$, where $\beta^m = b$ with β in an algebraic closure of F.*

Proof. By definition of norm-residue symbol we have

$$(a, b) = \psi_F(a)(\beta)/\beta.$$

Since β is a generator of the extension $F(\beta)/F$, the automorphism $\psi_F(a)$ acts trivially on $F(\beta)$ if and only if we have $(a, b) = 1$. By Theorem 3.59 this is the case if and only if a is in $\mathrm{N}_{F(\beta)/F} F(\beta)^*$. □

Lemma 3.73. *Let m be a positive integer, let K be a field containing a primitive m-th root of unity, and let $a \in K^*$. Then for every $x \in K$ the element $x^m - a$ is a norm from $K(\sqrt[m]{a})$.*

Proof. See Exercise 2.5 in [9] by Cassels and Fröhlich. □

We note that the norm-residue symbol necessarily satisfies the following three relations. We will very often use them.

Theorem 3.74. *Let m be a positive integer, let F be a local field containing a primitive m-th root of unity, let μ_m be the group of m-th roots of unity in F, and let $(\cdot, \cdot) : F^* \times F^* \to \mu_m$ be the norm-residue symbol. Then for all $a, b \in F^*$, $c \in F^* \setminus \{1\}$ the norm-residue symbol satisfies the equalities*

$$(-a, a) = 1 \quad \textit{and} \quad (1 - c, c) = 1$$

and the antisymmetric relation

$$(a, b)(b, a) = 1.$$

Proof. Lemma 3.73 implies that for all $a \in F^*$, $c \in F^* \setminus \{1\}$ the elements $-a$ and $1 - c$ are nonzero norms for $F(\sqrt[m]{a})/F$ and for $F(\sqrt[m]{c})/F$, respectively. By Lemma 3.72 we get the equalities $(-a, a) = 1$ and $(1 - c, c) = 1$. Now the antisymmetric relation follows easily from bilinearity and the first equality:

$$1 = (-ab, ab) = (-a, a)(b, a)(a, b)(-b, b) = (a, b)(b, a).$$ □

Corollary 3.75. *Let m be a positive integer, let F be a local field containing a primitive m-th root of unity, let μ_m be the group of m-th roots of unity in F, and let $(\cdot, \cdot) : F^* \times F^* \to \mu_m$ be the norm-residue symbol. Then for all $a \in F^*$ one has*

$$(-1, a) = (a, a)\,.$$

Proof. For all $a \in F^*$ we get

$$(-1, a) = (-1, a)\,(-a, a) = (a, a)\,,$$

because by Theorem 3.74 we have $(-a, a) = 1$ for all $a \in F^*$. □

Theorem 3.76. *Let m be a positive integer, let n be a positive divisor of m, let F be a local field containing a primitive m-th root of unity, let μ_m and μ_n be the groups of m-th roots of unity in F and of n-th roots of unity in F, respectively, let $(\cdot,\cdot)_{F,m} : F^* \times F^* \to \mu_m$ be the m-th power norm-residue symbol, and let $(\cdot,\cdot)_{F,n} : F^* \times F^* \to \mu_n$ be the n-th power norm-residue symbol. Then one has*

$$(\cdot,\cdot)_{F,n} = (\cdot,\cdot)_{F,m}^{m/n}.$$

Proof. This follows immediately from Definition 3.67. □

Remark 3.77. We will often assume that m is a prime power. In fact, if one has $m = m_1 m_2$ with m_1 and m_2 coprime positive integers, then by Theorem 3.76 and the Chinese remainder theorem the pairing

$$(\cdot,\cdot)_{F,m} : F^* \times F^* \to \mu_m$$

is uniquely determined by the two pairings

$$(\cdot,\cdot)_{F,m_1} : F^* \times F^* \to \mu_{m_1} \quad \text{and} \quad (\cdot,\cdot)_{F,m_2} : F^* \times F^* \to \mu_{m_2}.$$

3.6 A new elementary characterization

In this section we show that the norm-residue symbol can be characterized in an elementary way. The formulation of Theorem 3.80 does not use local class field theory.

Definition 3.78 (Second K-group)**.** Let F be a field. The *second K-group* of F is the group

$$K_2F = (F^* \otimes_{\mathbb{Z}} F^*)/\langle a \otimes b : a + b = 1\rangle.$$

The following theorem about the structure of K_2F is very important from both a theoretical and a computational point of view. The proof of this theorem, as found in [48] by Milnor, was used in [13] by Daberkow to give an algorithm for computing the norm-residue symbol.

Theorem 3.79 (Moore)**.** *Let F be a non-Archimedean local field and let n be the number of roots of unity in F. Then the group K_2F is the direct sum of a cyclic group of order n and a divisible group $(K_2F)^n$.*

Proof. See Theorem A.14 of Appendix in [48] by Milnor. □

In [48] by Milnor elementary arguments show that the group $K_2F/(K_2F)^n$ is cyclic. Local class field theory, in particular the existence of the norm-residue symbol, is used to prove that $K_2F/(K_2F)^n$ is of order n.

Theorem 3.80 (Elementary characterization of the norm-residue symbol)**.** *Let m be a positive integer, let F be a local field containing a primitive m-th root of unity, and let μ_m be the group of m-th roots of unity in F. Then the m-th power norm-residue symbol is the unique pairing*

$$(\cdot,\cdot) : F^* \times F^* \to \mu_m$$

with the following properties.

(a) *If a and b are elements in F^* satisfying the equality $a+b=1$, then one has $(a,b)=1$.*

(b) *If F is non-Archimedean, the elements a and b are in F^*, and the extension $F(\beta)/F$ is unramified, where $\beta^m = b$ with β in an algebraic closure of F, then one has*

$$(a,b) = \mathrm{Fr}^{\mathrm{v}_F(a)}(\beta)/\beta,$$

where Fr *is the Frobenius element in* $\mathrm{Gal}(F(\beta)/F)$ *and* $\mathrm{v}_F : F \to \mathbb{Z} \cup \{+\infty\}$ *is the normalized valuation on F.*

(c) *If F is isomorphic to $\mathbb{R}$, then the map $(\cdot,\cdot)$ is surjective.*

Proof. Firstly, by Theorem 3.69 the norm-residue symbol is a pairing

$$(\cdot,\cdot) : F^* \times F^* \to \mu_m.$$

Secondly, we have to prove that the norm-residue symbol satisfies the three conditions. By Theorem 3.74 we immediately see that the first condition is satisfied. The second and the third properties follow from the explicit expression of the norm-residue maps in these particular cases. In fact, if F is non-Archimedean, the elements a and b are in F^*, and the extension $F(\beta)/F$ is unramified, where $\beta^m = b$ with β in an algebraic closure of F, Property (c) in Theorem 3.57 gives

$$\psi_{F(\beta)/F}(a) = \mathrm{Fr}^{\mathrm{v}_F(a)}$$

and by definition of the norm-residue symbol we get

$$(a,b) = \mathrm{Fr}^{\mathrm{v}_F(a)}(\beta)/\beta.$$

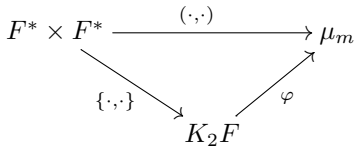
Now we consider the case when F is isomorphic to $\mathbb{R}$. The integer m is equal either to 1 or to 2. If m is 1, then the map $(\cdot,\cdot)$ is trivially surjective. If m is equal to 2, the surjectivity of the norm-residue map $\psi_{\mathbb{R}} : \mathbb{R}^* \to \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ implies

$$(-1,-1) = \psi_{\mathbb{R}}(-1)(\mathrm{i})/\mathrm{i} = -\mathrm{i}/\mathrm{i} = -1,$$

where $\mathrm{i}^2 = -1$ with $\mathrm{i} \in \mathbb{C}$. This proves that the norm-residue symbol is surjective.

Finally, we need to prove the uniqueness of this map. Suppose that F is a non-Archimedean local field. By Definition 3.78 it follows that for any pairing

$(\cdot,\cdot) : F^* \times F^* \to \mu_m$ with the first property there exists one and only one homomorphism $\varphi : K_2F \to \mu_m$ that carries for all $a, b \in F^*$ the image $\{a, b\}$ of (a, b) in K_2F to the norm-residue symbol (a, b). This means that the diagram



commutes. Theorem 3.79 implies that $K_2F/(K_2F)^m$ is a cyclic group of order m. The homomorphism φ has to be trivial on $(K_2F)^m$ and therefore there are only m such homomorphisms.

By Theorem 3.56 the Galois group of an unramified extension of non-Archimedean local field is cyclic and generated by the Frobenius element. If we choose $a, b \in F^*$ such that $\mathrm{v}_F(a) = 1$ and the extension $F(\beta)/F$ is unramified of degree m, where $\beta^m = b$ with β in an algebraic closure of F, then the norm-residue symbol (a, b) is a primitive m-th root of unity. To see that such a b exists, we can consider the unramified extension generated by adjoining to F a root of a polynomial of degree m with coefficients in F that is irreducible over the residue field of F. By Theorem 3.44 of Kummer theory this extension is of the form $F(\beta)/F$, where $\beta^m \in F$ with β in an algebraic closure of F. Hence $\{a, b\}$ generates $K_2F/(K_2F)^m$ and Property (b) fixes the homomorphism φ. The case when F is Archimedean is in the following section. □

3.7 Archimedean local fields

Let F be an Archimedean local field. By Theorem 3.16 the field F is isomorphic either to $\mathbb{C}$ or to $\mathbb{R}$. We will prove that the norm-residue symbol is the unique pairing

$$(\cdot,\cdot) : F^* \times F^* \to \mu_m$$

having the properties of Theorem 3.80.

Since every element of $\mathbb{C}$ is an m-th power, the norm-residue symbol is the trivial map if we have $F \cong \mathbb{C}$. Now suppose $F \cong \mathbb{R}$. Since there are only two roots of unity in $\mathbb{R}$, namely the elements 1 and -1, we have only two possible values for m: either $m = 1$ or $m = 2$. For $m = 1$ the first power norm-residue symbol is again the trivial map, because its image is the trivial group. For $m = 2$ we have a pairing

$$(\cdot,\cdot) : \mathbb{R}^*/\mathbb{R}_{>0} \times \mathbb{R}^*/\mathbb{R}_{>0} \longrightarrow \langle -1 \rangle.$$

Since by Property (c) in Theorem 3.80 this map is surjective and $\mathbb{R}^* \otimes \mathbb{R}^*$

modulo squares has order 2, for all $a, b \in \mathbb{R}^*$ we get

$$(a,b) = \begin{cases} -1 & \text{if } a < 0 \text{ and } b < 0, \\ 1 & \text{otherwise.} \end{cases}$$

Theorem 3.81. *The triple $(\mathbb{R}^*/\mathbb{R}_{>0}, \langle -1 \rangle, (\cdot,\cdot))$ is a skew abelian group of order 2 and its skew element is $-1 \cdot \mathbb{R}_{>0}$.*

Proof. The result follows from the explicit description of the norm-residue symbol for Archimedean local fields in Section 3.7. □

3.8 Non-Archimedean local fields

Theorem 3.82. *Let m be a positive integer, let F be a non-Archimedean local field containing a primitive m-th root of unity, let μ_m be the group of m-th roots of unity in F, and let $(\cdot,\cdot)_{F,m} : F^*/F^{*m} \times F^*/F^{*m} \to \mu_m$ be the pairing induced by the m-th power norm-residue symbol. Then the triple $(F^*/F^{*m}, \mu_m, (\cdot,\cdot)_{F,m})$ is a skew abelian group with the following properties.*

(a) *Its skew element is $-1 \cdot F^{*m}$.*

(b) *It is a symplectic abelian group if and only if one has $-1 \in F^{*m}$.*

(c) *If the characteristic of F is positive, then one has a group isomorphism*

$$F^*/F^{*m} \cong (\mathbb{Z}/m\mathbb{Z})^2.$$

(d) *If the characteristic of F is 0, then one has a group isomorphism*

$$F^*/F^{*m} \cong (\mathbb{Z}/m_p\mathbb{Z})^2 \oplus (\mathbb{Z}/p^{\mathrm{v}_p(m)}\mathbb{Z})^{d+2},$$

where p is the characteristic of the residue field of F, $m_p = m/p^{\mathrm{v}_p(m)}$, and $d = [F : \mathbb{Q}_p]$.

(e) *Its 2-rank is 0 if one has $m \not\equiv 0 \bmod 2$.*

(f) *Its 2-rank is 2 if one has $m \equiv 0 \bmod 2$ and the characteristic of the residue field of F is odd.*

(g) *Its 2-rank is $[F : \mathbb{Q}_2] + 2$ if one has $m \equiv 0 \bmod 2$, the characteristic of F is 0, and the characteristic of the residue field of F is 2.*

Proof. Since the norm-residue symbol is an antisymmetric pairing, by Theorem 3.70 the triple $(F^*/F^{*m}, \mu_m, (\cdot,\cdot)_{F,m})$ is a skew abelian group.

(a) This follows from Corollary 3.75.

(b) This follows from (a) and Theorem 2.15.

(c) This follows from Theorem 3.37 and Theorem 3.39.

(d) This follows from 3.37 and Theorem 3.38.

The statements about the 2-rank follow from the isomorphisms in (c) and (d). □

Definition 3.83 (Conductor)**.** Let F/E be an abelian extension of non-Archimedean local fields, let $n \in \mathbb{Z}_{\geq 0}$ be the smallest integer such that $U_E^{(n)} \subseteq \mathrm{N}_{F/E}\, F^*$, where $U_E^{(n)}$ is the n-th higher unit group of E, and let $\mathfrak{P}_E$ be the maximal ideal of the ring of integers of E. The *conductor* $\mathfrak{f}$ of F/E is the ideal

$$\mathfrak{f} = \mathfrak{P}_E^n.$$

Theorem 3.84. *Let F/E be an unramified extension of non-Archimedean local fields and for each $n \in \mathbb{Z}_{\geq 0}$ let $U_E^{(n)}$ and $U_F^{(n)}$ be the n-th higher unit groups of the rings of integers of E and of F, respectively. Then for each $n \in \mathbb{Z}_{\geq 0}$ one has*

$$\mathrm{N}_{F/E}\, U_F^{(n)} = U_E^{(n)}.$$

Proof. See Corollary 1.4 of Chapter III in [50] by Neukirch. □

Theorem 3.85. *An abelian extension F/E of non-Archimedean local fields is unramified if and only if its conductor $\mathfrak{f}$ is equal to $1 = \mathfrak{P}_E^0$, where $\mathfrak{P}_E$ is the maximal ideal of the ring of integers of E.*

Proof. See Proposition 3.4 of Chapter III in [50] by Neukirch. □

Theorem 3.86. *Let m be a positive integer, let F be a non-Archimedean local field containing a primitive m-th root of unity, let U_F be the group of units of the ring of integers of F, and let $b \in F^*$. Then the following are equivalent.*

(i) *The extension $F(\beta)/F$ is unramified, where $\beta^m = b$ with β in an algebraic extension of F.*

(ii) *For all $a \in U_F$ one has $(a, b) = 1$.*

Proof. (i) $\Longrightarrow$ (ii) If $F(\beta)/F$ is unramified, then by (b) in Theorem 3.80 for all $a \in U_F$ we have

$$(a, b) = \mathrm{Fr}^{\mathrm{v}_F(a)}(\beta)/\beta = \mathrm{Fr}^0(\beta)/\beta = 1.$$

(i) $\Longrightarrow$ (ii) Now suppose $(a, b) = 1$ for all $a \in U_F$. From Lemma 3.72 we obtain that a is contained in $\mathrm{N}_{F(\beta)/F}\, F(\beta)^*$. Hence, we have

$$U_F \subseteq \mathrm{N}_{F(\beta)/F}\, F(\beta)^*,$$

that is, the conductor of the extension $F(\beta)/F$ is 1. By Theorem 3.85 the extension $F(\beta)/F$ is unramified. □

Lemma 3.87. *Let m be a positive integer, let F be a non-Archimedean local field, and let $a \in F^*$. If the extension $F(\alpha)/F$ is unramified, where $\alpha^m = a$ with α in an algebraic extension of F, then one has*

$$\mathrm{v}_F(a) \equiv 0 \bmod m,$$

where $\mathrm{v}_F : F \to \mathbb{Z} \cup \{+\infty\}$ is the normalized valuation on F.

Proof. Suppose that the extension $F(\alpha)/F$ is unramified. By Theorem 3.53 the normalized valuation $\mathrm{v}_{F(\alpha)}$ on $F(\alpha)$ restricted to F equals the normalized valuation v_F on F. From the equality $\alpha^m = a$, we get

$$\mathrm{v}_F(a) = \mathrm{v}_{F(\alpha)}(a) = \mathrm{v}_{F(\alpha)}(\alpha^m) = m\,\mathrm{v}_{F(\alpha)}(\alpha) \equiv 0 \bmod m.$$

This concludes the proof. □

Remark 3.88. Let m be a positive integer, let F be a non-Archimedean local field, and let U_F be the group of units of the ring of integers of F. Since we have $U_F^m = F^{*m} \cap U_F$, the second isomorphism theorem for groups gives the isomorphism $U_F F^{*m}/F^{*m} \cong U_F/U_F^m$. Hence, we may consider U_F/U_F^m as a subgroup of F^*/F^{*m}.

Theorem 3.89. *Let m be a positive integer, let F be a non-Archimedean local field containing a primitive m-th root of unity, and let μ_m be the group of m-th roots of unity in F. Let U_F be the group of units of the ring of integers of F and let $(U_F/U_F^m)^\perp$ be the annihilator in F^*/F^{*m} of U_F/U_F^m with respect to pairing*

$$(\cdot,\cdot) : F^*/F^{*m} \times F^*/F^{*m} \longrightarrow \mu_m$$

induced by the norm-residue symbol. Then the group $(U_F/U_F^m)^\perp$ is cyclic of order m and is a subgroup of U_F/U_F^m of index $|m|^{-1}$, where $|\cdot| : F \to \mathbb{R}_{\geq 0}$ is the normalized absolute value on F.

Proof. Theorem 3.86 states that any m-th root of an element $a \in F^*$ that is mapped into $(U_F/U_F^m)^\perp$ by the projection $F^* \to F^*/F^{*m}$ generates an unramified extension of F. By Lemma 3.87 we have $\mathrm{v}_F(a) \equiv 0 \mod m$, that is, the element a is mapped into U_F/U_F^m. Therefore, we obtain the inclusion $(U_F/U_F^m)^\perp \subseteq U_F/U_F^m$.

Theorem 3.37 implies that U_F/U_F^m is an index m subgroup of F^*/F^{*m} and the quotient group $(F^*/F^{*m})/(U_F/U_F^m)$ is cyclic of order m. Since the induced pairing is a perfect, the group $(U_F/U_F^m)^\perp$ is cyclic of order m. By Theorem 3.71 the group $(U_F/U_F^m)^\perp$ is an index $|m|^{-1}$ subgroup of U_F/U_F^m. □

Corollary 3.90. *Let $U_F^\perp$ be the annihilator in U_F of U_F with respect to the norm-residue symbol. Then one has the equality $(U_F/U_F^m)^\perp = U_F^\perp/U_F^m$ and the norm-residue symbol induces a perfect pairing*

$$(\cdot,\cdot) : U_F/U_F^\perp \times U_F/U_F^\perp \to \mu_m.$$

Proof. Since we have $U_F^m = F^{*m} \cap U_F^\perp$, we may also consider $U_F^\perp/U_F^m$ as a subgroup of F^*/F^{*m}. From the inclusion $(U_F/U_F^m)^\perp \subseteq U_F/U_F^m$ of Theorem 3.89 we obtain the equality $(U_F/U_F^m)^\perp = U_F^\perp/U_F^m$. Taking the quotient $(U_F/U_F^m)/(U_F/U_F^m)^\perp$ we get the induced perfect pairing. □

The present situation is summarized in the following diagram.

$$\begin{array}{c} F^*/F^{*m} \\ \Big| m \\ U_F/U_F^m \\ \Big| |m|^{-1} \\ (U_F/U_F^m)^\perp = U_F^\perp/U_F^m \\ \Big| m \\ 1 \end{array}$$

Corollary 3.91. *Let $U_F^\perp$ be the annihilator in U_F of U_F with respect to the norm-residue symbol. Then one has the following.*

(a) *There is a group isomorphism $U_F^\perp/U_F^m \cong \mathbb{Z}/m\mathbb{Z}$.*

(b) *If the characteristic of F is positive, then the group $U_F/U_F^\perp$ is trivial.*

(c) *If the characteristic of F is 0, then one has a group isomorphism*

$$U_F/U_F^\perp \cong (\mathbb{Z}/p^{\mathrm{v}_p(m)}\mathbb{Z})^d,$$

where p is the characteristic of the residue field of F and $d = [F : \mathbb{Q}_p]$.

Proof. (a) By Theorem 3.37 we get $F^*/(U_F F^{*m}) \cong \mathbb{Z}/m\mathbb{Z}$. Since the finite group $(U_F/U_F^m)^\perp$ is the dual of $F^*/(U_F F^{*m})$ with respect to a perfect pairing, by Theorem 2.17 we have $(U_F/U_F^m)^\perp \cong F^*/(U_F F^{*m})$. From the equality $(U_F/U_F^m)^\perp = U_F^\perp/U_F^m$ of Corollary 3.90 we obtain an isomorphism

$$U_F^\perp/U_F^m \cong \mathbb{Z}/m\mathbb{Z}.$$

(b) If the characteristic of F is positive, then we have $|m| = 1$, where $|\cdot| : F \to \mathbb{R}_{\geq 0}$ is the normalized absolute value on F. The result follows from Theorem 3.89 and Corollary 3.90.

(c) Suppose that the characteristic of F is 0. Theorem 3.38 gives an isomorphism

$$U_F/U_F^m \cong \mathbb{Z}/m\mathbb{Z} \oplus (\mathbb{Z}/p^{\mathrm{v}_p(m)}\mathbb{Z})^d.$$

Since $U_F^\perp/U_F^m$ is a cyclic subgroup of U_F/U_F^m of maximal order, the exact sequence

$$1 \to U_F^\perp/U_F^m \to U_F/U_F^m \to U_F/U_F^\perp \to 1$$

splits. An isomorphism

$$U_F/U_F^\perp \cong (\mathbb{Z}/p^{\mathrm{v}_p(m)}\mathbb{Z})^d$$

follows from the splitting of the exact sequence. □

Corollary 3.92. *Let m be a positive integer, let F be a non-Archimedean local field containing a primitive m-th root of unity, let μ_m be the group of m-th roots of unity in F, let p be the characteristic of the residue field of F, let U_F be the group of units of the ring of integers of F, and let $U_F^{\perp}$ be the annihilator in U_F of U_F with respect to the norm-residue symbol $(\cdot,\cdot)_{F,m} : F^* \times F^* \to \mu_m$. Then the triple $(U_F/U_F^{\perp}, \mu_m, (\cdot,\cdot)_{F,m})$ is a skew abelian group with the following properties.*

(a) *Its skew element is $-1 \cdot U_F^{\perp}$.*

(b) *It is a symplectic abelian group if and only if the extension $F(\sqrt[m]{-1})/F$ is unramified.*

(c) *It is the trivial group if and only if the characteristic of F is positive or one has $m \not\equiv 0 \bmod p$.*

(d) *Its 2-rank equals 0 if $p \neq 2$.*

(e) *Its 2-rank equals $[F : \mathbb{Q}_p]$ if $p = 2$, the characteristic of F is 0, and $m \equiv 0 \bmod 2$.*

Proof. Since the norm-residue symbol is an antisymmetric pairing, Corollary 3.90 implies that the triple $(U_F/U_F^{\perp}, \mu_m, (\cdot,\cdot)_{F,m})$ is a skew abelian group. Corollary 3.75 gives (a). Now Theorem 2.15 and Theorem 3.86 imply (b). By Theorem 3.89 and Corollary 3.90 the cardinality of $U_F/U_F^{\perp}$ equals $|m|^{-1}$, where $|\cdot| : F \to \mathbb{R}_{\geq 0}$ is the normalized absolute value on F. Hence (c) and (d) follow. Corollary 3.91 gives (e). □

Corollary 3.93. *Let m be a positive integer, let F be a non-Archimedean local field of characteristic zero containing a primitive m-th root of unity, let p the characteristic of the residue field of F, let U_F be the group of units of the ring of integers of F, and let $n = p^{\mathrm{v}_p(m)}$. Let $U_{F,m}^{\perp}$ and $U_{F,n}^{\perp}$ be the annihilators in U_F of U_F with respect to the m-th power norm-residue symbol and to the n-th power norm-residue symbol, respectively. Then one has the equality $U_{F,m}^{\perp} = U_{F,n}^{\perp}$ and the pair (φ, ψ) of group isomorphisms*

$$\begin{aligned} \varphi : U_F/U_{F,m}^{\perp} &\to U_F/U_{F,n}^{\perp}, & \psi : \mu_m^{m/n} &\to \mu_n, \\ a \cdot U_{F,m}^{\perp} &\mapsto a \cdot U_{F,n}^{\perp}, & \zeta &\mapsto \zeta^{m/n}, \end{aligned}$$

is a similarity of skew abelian groups from $(U_F/U_{F,m}^{\perp}, \mu_m, (\cdot,\cdot)_{F,m})$ to $(U_F/U_{F,n}^{\perp}, \mu_n, (\cdot,\cdot)_{F,n})$, where μ_m and μ_n are the groups of m-th roots of unity in F and of n-th roots of unity in F, respectively.

Proof. By Theorem 3.76 we have the inclusion $U_{F,m}^{\perp} \subseteq U_{F,n}^{\perp}$. Hence, there is a natural projection $\varphi : U_F/U_{F,m}^{\perp} \to U_F/U_{F,n}^{\perp}$. Since it is a surjective group homomorphism and by Corollary 3.91 is a map between two group of the same cardinality, it is a group isomorphism. This proves the equality $U_{F,m}^{\perp} = U_{F,n}^{\perp}$.

Let χ be the group homomorphism $\chi : \mu_m \to \mu_n$, $\zeta \mapsto \zeta^{m/n}$. By Theorem 3.76 the diagram

$$\begin{array}{ccc} U_F/U_{F,m}^{\perp} \times U_F/U_{F,m}^{\perp} & \xrightarrow{(\cdot,\cdot)_{F,m}} & \mu_m \\ \varphi \downarrow \quad \varphi \downarrow & & \chi \downarrow \\ U_F/U_{F,n}^{\perp} \times U_F/U_{F,n}^{\perp} & \xrightarrow{(\cdot,\cdot)_{F,n}} & \mu_n \end{array}$$

commutes. Since by Corollary 3.91 the group $U_F/U_{F,m}^{\perp}$ is a p-group, the image of $(\cdot,\cdot)_{F,m}$ is contained in μ_n. It equals $\mu_m^{m/n}$, because by Corollary 3.90 the pairing $(\cdot,\cdot)_{F,m} : U_F/U_{F,m}^{\perp} \times U_F/U_{F,m}^{\perp} \to \mu_m$ is perfect and by Corollary 3.91 the group $U_F/U_{F,m}^{\perp}$ contains an element of order n. Hence $\psi = \chi|_{\mu_m^{m/n}}$ is a group isomorphism between the images of $(\cdot,\cdot)_{F,m}$ and $(\cdot,\cdot)_{F,n}$. We conclude that the pair (φ, ψ) is a similarity of skew abelian groups. □

Theorem 3.94. *Let F be a non-Archimedean local field with residue field $\mathbb{F}$ and let $f(X)$ be a monic polynomial over the ring of integers of F whose residue class in $\mathbb{F}[X]$ is a monic separable polynomial over $\mathbb{F}$. Let α be a root of $f(X)$ in an algebraic closure of F. Then the extension $F(\alpha)/F$ is unramified.*

Proof. See (ii) of Proposition 1 in Section 7 of Chapter I in [9] by Cassels and Fröhlich or Proposition 3.2 of Chapter II in [15] by Fesenko and Vostokov. □

Theorem 3.95. *Let p be a prime number, let ζ_p be a primitive p-th root of unity, and let F be a finite extension of $\mathbb{Q}_p(\zeta_p)$. Let $\mathfrak{P}$ be the maximal ideal of the ring of integers $\mathcal{O}_F$ of F and let $\lambda = 1 - \zeta_p$. Let $a \in F^*$ and let α be an element in an algebraic closure of F with $\alpha^p = a$. Then one has the following.*

(a) *The extension $F(\alpha)/F$ is unramified if and only if $a \in (1+\lambda^p\mathcal{O}_F) \cdot F^{*p}$.*

(b) *The extension $F(\alpha)/F$ is unramified of degree p if and only if there exists $c \in \mathcal{O}_F$ such that $\mathrm{Tr}_{(\mathcal{O}_F/\mathfrak{P})/(\mathbb{Z}/p\mathbb{Z})}\, \overline{c} \neq 0$ and $a \in (1 + c\lambda^p) \cdot F^{*p}$, where $\overline{c}$ is the reduction modulo $\mathfrak{P}$ of c and $\mathrm{Tr}_{(\mathcal{O}_F/\mathfrak{P})/(\mathbb{Z}/p\mathbb{Z})}$ is the trace map from $\mathcal{O}_F/\mathfrak{P}$ to $\mathbb{Z}/p\mathbb{Z}$.*

To prove Theorem 3.95 we will use Lemma 3.96. For a different proof of the lemma see [66] and Exercise 9.4 in [74].

Lemma 3.96. *One has*

$$\frac{\lambda^{p-1}}{p} \equiv -1 \bmod \lambda\mathcal{O}_F.$$

Proof. The case $p = 2$ is trivial. Setting X equal to λ in the equality

$$\sum_{i=0}^{p-1}(1-X)^i = \frac{(1-X)^p - 1}{-X} = (-X)^{p-1} + pXf + p,$$

where f a polynomial in X with integer coefficients, we get

$$0 = \sum_{i=0}^{p-1} \zeta_p^i \equiv (-\lambda)^{p-1} + p \bmod p\lambda\mathcal{O}_F.$$

Since we have $(-\lambda)^{p-1} = \lambda^{p-1}$ if p is odd, dividing by p gives us the desired result. □

Proof (of Theorem 3.95*).* Let $b \in \mathcal{O}_F$ with $b \equiv 1 \bmod \lambda^p\mathcal{O}_F$. We can write $b = 1 + \lambda^p c$ with $c \in \mathcal{O}_F$. Let $x = (\beta - 1)/\lambda$, where β is in an algebraic closure of F and $\beta^p = b$. From the identity

$$(1 + \lambda x)^p = b$$

we obtain

$$x^p + \left(\sum_{i=1}^{p-1} \binom{p}{i} \frac{(\lambda x)^i}{\lambda^p} \right) + \frac{1-b}{\lambda^p} = 0.$$

Let $f(X)$ be the polynomial

$$f(X) = X^p + \left(\sum_{i=2}^{p-1} \binom{p}{i} \frac{(\lambda X)^i}{\lambda^p} \right) + \frac{\lambda p X}{\lambda^p} - c$$

in $F[X]$. All coefficients of the terms of degree d with $2 \le d \le p-1$ are in $\mathfrak{P}$. By Lemma 3.96 we know $\frac{\lambda^{p-1}}{p} \equiv -1 \bmod \lambda\mathcal{O}_F$. Hence x is a root of a polynomial $f(X) \in \mathcal{O}_F[X]$ such that $f(X) \equiv X^p - X - \overline{c} \bmod \mathfrak{P}$, where $\overline{c}$ is the reduction modulo $\mathfrak{P}$ of c. Since we have $f'(X) \equiv -1 \bmod \mathfrak{P}$, by Theorem 3.94 the extension $F(x)/F = F(\beta)/F$ is unramified. This proves that if we have $a \in (1 + \lambda^p\mathcal{O}_F) \cdot F^{*p}$ then the extension $F(\alpha)/F$ is unramified.

The Artin–Schreier polynomial $X^p - X - \overline{c} \in (\mathcal{O}_F/\mathfrak{P})[X]$ splits into linear factors, which is equivalent by Hensel's lemma to the extension $F(\beta)/F$ being trivial, if and only if we have $\mathrm{Tr}_{(\mathcal{O}_F/\mathfrak{P})/(\mathbb{Z}/p\mathbb{Z})}\, \overline{c} = 0$. Otherwise, it is irreducible and the extension $F(\beta)/F$ has degree p. This proves the if part of (b).

Now assume $\mathrm{Tr}_{(\mathcal{O}_F/\mathfrak{P})/(\mathbb{Z}/p\mathbb{Z})}\, \overline{c} \neq 0$. The uniqueness of unramified extensions of given degree and Kummer theory imply that the extension $F(\alpha)/F$ is unramified if and only if we have $a \in \langle b \rangle \cdot F^{*p}$. Since for every $n \in \mathbb{Z}$ we have $b^n \equiv 1 \bmod \lambda^p\mathcal{O}_F$, we get (a). Moreover, the extension $F(\alpha)/F$ is unramified of degree p if and only if we have $a \in b^n \cdot F^{*p}$ with $n \in \mathbb{Z} \setminus p\mathbb{Z}$. Since for every $n \in \mathbb{Z} \setminus p\mathbb{Z}$ we have $b^n \equiv 1 + \lambda^p nc \bmod \lambda^{p+1}\mathcal{O}_F$ and $\mathrm{Tr}_{(\mathcal{O}_F/\mathfrak{P})/(\mathbb{Z}/p\mathbb{Z})}\, \overline{nc} \neq 0$, we get (b). □

Lemma 3.97. *Let p be a prime number, let ζ_p be a primitive p-th root of unity, let F be a finite extension of $\mathbb{Q}_p(\zeta_p)$, let e be the normalized valuation $\mathrm{v}_F(p)$,*

let $e_0 = e/(p-1)$, and for each $n \in \mathbb{Z}_{>0}$ let $U^{(n)}$ be the n-th higher unit group of the ring of integers of F. Then for each integer $i > e_0$ the p-th power group homomorphism $F^* \to F^*$, $a \mapsto a^p$, induces an isomorphism $U^{(i)} \xrightarrow{\sim} U^{(i+e)}$.

Proof. See Lemma A.4 of Appendix in [48] by Milnor. □

Lemma 3.98. *Let p be a prime, let n be a positive integer, and let $m = p^n$. Let ζ_p and ζ_m be a primitive p-th root of unity and a primitive m-th root of unity, respectively. Let F be a finite extension of $\mathbb{Q}_p(\zeta_m)$, let $\mathcal{O}_F$ be the ring of integers of F, and let $\lambda = 1 - \zeta_p$. Let $a \in F$ with $a \equiv 1 \bmod p^n\lambda\mathcal{O}_F$ and let α be an element in an algebraic closure of F with $\alpha^{p^n} = a$. Then the extension $F(\alpha)/F$ is unramified of degree dividing p.*

Proof. By Lemma 3.97 the p^{n-1}-th power group homomorphism $F^* \to F^*$, $x \mapsto x^{p^{n-1}}$, induces an isomorphism $U^{(e_0+e)} \xrightarrow{\sim} U^{(e_0+ne)}$, where $e = \mathrm{v}_F(p)$ and $e_0 = e/(p-1) = \mathrm{v}_F(\lambda)$. We choose $\beta \in \alpha \cdot \langle\zeta_m\rangle$ with $\beta^p \in F^*$ and $\beta^p \equiv 1 \bmod p\lambda\mathcal{O}_K$. It exists, because we have $\mathrm{v}_F(a-1) \geq e_0 + ne$. The equality $F(\alpha) = F(\beta)$ shows that it is sufficient to prove that the extension $F(\beta)/F$ is unramified of degree dividing p. Theorem 3.95 implies that the extension $F(\beta)/F$ is unramified. It is of degree dividing p, because we have $\beta^p \in F^*$ and $\zeta_p \in F$. □

Lemma 3.99 (Bouw [7])**.** *Let p be a prime, let n be a positive integer, and let $m = p^n$. Let ζ_p and ζ_m be a primitive p-th root of unity and a primitive m-th root of unity, respectively, and let $\lambda = 1 - \zeta_p$. Let F be a finite extension of $\mathbb{Q}_p(\zeta_m)$, let $\mathrm{v}_F : F \to \mathbb{Z} \cup \{+\infty\}$ be the normalized valuation on F, and let E/F be an unramified extension of non-Archimedean local fields of degree m. Then there exists $\alpha \in E^*$ such that $\alpha^m \in F^*$, $E = F(\alpha)$, and $\mathrm{v}_F(\alpha^m - 1) = \mathrm{v}_F(p\lambda)$.*

Proof. Let $K/\mathbb{Q}_p$ be the maximal unramified extension of $\mathbb{Q}_p$ that is contained in F and let $L = K(\zeta_m)$. Let M/L be the maximal unramified extension of L that is contained in E. Since the extension E/F is unramified of degree m and F/E is totally ramified, the extension M/L is unramified of degree m. By Kummer theory there is $\alpha \in M$ such that $\alpha^m \in L^*$ and $M = L(\alpha)$. Moreover, we have $E = F(\alpha)$. By Lemma 3.87 we can assume $\mathrm{v}_M(\alpha) = 0$. Since every root of unity of order coprime to p is an m-th power, we can assume $\mathrm{v}_M(\alpha - 1) \geq 1$. By Theorem 3.53 the normalized valuation v_M on M restricted to L equals the normalized valuation v_L on L. Since we have $\alpha^m - 1 = \prod_{i=0}^{m-1}(\alpha\zeta_m^i - 1)$ and $\mathrm{v}(\zeta_m - 1) \geq 1$, we get

$$\mathrm{v}_L(\alpha^m - 1) = \mathrm{v}_M(\alpha^m - 1) = \sum_{i=0}^{m-1} \mathrm{v}_M(\alpha\zeta_m^i - 1) \geq m.$$

Since we have $\alpha^m \notin L^{*p}$, Theorem 3.95 gives $\mathrm{v}_L(\alpha^m - 1) \leq \mathrm{v}_L(\lambda^p)$. We obtain

$$\mathrm{v}_L(\alpha^m - 1) \leq \mathrm{v}_L(\lambda^p) = m\,\mathrm{v}_L(1 - \zeta_m) = m,$$

because the extension $L/\mathbb{Q}_p(\zeta_m)$ is unramified and $1-\zeta_m$ is a prime element of $\mathbb{Q}_p(\zeta_m)$. Hence, we get $\mathrm{v}_L(\alpha^m-1) = m = \mathrm{v}_L(\lambda^p)$. Lemma 3.96 implies $\mathrm{v}_L(\lambda^{p-1}) = \mathrm{v}_L(p)$ and therefore we have $\mathrm{v}_L(\alpha^m-1) = \mathrm{v}_L(p\lambda)$. The equality $\mathrm{v}_F(\alpha^m-1) = \mathrm{v}_F(p\lambda)$ follows. □

3.9 Functorial properties

Theorem 3.100. *Let d and m be positive integers such that d divides m. Let F and E be local fields containing a primitive m-th root of unity and a primitive d-th root of unity, respectively. Let $\mu_m(F)$ and $\mu_d(E)$ be the groups of m-th and d-th roots of unity in F and in E, respectively, and let $\sigma : E \to F$ be a continuous homomorphism. Let $\sigma_* = \sigma|_{E^*} : E^* \to F^*$ and $\sigma^* = F^* \to E^*$ be the maps*

$$\sigma_* = \sigma|_{E^*} : E^* \to F^* \quad \text{and} \quad \sigma^* = \sigma^{-1} \circ \mathrm{N}_{F^*/\sigma E^*} : F^* \to E^*.$$

Then the maps $\sigma^* : F^* \to E^*$ and $(a \mapsto a^{m/d}) \circ \sigma_* : E^* \to F^*$ shown in the diagram

$$\begin{array}{ccc} F^* \times F^* & \xrightarrow{(\cdot,\cdot)_{F,m}} & \mu_m(F) \\ {\scriptstyle \sigma^*}\downarrow & \uparrow{\scriptstyle (a\mapsto a^{m/d})\circ\sigma_*} & \uparrow{\scriptstyle \sigma|_{\mu_d(E)}} \\ E^* \times E^* & \xrightarrow{(\cdot,\cdot)_{E,d}} & \mu_d(E) \end{array}$$

are adjoint with respect to the norm-residue symbol, that is, for all $a \in E^*$ and $b \in F^*$ one has

$$\sigma\left(\sigma^*(b), a\right)_{E,d} = \left(b, \sigma_*(a)^{m/d}\right)_{F,m}.$$

Proof. See Lemma 1 in Section 3.1 of Chapter IV in [28] by Iyanaga. □

Corollary 3.101. *Let m be a positive integer, let F be a local field containing a primitive m-th root of unity, and let $\sigma : F \to F$ be a continuous automorphism of F. Then, for all a, $b \in F^*$ one has*

$$(\sigma a, \sigma b) = \sigma\left(a, b\right).$$

Proof. Apply Theorem 3.100 with $E = F$ and $d = m$. □

3.10 The field of two-adic rationals and its unramified extensions

We present in a more explicit way the quadratic norm-residue symbol in the field $\mathbb{Q}_2$ of 2-adic rationals. For unramified extensions of $\mathbb{Q}_2$ we state and prove

Lemma 3.106.

Lemma 3.102. *Let $\mathbb{Q}_2$ be the field of 2-adic rationals, let $\mathbb{Z}_2$ be its ring of integers, let U be group of units of $\mathbb{Z}_2$, and for each $n \in \mathbb{Z}_{\geq 0}$ let $U^{(n)}$ be its n-th higher unit group. Then there is the equality*

$$\mathbb{Z}_2^{*2} = U^{(3)}.$$

Proof. By Theorem 3.37 we have the equalities

$$\mathbb{Z}_2^* = U = U^{(1)}.$$

Hence, if a is an element in $\mathbb{Z}_2^*$, we can write $a = 1 + 2x$ with $x \in \mathbb{Z}_2$. By squaring we obtain

$$a^2 = 1 + 4x(1 + x) \equiv 1 \bmod 8.$$

Since by definition we have $1 + 8\mathbb{Z}_2 = U^{(3)}$, we get $a^2 \in U^{(3)}$ and therefore the inclusion $\mathbb{Z}_2^{*2} \subseteq U^{(3)}$. Theorem 3.71 gives $[\mathbb{Z}_2^* : \mathbb{Z}_2^{*2}] = 4$. Since $U^{(3)}$ has also index 4 in $\mathbb{Z}_2^*$, we obtain the equality $\mathbb{Z}_2^{*2} = U^{(3)}$. □

Theorem 3.103. *Let $\mathbb{Q}_2$ be the field of 2-adic rationals and for every $a \in \mathbb{Q}_2^*$ let $\overline{a}$ be the residue class $a \bmod \mathbb{Q}_2^{*2}$ of a in $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$. Then the natural map*

$$\langle \overline{2} \rangle \times \langle \overline{-1} \rangle \times \langle \overline{5} \rangle \xrightarrow{\sim} \mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$$

is a group isomorphism and each of the groups $\langle \overline{2} \rangle$, $\langle \overline{-1} \rangle$, and $\langle \overline{5} \rangle$ has order 2.

Proof. The split sequence of Theorem 3.37 gives the isomorphism

$$\mathbb{Q}_2^* \cong \langle 2 \rangle \times \mathbb{Z}_2^*.$$

By squaring and applying Lemma 3.102 we obtain the isomorphism

$$\mathbb{Q}_2^{*2} \cong \langle 4 \rangle \times U^{(3)}.$$

Taking the quotients we get the desired isomorphism. Since by definition we have $1 + 8\mathbb{Z}_2 = U^{(3)}$, each element in $\{\overline{2}, \overline{-1}, \overline{5}\}$ has nontrivial image in $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$ and therefore each of the groups $\langle \overline{2} \rangle$, $\langle \overline{-1} \rangle$, and $\langle \overline{5} \rangle$ has order 2. □

Theorem 3.104. *Let $\mathbb{Q}_2$ be the field of 2-adic rationals and for every $a \in \mathbb{Q}_2^*$ let $\overline{a}$ be the residue class $a \bmod \mathbb{Q}_2^{*2}$ of a in $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$. Then the table*

$(\cdot,\cdot)$	$\overline{2}$	$\overline{-1}$	$\overline{5}$
$\overline{2}$	1	1	-1
$\overline{-1}$	1	-1	1
$\overline{5}$	-1	1	1

gives an explicit description of the perfect pairing

$$(\cdot,\cdot) : \mathbb{Q}_2^*/\mathbb{Q}_2^{*2} \times \mathbb{Q}_2^*/\mathbb{Q}_2^{*2} \to \{\pm 1\}$$

induced by the quadratic norm-residue symbol

$$(\cdot,\cdot)_{\mathbb{Q}_2,2} : \mathbb{Q}_2^* \times \mathbb{Q}_2^* \to \{\pm 1\}.$$

Proof. Using bilinearity of Theorem 3.69 and the relations of Theorem 3.74 we obtain the equalities

$$\begin{gathered}
1 = (1-2,2) = (-1,2), \\
1 = (1-5,5) = (4,5)(-1,5) = (2^2,5)(-1,5) = (2,5)^2(-1,5) = (-1,5), \\
1 = (-2,2) = (-1,2)(2,2) = (2,2), \\
1 = (-5,5) = (-1,5)(5,5) = (5,5), \\
1 = (-1,2)(2,-1) = (2,-1), \\
1 = (-1,5)(5,-1) = (5,-1).
\end{gathered}$$

Since by Theorem 3.70 the pairing induced by the norm-residue symbol is perfect, we get

$$(2,5) = (5,2) = (-1,-1) = -1. \qquad \square$$

Corollary 3.105. *Let $\mathbb{Q}_2$ be the field of 2-adic rationals and let U be the unit group of the ring of integers of $\mathbb{Q}_2$. Then the annihilator $U^\perp$ in U of U with respect to the norm-residue symbol $(\cdot,\cdot)_{\mathbb{Q}_2,2} : \mathbb{Q}_2 \times \mathbb{Q}_2 \to \{\pm 1\}$ is the second higher unit group $U^{(2)}$ of the ring of integers of $\mathbb{Q}_2$ and the perfect pairing*

$$(\cdot,\cdot) : U/U^\perp \times U/U^\perp \to \mu_2$$

induced by the norm-residue symbol is given by

$$\text{for } a,b \in \mathbb{Z}_2^* \quad (a,b) = \begin{cases} -1 \text{ if } a \equiv b \equiv 3 \bmod 4, \\ 1 \text{ otherwise.} \end{cases}$$

Proof. This follows from Theorem 3.104. $\square$

The diagram of Section 3.8 becomes the following one on the left. On the right

we show what each piece is canonically equal to.

$$\begin{array}{c} \mathbb{Q}_2^*/\mathbb{Q}_2^{*2} \\ \Big| \\ {\scriptstyle 2} \\ \Big| \\ U/U^2 \\ \Big| \\ {\scriptstyle |2|^{-1}=2} \\ \Big| \\ (U/U^2)^{\perp} \\ \Big| \\ {\scriptstyle 2} \\ \Big| \\ 1 \end{array} \qquad \begin{array}{c} \langle \overline{2} \rangle \times (\mathbb{Z}/8\mathbb{Z})^* \\ \Big| \\ {\scriptstyle \mathbb{Z}/2\mathbb{Z}} \\ \Big| \\ (\mathbb{Z}/8\mathbb{Z})^* \\ \Big| \\ {\scriptstyle (\mathbb{Z}/4\mathbb{Z})^*} \\ \Big| \\ \langle \overline{5} \rangle \\ \Big| \\ {\scriptstyle \mathbb{Z}/2\mathbb{Z}} \\ \Big| \\ 1 \end{array}$$

Lemma 3.106. *Let F be a finite unramified extension of the field $\mathbb{Q}_2$ of 2-adic rationals, let $\mathcal{O}_F$ be the ring of integers of F, let $\mathfrak{P}$ be the maximal ideal of $\mathcal{O}_F$, and let $(\cdot,\cdot)_F : F^* \times F^* \to \{\pm 1\}$ be the quadratic norm-residue symbol of F. Then for all $a, b \in \mathcal{O}_F$ one has*

$$(1+2a, 1+2b)_F = (-1)^{\mathrm{Tr}_{\mathfrak{P}}((a+\mathfrak{P})(b+\mathfrak{P}))}$$

with $\mathrm{Tr}_{\mathfrak{P}}$ denoting the trace map from $\mathcal{O}_F/\mathfrak{P}$ to $\mathbb{Z}/2\mathbb{Z}$.

Proof. Let U_F be the group of units of the ring of integers of F. Let $d \in 1+4\mathcal{O}_F$ and let δ be an element in an algebraic closure of F with $\delta^2 = d$. Since by Theorem 3.95 the extension $F(\delta)/F$ is unramified, Theorem 3.86 implies that for all $c \in U_F$ we have $(c, d) = 1$. Hence, we may assume $a, b \in U_F$ and therefore we have

$$\frac{1+2b}{1-4ab} \in F^* \setminus \{1\}.$$

By Theorem 3.74 for each $c \in F^* \setminus \{1\}$ one has $(1-c, c)_F = 1$. The equality

$$\left(\frac{-2b(1+2a)}{1-4ab}, \frac{1+2b}{1-4ab} \right)_F = 1$$

follows. Since the norm-residue symbol is an antisymmetric bilinear map and we have just proved that for all $c \in U_F$ we have $(c, 1-4ab) = 1$, we obtain the equality

$$(1+2a, 1+2b)_F = (1-4ab, 2)_F .$$

Let $(\cdot,\cdot)_{\mathbb{Q}_2} : \mathbb{Q}_2^* \times \mathbb{Q}_2^* \to \{\pm 1\}$ be the quadratic norm-residue symbol of $\mathbb{Q}_2$ and denote the norm map from F to $\mathbb{Q}_2$ by $\mathrm{N}_{F/\mathbb{Q}_2}$. Theorem 3.100 implies the equality

$$(1-4ab, 2)_F = \left(\mathrm{N}_{F/\mathbb{Q}_2}(1-4ab), 2\right)_{\mathbb{Q}_2} .$$

Since we have the congruence

$$\mathrm{N}_{F/\mathbb{Q}_2}(1-4ab) \equiv 1 - 4\,\mathrm{Tr}_{\mathfrak{P}}((a+\mathfrak{P})(b+\mathfrak{P})) \bmod 8,$$

the statement of Lemma 3.106 follows from Theorem 3.104. □

CHAPTER 4

The global norm-residue symbol

We extend the theory of the norm-residue symbol to global fields and groups of ideles. As a corollary of Theorem 4.59 we obtain a new proof [Corollary 4.67] of the fact that the Tate pairing is a perfect pairing [Theorem 4.69]. Moreover, Theorem 4.86 gives a pairing similar to the Tate pairing in the case of number fields.

4.1 Global fields

The reference for this section is Chapter II in [9] by Cassels and Fröhlich. Note that they call 'valuation' what we will call 'absolute value'.

Definition 4.1 (Number field)**.** A *number field* is a finite field extension of the field $\mathbb{Q}$ of rational numbers.

Definition 4.2 (Function field)**.** A *function field* is a finite field extension of the field $\mathbb{F}(t)$ of rational functions in one variable t over a finite field $\mathbb{F}$.

Definition 4.3 (Global field)**.** A *global field* is a field that is either a number field or a function field.

Definition 4.4 (Absolute value)**.** An *absolute value* $|\cdot|$ on a field K is a function

$$|\cdot| : K \to \mathbb{R}_{\geq 0}$$

with the following properties.

(a) For all $a \in K$ one has: $|a| = 0$ if and only if $a = 0$.
(b) For all $a, b \in K$ one has $|ab| = |a| \cdot |b|$.
(c) There exists $C \in \mathbb{R}$ such that for all $a \in K$ with $|a| \leq 1$ one has $|1 + a| \leq C$.

Remark 4.5. In many books (c) of Definition 4.4 is replaced by the triangle inequality $|a+b| \leq |a|+|b|$ for all $a, b \in K$. Our choice is inspired by the desire to call the normalized absolute value on the field of complex numbers, which is the square of the ordinary absolute value, an absolute value.

Definition 4.6 (Trivial absolute value)**.** The *trivial absolute value* on a field K is the unique function $K \to \{0, 1\}$ that is an absolute value on K.

Definition 4.7 (Equivalent absolute values)**.** Two absolute values $|\cdot|_1 : K \to \mathbb{R}_{\geq 0}$ and $|\cdot|_2 : K \to \mathbb{R}_{\geq 0}$ on a field K are *equivalent* if there exists $C \in \mathbb{R}_{>0}$ such that for all $a \in K$ one has

$$|a|_1 = |a|_2^C.$$

Remark 4.8. Let K be a field. An absolute value $|\cdot|$ on K induces a topology on K that is generated by all sets of the form $\{x \in K : |x-a| < d\}$ with $a \in K$ and $d \in \mathbb{R}_{>0}$.

Theorem 4.9. *Let K be a field. Two absolute values on K are equivalent if and only if they induce the same topology on K.*

Proof. See Section 4 of Chapter II in [9] by Cassels and Fröhlich. □

Definition 4.10 (Place)**.** A *place* v of a global field K is an equivalence class of nontrivial absolute values on K.

Definition 4.11 (Non-Archimedean and Archimedean places)**.** A place v of a global field K is *non-Archimedean* if the completion K_v of K at v is a non-Archimedean local field. Otherwise, it is *Archimedean*.

For a place v of a global field K we denote the normalized absolute value on the completion K_v of K at v by $|\cdot|_v : K_v \to \mathbb{R}_{\geq 0}$.

Theorem 4.12. *Let K be a function field. Then all places of K are non-Archimedean.*

Proof. See Section 1 of Chapter III in [18] by Fröhlich and Taylor. □

Theorem 4.13. *Let K be a number field, let F be either $\mathbb{R}$ or $\mathbb{C}$, let $|\cdot|_F : F \to \mathbb{R}_{\geq 0}$ be the ordinary absolute value on F, and let $\sigma : K \hookrightarrow F$ be a field embedding. Then the function $|\cdot| : K \to \mathbb{R}_{\geq 0}$, $a \mapsto |\sigma(a)|_F$, is an absolute value on K.*

Proof. This follows from the definition of the ordinary absolute value on $\mathbb{C}$. □

Theorem 4.14. *Let K be a number field, let r_1 be the number of real embeddings $K \hookrightarrow \mathbb{R}$, and let r_2 be the number of conjugate pairs of complex embeddings $\sigma : K \hookrightarrow \mathbb{C}$ with $\sigma(K) \not\subseteq \mathbb{R}$. Then each Archimedean place of K is the equivalence class of an absolute value on K defined by a field embedding as in* Theorem 4.13*, there are exactly $r_1 + r_2$ Archimedean places of K, each of which corresponds to either a real embedding of K or a conjugate pair of complex embeddings of K, and all other places of K are non-Archimedean.*

Proof. See Section 1 of Chapter III in [18] by Fröhlich and Taylor. □

4.2 Adeles and ideles

In this section we recall the concepts of adeles and ideles. As a reference see Chapter II in [9] by Cassels and Fröhlich. We point out that given a set Λ the expression 'for almost all $\lambda \in \Lambda$' means 'for all but finitely many $\lambda \in \Lambda$'.

Definition 4.15 (Restricted topological product)**.** Let Λ be an index set and for each $\lambda \in \Lambda$ let X_λ be a topological space. For all but finitely many $\lambda \in \Lambda$ fix an open subset $Y_\lambda \subseteq X_\lambda$ and consider the space X of sequences $\alpha = (\alpha_\lambda)_{\lambda\in\Lambda}$ with $\alpha_\lambda \in X_\lambda$ for all $\lambda \in \Lambda$ and $\alpha_\lambda \in Y_\lambda$ for all but finitely many $\lambda \in \Lambda$. Introduce a topology on X by taking as a basis of open sets the sets of the form $\prod_{\lambda\in\Lambda} W_\lambda$, where $W_\lambda \subseteq X_\lambda$ is open for all λ and $W_\lambda = Y_\lambda$ for all but finitely many λ. The space X with this topology is the *restricted topological product* of the spaces X_λ with respect to the subsets Y_λ and is denoted by

$$X = \prod_{\lambda\in\Lambda}{}' X_\lambda.$$

Definition 4.16 (Ring of adeles)**.** The *ring of adeles* Ad_K of a global field K is the ring of all elements of the restricted topological product of the completions K_v of K at v, where v ranges over all places of K, with respect to their rings of integers $\mathcal{O}_v$. Sum and multiplication are defined componentwise.

Remark 4.17. The ring of adeles with the topology induced by the restricted topological product is a topological ring.

Remark 4.18. An adele α of K is a sequence $\alpha = (\alpha_v)_{v\in S}$ of elements $\alpha_v \in K_v$, where S is the set of places of K, such that α_v is an integer in K_v for all but finitely many v.

Since each element of K is an element of $\mathcal{O}_v$ for almost all v, we can define the map $i : K \hookrightarrow \mathrm{Ad}_K$ by $i(x) = (x)_v$. This map is injective and, identifying K with its image under i, we shall view it as a subring that is a field of Ad_K.

Definition 4.19 (Group of ideles)**.** The *group of ideles* J_K of a global field K is the topological group of all invertible elements of the ring of adeles Ad_K with the topology induced by the inclusion $\mathrm{J}_K \hookrightarrow \mathrm{Ad}_K \times \mathrm{Ad}_K$ that maps each element $x \in \mathrm{J}_K$ to (x, x^{-1}).

Remark 4.20. Let K be a global field. For each place v of K let K_v be the completion of K at v, let U_v be the unit group of the ring of integers of K_v if v is non-Archimedean, and let U_v equal K_v^* otherwise. The group of ideles J_K of K can be equivalently defined as the topological group given by the restricted topological product of the spaces K_v^*, where v ranges over all places of K, with respect to the groups U_v, where multiplication is defined componentwise.

We will often write only J when the field K is understood. Just as K maps injectively into Ad_K, so there is a natural inclusion $K^* \hookrightarrow \mathrm{J}_K$.

Definition 4.21 (Group of unit ideles)**.** The *group of unit ideles* U_K of a global field K is the group

$$\mathrm{U}_K = \{(a_v)_{v \in S} \in \prod_v K_v^* : \forall v \notin S_\infty : |a_v|_v = 1\},$$

where S and S_∞ are the set of places of K and the set of Archimedean places of K, respectively.

We will often write only U when the field K is understood.

Remark 4.22. Let the notation be as in Remark 4.20. The group of unit ideles U_K of a global field K can be equivalently written as

$$\mathrm{U}_K = \prod_{v \in S} U_v,$$

where S is the set of places of K.

Theorem 4.23. *Let K be a global field and let Ad_K be the ring of adeles of K. Then K is a discrete subring of Ad_K and the additive group Ad_K/K is compact in the quotient topology.*

Proof. See Theorem in Section 14 of Chapter II in [9] by Cassels and Fröhlich. □

Lemma 4.24. *Let K be a global field and let J_K be group of ideles of K. Then K^* is a discrete subgroup of J_K.*

Proof. By Theorem 4.23 the field K is a discrete subgroup of Ad_K. The map $\mathrm{Ad}_K^* \to \mathrm{Ad}_K \times \mathrm{Ad}_K$, $x \mapsto (x, x^{-1})$, injects K^* as a discrete subset. Hence, the group K^* is a discrete subgroup of J_K. □

Definition 4.25 (Content map)**.** Let K be a global field, let S be the set of places of K, and let J_K be the group of ideles of K. The *content map* c of K is the map

$$\begin{aligned} c : \mathrm{J}_K &\to \mathbb{R}_{>0}, \\ j = (j_v)_v &\mapsto \prod_{v \in S} |j_v|_v, \end{aligned}$$

where for each $v \in S$ the map $|\cdot|_v : K_v \to \mathbb{R}_{>0}$ denotes the normalized absolute value on the completion K_v of K at v.

The map $c : \mathrm{J}_K \to \mathbb{R}_{>0}$, $a \mapsto c(a)$, is a continuous group homomorphism of the topological group J_K to the multiplicative group of positive real numbers. We denote by J_K^0 its kernel. When K is a number field this map is surjective and gives the split exact sequence

$$1 \to \mathrm{J}_K^0 \to \mathrm{J}_K \to \mathbb{R}_{>0} \to 1. \tag{4.26}$$

A right splitting of this exact sequence is the map $\mathbb{R}_{>0} \to \mathrm{J}_K$, $a \to (a_v)_v$, where $a_v = 1$ if v is non-Archimedean and $a_v = a^{1/[K:\mathbb{Q}]}$ if v is Archimedean.

When K is a function field the image of the group homomorphism c is a nontrivial discrete subgroup of $\mathbb{R}_{>0}$. The map c gives rise to the split exact sequence

$$1 \to \mathrm{J}_K^0 \to \mathrm{J}_K \to \mathbb{Z} \to 1. \tag{4.27}$$

Theorem 4.28 (Product formula)**.** *Let K be a global field and let J_K^0 be the kernel of the content map $c : \mathrm{J}_K \to \mathbb{R}_{>0}$ of K. Then one has the inclusion*

$$K^* \subset \mathrm{J}_K^0 .$$

Proof. See Theorem in Section 12 of Chapter II in [9] by Cassels and Fröhlich. □

Remark 4.29. Theorem 4.28 is known as the product formula for global fields, because the inclusion $K^* \subset \mathrm{J}_K^0$ can be equivalently written as follows: for all $a \in K^*$ one has

$$\prod_{v \in S} |a|_v = 1,$$

where S is the set of places of K.

Theorem 4.30. *Let K be a global field and let J_K^0 be the kernel of the content map $c : \mathrm{J}_K \to \mathbb{R}_{>0}$ of K. Then the quotient J_K^0/K^* is compact in the quotient topology.*

Proof. See Chapter II in [9] by Cassels and Fröhlich. □

Theorem 4.31. *Let m be a positive integer, let K be a global field, let J_K be the group of ideles of K, and let U_K be the group of unit ideles of K. Then the quotient group $\mathrm{J}_K/(K^* \cdot \mathrm{U}_K \cdot \mathrm{J}_K^m)$ is finite.*

Proof. The quotient group $\mathrm{J}_K/(K^* \cdot \mathrm{U}_K \cdot \mathrm{J}_K^m)$ is discrete, because by definition the group U_K is open in J_K. Using the inclusion $K^* \subset \mathrm{J}_K^0$ given by Theorem 4.28 and the short split exact sequences 4.26 and 4.27 we get an isomorphism of topological groups:

$$\mathrm{J}_K/K^* \cong \mathbb{R} \times (\mathrm{J}_K^0/K^*) \text{ if } K \text{ is a number field,}$$
$$\mathrm{J}_K/K^* \cong \mathbb{Z} \times (\mathrm{J}_K^0/K^*) \text{ if } K \text{ is a function field.}$$

Since by Theorem 4.30 the group J_K^0/K^* is compact, the quotient group $\mathrm{J}_K/(K^* \cdot \mathrm{J}_K^m)$ is the direct product of a finite group and a compact group and therefore is compact. Hence, the quotient group $\mathrm{J}_K/(K^* \cdot \mathrm{U}_K \cdot \mathrm{J}_K^m)$ is compact. Since it is also discrete, it is finite. □

4.3 Locally compact abelian groups

For this section the references are [56] by Pontryagin, [75] by Weil, and [49] by Morris.

Definition 4.32 (Locally compact group)**.** A *locally compact group* is a topological group that is locally compact as a topological space.

Definition 4.33 (Character)**.** A *character* of a locally compact Hausdorff abelian group G is a continuous group homomorphism from G to the circle group $\mathbb{R}/\mathbb{Z}$.

The set of all characters of G forms a group under pointwise addition.

Definition 4.34 (Dual group or character group)**.** The group $\widehat{G}$ of characters of a locally compact Hausdorff abelian group G is the *dual group* or *character group* of G.

Remark 4.35. We endow the dual group $\widehat{G}$ of a locally compact Hausdorff abelian group G with the open-compact topology. This renders $\widehat{G}$ a topological group.

Theorem 4.36. *Let G be a locally compact Hausdorff abelian group. Then the dual group $\widehat{G}$ of G is a locally compact Hausdorff abelian group.*

Proof. See Theorem 36 in Section 34 of Chapter 6 in [56] by Pontryagin. □

Theorem 4.37 (Pontryagin Duality)**.** *Let $\mathcal{L}$ be the category of locally compact Hausdorff abelian groups with continuous group homomorphisms. Then the dualization $\widehat{\ } : \mathcal{L} \to \mathcal{L}$ provides an anti-equivalence of categories*

$$\begin{array}{ccc} \mathcal{L} & \longrightarrow & \mathcal{L} \\ G & \mapsto & \widehat{G} \end{array}$$

and the canonical map from a locally compact Hausdorff abelian group G to $\widehat{\widehat{G}}$ that maps an element $x \in G$ to the character $\widehat{x} \to \widehat{x}(x)$ of $\widehat{G}$ is a functor isomorphism from the identity functor on $\mathcal{L}$ and the iterated dualization $\widehat{\ } \circ \widehat{\ } : \mathcal{L} \to \mathcal{L}$. This duality also restricts to the anti-equivalence

$$\{\textit{compact abelian groups}\} \longleftrightarrow \{\textit{discrete abelian groups}\}.$$

Proof. See Theorem 52 in Section 40 of Chapter 6 in [56] by Pontryagin. □

The canonical map from a locally compact Hausdorff abelian group G to $\widehat{\widehat{G}}$ that maps an element $x \in G$ to the character $\widehat{x} \to \widehat{x}(x)$ of $\widehat{G}$ is a topological group isomorphism. We may therefore consider G as the character group of $\widehat{G}$.

Definition 4.38 (Annihilator)**.** Let H be a subset of a locally compact Hausdorff abelian group G. The *annihilator* $H^\perp$ of H in G is the set

$$H^\perp = \{\widehat{x} | \widehat{x} \in \widehat{G}, \forall x \in H : \widehat{x}(x) = 0\}.$$

Theorem 4.39. *Let G be a locally compact Hausdorff abelian group. Then the maps*

$$\begin{array}{ccc} \{\textit{closed subgroups of } G\} & \longleftrightarrow & \{\textit{closed subgroups of } \widehat{G}\} \\ H & \mapsto & H^\perp \\ I^\perp & \hookleftarrow & I \end{array}$$

are inclusion-reversing bijections and are inverse to each other. Moreover, if H is a closed subgroup of G, then the natural maps

$$H^\perp \xrightarrow{\sim} \widehat{G/H} \quad \textit{and} \quad \widehat{G}/H^\perp \xrightarrow{\sim} \widehat{H}$$

are isomorphisms of topological groups.

Proof. See Theorem 27 in Chapter 7 in [49] by Morris. □

Remark 4.40 (Pairing on topological groups)**.** When A, B, and C are topological abelian groups, a pairing

$$\beta : A \times B \to C$$

will be also required to be a continuous map from $A \times B$ to C. See Definition 2.1 for the definition of a pairing on abelian groups.

Definition 4.41 (Dual groups with respect to a pairing)**.** Let G and G' be locally compact Hausdorff abelian groups and let

$$\beta : G \times G' \to \mathbb{R}/\mathbb{Z}$$

be a pairing. The groups G and G' are *dual with respect to the pairing* $\beta : G \times G' \to \mathbb{R}/\mathbb{Z}$ if the map $G' \to \widehat{G}$, $g' \mapsto (\beta(\cdot, g') : G \to \mathbb{R}/\mathbb{Z})$, is a topological group isomorphism.

See Definition 2.41 for the definition of a nondegenerate pairing.

Lemma 4.42. *Let G and G' be locally compact Hausdorff abelian groups and let $(\cdot,\cdot)$ be a nondegenerate pairing*

$$(\cdot,\cdot) : G \times G' \to \mathbb{R}/\mathbb{Z}.$$

If H and H' are compact subgroups of G and G', respectively, such that the subgroup H is the annihilator of H' in G with respect to the pairing $(\cdot,\cdot)$, then the groups G and G' are dual with respect to the pairing $(\cdot,\cdot)$ and the subgroups H and H' are open subgroups of G and G', respectively.

Proof. See Lemma 4 in Section 1.3 of Chapter III in [28] by Iyanaga. □

Lemma 4.43. *Let G and G' be locally compact Hausdorff abelian groups and let $(\cdot,\cdot)$ be a nondegenerate pairing*

$$(\cdot,\cdot) : G \times G' \to \mathbb{R}/\mathbb{Z}.$$

If H and H' are closed subgroups of G and G', respectively, such that the quotient groups G/H and G'/H' are compact and the subgroup H is the annihilator of H' in G with respect to the pairing $(\cdot,\cdot)$, then the groups G and G' are dual with respect to the pairing $(\cdot,\cdot)$ and the subgroups H and H' are discrete subgroups of G and G', respectively.

Proof. See Lemma 5 in Section 1.3 of Chapter III in [28] by Iyanaga. □

Lemma 4.44. *Let G be a topological group and let A and B be subsets of G. Then one has the following.*

(a) *If A and B are compact, then AB is compact;*
(b) *If A is compact and B is closed, then AB is closed.*

Proof. If A and B are compact, then by Tychonoff's theorem the subset $A \times B$ of $G \times G$ is compact. The set AB is compact, because it is the continuous image of the compact set $A \times B$ under multiplication.

For a proof of the second fact see Lemma 1 of Section 2 in Chapter X in [2] by Artin and Tate. □

Note that if in Lemma 4.44 the subsets A and B are closed then AB does not need to be closed. For example, take the closed subgroups $\mathbb{Z}$ and $\mathbb{Z} \cdot \sqrt{2}$ of $\mathbb{R}$ as A and B, respectively.

4.4 Self-duality

We want to extend the concept of norm-residue symbol to global fields.

Definition 4.45 (Tame place and wild place)**.** Let m be a positive integer. A place v of a global field containing a primitive m-th root of unity is a *tame place* with respect to m if one has $|m|_v = 1$, otherwise it is a *wild place* with respect to m.

Remark 4.46. Let m be a positive integer. An Archimedean place v of a global field containing a primitive m-th root of unity is tame with respect to m if and only if one has $m = 1$.

Definition 4.47 (Idelic m-th power norm-residue symbol)**.** Let m be a positive integer, let K be a global field containing a primitive m-th root of unity, let μ_m be the group of m-th roots of unity in K, let S be the set of places of K, and let J_K be the group of ideles of K. The *idelic m-th power norm-residue symbol* is the map

$$\begin{aligned}(\cdot,\cdot)_{K,m} : \mathrm{J}_K \times \mathrm{J}_K &\to \mu_m,\\ (a,b) &\mapsto (a,b)_{K,m}\,,\end{aligned}$$

such that for all $a = (a_v)_v, b = (b_v)_v \in \mathrm{J}_K$ one has

$$(a,b)_{K,m} = \prod_{v\in S} (a_v, b_v)_{K_v,m}\,,$$

where for each place v of K the map $(\cdot,\cdot)_{K_v,m} : K_v^* \times K_v^* \to \mu(K_v)$ denotes the m-th power norm-residue symbol of the completion K_v of K at v and the group $\mu(K_v)$ of m-th roots of unity in K_v is identified with the group μ_m by the inclusion $K \hookrightarrow K_v$.

We will often write only '$(\cdot,\cdot)$' and 'norm-residue symbol' when m and K are understood.

Remark 4.48. The norm-residue symbol is well-defined on the group of ideles J_K. For all $a = (a_v)_v, b = (b_v)_v \in \mathrm{J}_K$ we have that all but finitely many places of K are tame and for all but finitely many of them both arguments a_v and b_v are units. Since by Theorem 3.89 we have $(a_v, b_v) = 1$ when both a_v and b_v are units and v is a tame place, the infinite product $\prod_v (a_v, b_v)_v$ is actually a finite product.

Theorem 4.49. *Let m be a positive integer, let K be a global field containing a primitive m-th root of unity, and let μ_m be the group of m-th roots of unity in K. Then the norm-residue symbol*

$$(\cdot,\cdot)_{K,m} : \mathrm{J}_K \times \mathrm{J}_K \to \mu_m$$

is an antisymmetric pairing and induces a nondegenerate antisymmetric pairing

$$(\cdot,\cdot) : \mathrm{J}_K/\mathrm{J}_K^m \times \mathrm{J}_K/\mathrm{J}_K^m \to \mu_m.$$

Proof. The norm-residue symbol is bilinear and antisymmetric, because it is the product of bilinear antisymmetric maps. Let $a = (a_v)_v, b = (b_v)_v \in \mathrm{J}_K$ and let S be the finite set of places of K consisting of all Archimedean places, all wild places, and all places v of K where a_v and b_v are not both units. Let H_a and H_b be the subsets of J_K

$$H_a = \prod_{v\in S} a_v K_v^{*m} \times \prod_{v\notin S} U_v \quad \text{and} \quad H_b = \prod_{v\in S} b_v K_v^{*m} \times \prod_{v\notin S} U_v.$$

They are open neighbourhoods of a and b, respectively, and by Theorem 3.89 the value (h_a, h_b) does not depend on the choice of $h_a \in H_a$ and $h_b \in H_b$. Hence, the norm-residue symbol is a continuous map.

The induced map is an antisymmetric pairing. It is also nondegenerate. Let $a \in \mathrm{J}_K$ be such that for all $b \in \mathrm{J}_K$ the product $\prod_v (a_v, b_v)_v$ is 1. Letting b range over the elements of the form $(1, 1, \ldots, 1, b_w, 1, \ldots)$ with w a place of K, we get $a_v \in (K_v^*)^m$ for all places v of K. Hence, we have $a \in \mathrm{J}_K^m$. □

We will often call 'norm-residue symbol' the pairing induced by the norm-residue symbol in Theorem 4.49.

Theorem 4.50. *Let m be a positive integer, let K be a global field containing a primitive m-th root of unity, let μ_m be the group of m-th roots of unity in K, let J_K be the group of ideles of K, and let $\psi : \mu_m \to \mathbb{R}/\mathbb{Z}$ be an injective group homomorphism. Then the quotient group $\mathrm{J}_K/\mathrm{J}_K^m$ is a locally compact Hausdorff abelian group and is its own dual with respect to the pairing*

$$\psi \circ (\cdot,\cdot) : \mathrm{J}_K/\mathrm{J}_K^m \times \mathrm{J}_K/\mathrm{J}_K^m \to \mathbb{R}/\mathbb{Z}$$

induced by the norm-residue symbol.

Proof. Since J_K^m is closed in J_K, the quotient group $\mathrm{J}_K/\mathrm{J}_K^m$ is Hausdorff. Note that $\mathrm{J}_K/\mathrm{J}_K^m$ is the restricted topological product of the groups K_v^*/K_v^{*m} with respect to the subgroups U_v/U_v^m. Let S be the finite set of places of K consisting of all wild places. The group

$$H = \prod_{v\in S} K_v^*/K_v^{*m} \times \prod_{v\notin S} U_v/U_v^m$$

is the product of two compact groups and by Lemma 4.44 it is compact. Moreover, the annihilator of H in $\mathrm{J}_K/\mathrm{J}_K^m$ is the compact group

$$H^\perp = \{1\} \times \prod_{v\notin S} U_v/U_v^m,$$

because by Remark 4.46 an Archimedean place is tame if and only if one has $m = 1$ and Theorem 3.89 implies that for every tame non-Archimedean place v of K the group U_v/U_v^m equals its own annihilator in K_v^*/K_v^{*m} with respect to the local norm-residue symbol. Consider any injective group homomorphism $\psi : \mu_m \to \mathbb{R}/\mathbb{Z}$. By Lemma 4.42 the group $\mathrm{J}_K/\mathrm{J}_K^m$ is its own dual with respect to the pairing

$$\psi \circ (\cdot, \cdot) : \mathrm{J}_K/\mathrm{J}_K^m \times \mathrm{J}_K/\mathrm{J}_K^m \to \mathbb{R}/\mathbb{Z}$$

induced by the norm-residue symbol. □

Lemma 4.51. *Let m be a positive integer, let K be a global field containing a primitive m-th root of unity, and let J_K be the group of ideles of K. Then one has the equality*

$$K^* \cap \mathrm{J}_K^m = K^{*m}.$$

Proof. See Lemma 5 in Section 4.3 of Chapter V in [28] by Iyanaga. □

Theorem 4.52. *Let m be a positive integer, let K be a global field containing a primitive m-th root of unity, and let J_K be the group of ideles of K. Then the subgroup $K^*/(K^*)^m$ of $\mathrm{J}_K/\mathrm{J}_K^m$ equals its own annihilator in $\mathrm{J}_K/\mathrm{J}_K^m$ with respect to the norm-residue symbol.*

Proof. See Section 4 of Chapter V in [28] by Iyanaga. □

Theorem 4.53. *Let m be a positive integer, let K be a global field containing a primitive m-th root of unity, and let J_K be the group of ideles of K. Then the subgroup $K^*/(K^*)^m$ of $\mathrm{J}_K/\mathrm{J}_K^m$ is discrete.*

Proof. The annihilator $\mathrm{U}_K^\perp$ of the group U_K of unit ideles of K in J_K with respect to the norm-residue symbol is open in J_K and therefore its image $\varphi(\mathrm{U}_K^\perp)$ in $\mathrm{J}_K/\mathrm{J}_K^m$ under the quotient map $\varphi : \mathrm{J}_K \to \mathrm{J}_K/\mathrm{J}_K^m$ is also open. Using Theorem 4.52 the group

$$\varphi(K^*) \cap \varphi(\mathrm{U}_K^\perp) = ((K^* \cdot \mathrm{J}_K^m) \cap (\mathrm{U}_K^\perp \cdot \mathrm{J}_K^m))/\,\mathrm{J}_K^m$$

is the annihilator of the group $(K^* \cdot \mathrm{U}_K \cdot \mathrm{J}_K^m)/\,\mathrm{J}_K^m$ with respect to the pairing $(\cdot, \cdot) : \mathrm{J}_K/\mathrm{J}_K^m \times \mathrm{J}_K/\mathrm{J}_K^m \to \mu_m$ induced by the norm-residue symbol. Since by Theorem 4.31 the quotient group $\mathrm{J}_K/(K^* \cdot \mathrm{U}_K \cdot \mathrm{J}_K^m)$ is finite, by duality the group $\varphi(K^*) \cap \varphi(\mathrm{U}_K^\perp)$ is also finite. It is a discrete subgroup of $\mathrm{J}_K/\mathrm{J}_K^m$, because it is a finite subgroup of the open subgroup $\varphi(\mathrm{U}_K^\perp)$ of $\mathrm{J}_K/\mathrm{J}_K^m$. It follows that $K^*/(K^*)^m$ is a discrete subgroup of $\mathrm{J}_K/\mathrm{J}_K^m$. □

Theorem 4.54 (Hilbert's product formula)**.** *Let m be a positive integer, let K be a global field containing a primitive m-th root of unity, and let S be the set of places of K. Then for all $a, b \in K^*$ one has*

$$\prod_{v \in S} (a, b)_v = 1.$$

Proof. By Theorem 4.52 the subgroup $K^*/(K^*)^m$ of $\mathrm{J}_K/\mathrm{J}_K^m$ equals its own annihilator in $\mathrm{J}_K/\mathrm{J}_K^m$ with respect to the norm-residue symbol. This implies that the annihilator of $K^*/(K^*)^m$ contains $K^*/(K^*)^m$. Hilbert's product formula follows. □

4.5 Function fields

Let $\mathbb{F}$ be a finite field, let q be the cardinality of $\mathbb{F}$, and let m be a positive integer dividing $q-1$. Thus, the field $\mathbb{F}$ contains a primitive m-th root of unity. Let $\mu_m(\mathbb{F})$ be the group of m-th roots of unity in $\mathbb{F}$. Let K be a function field with exact field of constants $\mathbb{F}$ and let S be the set of places of K. For every place $v \in S$ let d_v be the degree of the place v, that is, the degree of the residue field $\mathcal{O}_v/\mathfrak{P}_v$ of the completion K_v of K at v over $\mathbb{F}$. Moreover, we denote the group of ideles of K by J and the group $\prod_v U_v$ of unit ideles by U. Let $\overline{} : J \to J/J^m$ be the canonical projection of J onto J/J^m. Given a subgroup A of J we will write $\overline{A}$ for the group $(A \cdot J)/J^m$. Since the field K is understood, we will often drop any subscript K when it is used in formulas.

Definition 4.55 (Group of divisors)**.** Let $\mathbb{F}$ be a finite field and let K be a function field with exact field of constants $\mathbb{F}$. The *group of divisors* Div_K of K is the free abelian group on the set of places of K.

We have the degree map

$$\begin{aligned} \deg : \mathrm{Div} &\to \mathbb{Z}, \\ \sum_{v \in S} n_v v &\mapsto \sum_{v \in S} n_v d_v. \end{aligned}$$

It is a surjective map [Corollary V.1.11 in [68]] and its kernel is the group Div^0 of divisors of K of degree 0. There is a natural continuous map

$$\begin{aligned} \mathrm{div} : J &\to \mathrm{Div}, \\ j = (j_v)_v &\mapsto \mathrm{div}(j) = \sum_v (\mathrm{ord}_v\, j_v) \cdot v, \end{aligned}$$

where ord_v denotes the normalized valuation v_{K_v} on K_v. This is a common notation for function fields and their completions. We denote the integer $\deg(\mathrm{div}(j)) = \sum_v (\mathrm{ord}_v\, j_v) d_v$ by $\deg j$ and call it the degree of j. Hence, we get the short exact sequence

$$1 \longrightarrow U \longrightarrow J \xrightarrow{\mathrm{div}} \mathrm{Div} \longrightarrow 0.$$

Definition 4.56 (Group of principal divisors)**.** Let $\mathbb{F}$ be a finite field, let K be a function field with exact field of constants $\mathbb{F}$, let J_K be the group of ideles of

K, and let Div_K be the group of divisors of K. The *group of principal divisors* Pr_K of K is the image of $K^* \subset \mathrm{J}_K$ in Div_K under the map $\mathrm{div} : \mathrm{J}_K \to \mathrm{Div}_K$.

Composing the map $\mathrm{div} : J \to \mathrm{Div}$ with the degree map $\deg : \mathrm{Div} \to \mathbb{Z}$ we obtain a map $J \to \mathbb{Z}$, which gives rise to the split short exact sequences

$$1 \longrightarrow J^0 \longrightarrow J \longrightarrow \mathbb{Z} \longrightarrow 0$$

and

$$1 \longrightarrow \overline{J^0} \longrightarrow \overline{J} \longrightarrow \mathbb{Z}/m\mathbb{Z} \longrightarrow 0, \tag{4.57}$$

where J^0 is the group of ideles of K of degree zero.

Theorem 4.58. *Let $\mathbb{F}$ be a finite field, let q be the cardinality of $\mathbb{F}$, let m be a positive integer dividing $q-1$, and let $\mu_m(\mathbb{F})$ be the group of m-th roots of unity in $\mathbb{F}$. Let K be a function field with exact field of constants $\mathbb{F}$, let J be the group of ideles of K, and let U be the group of unit ideles of K. Then the subgroup $\overline{U}$ of J/J^m equals its own annihilator in J/J^m with respect to the norm-residue symbol*

$$(\cdot,\cdot) : J/J^m \times J/J^m \to \mu_m(\mathbb{F}).$$

Proof. Theorem 3.89 implies that for every tame non-Archimedean place v the group U_v/U_v^m equals its own annihilator in $K_v^*/(K_v^*)^m$ with respect to the local norm-residue symbol. Since all places are tame non-Archimedean, we get the identity $\overline{U} = \overline{U}^{\perp}$. □

Theorem 4.59. *Let $\mathbb{F}$ be a finite field, let q be the cardinality of $\mathbb{F}$, let m be a positive integer dividing $q-1$, and let $\mu_m(\mathbb{F})$ be the group of m-th roots of unity in $\mathbb{F}$. Let K be a function field with exact field of constants $\mathbb{F}$, let J be the group of ideles of K, and let U be the group of unit ideles of K. Then the inverse of the norm-residue symbol induces a perfect pairing of finite abelian groups*

$$(\cdot,\cdot)^{-1} : (\overline{K^*} \cap \overline{U}) \times \overline{J}/(\overline{K^*} \cdot \overline{U}) \to \mu_m(\mathbb{F})$$

that is characterized by (a)*, and its domain has the property* (b)*.*

(a) *For each pair $(f,j) \in (K^* \cap (U \cdot J^m)) \times J$ such that the divisors* $\mathrm{div}(f)$ *and* $\mathrm{div}(j)$ *have disjoint supports one has*

$$\left(\overline{f}, \overline{j} \cdot (\overline{K^*} \cdot \overline{U})\right) \xmapsto{(\cdot,\cdot)^{-1}} (f,j)^{-1} = f(\mathrm{div}(j))^{\frac{q-1}{m}},$$

where

$$f(\mathrm{div}(j)) = \prod_v \mathrm{N}_{(\mathcal{O}_v/\mathfrak{P}_v)/\mathbb{F}}(f^{n_v} \bmod \mathfrak{P}_v) \text{ if } \mathrm{div}(j) = \sum_v n_v v.$$

(b) *Any pair of elements in* $(\overline{K^*} \cap \overline{U}) \times \overline{J}/(\overline{K^*} \cdot \overline{U})$ *is of the form* $\big(\overline{f}, \overline{j} \cdot (\overline{K^*} \cdot \overline{U})\big)$ *with* f *and* j *as in* (a).

Proof. By Lemma 4.24 the group K^* is a discrete subgroup of J. Since the group U is a compact subgroup of J, by Lemma 4.44 the subgroup $K^* \cdot U$ is closed. Hence, the group $\overline{K^*} \cdot \overline{U}$ is a closed subgroup of J/J^m. Taking its annihilator and using Theorem 4.52 and Theorem 4.58 we get

$$(\overline{K^*} \cdot \overline{U})^\perp = \overline{K^*}^\perp \cap \overline{U}^\perp = \overline{K^*} \cap \overline{U}.$$

The group $\overline{K^*} \cap \overline{U}$ is finite, because it is discrete by Theorem 4.53 and compact. Theorem 4.39 implies that the induced pairing exists and is a perfect pairing of finite abelian groups.

Now we are going to prove the formula in (a). Let S be the set of places of K and for each $v \in S$ let K_v be the completion of K at v. By Theorem 3.89 and Theorem 3.86 for each $v \in S$ the extension $K_v(f_v^{1/m})/K_v$ is unramified. For each $v \in S$ we denote by Fr_v the Frobenius element in the Galois group $\mathrm{Gal}(K_v(f_v^{1/m})/K_v)$. By the weak approximation theorem for every $f \in K^* \cap (U \cdot J^m)$ the set of all $j \in J$ such that $\mathrm{div}(f)$ and $\mathrm{div}(j)$ have disjoint supports maps surjectively to $\overline{J}/(\overline{K^*} \cdot \overline{U})$. This proves (b). Since both the inverse of the norm-residue symbol and the formula give rise to a group homomorphism $\overline{J}/(\overline{K^*} \cdot \overline{U}) \to \mu_m(\mathbb{F})$ when the first argument is fixed, we can assume that $j \in J$ has divisor $\mathrm{div}(j) = w$, where w is a place of K not in the support of $\mathrm{div}(f)$. Let d_w be the degree of the place w. The computation

$$\begin{aligned}(f,j)^{-1} = (j,f) = \prod_{v \in S} (j,f)_v = \prod_{v \in S} \mathrm{Fr}_v^{\mathrm{ord}_v(j)}(f_v^{\frac{1}{m}})/f_v^{\frac{1}{m}} = \\ = \mathrm{Fr}_w(f_w^{\frac{1}{m}})/f_w^{\frac{1}{m}} = \left(f_w^{\frac{q^{d_w}-1}{m}} \bmod \mathfrak{P}_w\right) = \left(f_w^{\frac{q^{d_w}-1}{q-1}\frac{q-1}{m}} \bmod \mathfrak{P}_w\right) = \\ = (\mathrm{N}_{(\mathcal{O}_w/\mathfrak{P}_w)/\mathbb{F}}(f \bmod \mathfrak{P}_w))^{\frac{q-1}{m}} = f(\mathrm{div}(j))^{\frac{q-1}{m}},\end{aligned}$$

where the last equality in the first line follows from (b) in Theorem 3.80, gives the desired result. □

Corollary 4.60. *For all* $b \in J$ *and* $\zeta \in \mathbb{F}^*$ *one has*

$$(b,\zeta) = \left(\zeta^{\frac{q-1}{m}}\right)^{\deg b}.$$

Proof. Let $\mathrm{div}(b) = \sum_v n_v v$. Hence, we have $\deg b = \sum_v n_v d_v$. Using Theorem 4.59 we get

$$(b,\zeta) = (\zeta,b)^{-1} = \left(\prod_v \mathrm{N}_{(\mathcal{O}_v/\mathfrak{P}_v)/\mathbb{F}}\, \zeta^{n_v}\right)^{\frac{q-1}{m}} = \left(\zeta^{\sum_v n_v d_v}\right)^{\frac{q-1}{m}} = \left(\zeta^{\frac{q-1}{m}}\right)^{\deg b}.$$

□

Corollary 4.61. *The norm-residue symbol induces a perfect pairing*

$$(\cdot,\cdot) : \overline{J}/\overline{J^0} \times \overline{\mathbb{F}^*} \to \mu_m.$$

Proof. It follows from Corollary 4.60 and the short exact sequence 4.57 that the annihilator of $\overline{\mathbb{F}^*}$ in $\overline{J}$ is $\overline{J^0}$. □

Raising to the $(q-1)/m$-th power and the degree map give the isomorphisms

$$\overline{\mathbb{F}^*} \xrightarrow{\sim} \mu_m \quad \text{and} \quad \overline{J}/\overline{J^0} \xrightarrow{\sim} \mathbb{Z}/m\mathbb{Z},$$

respectively. Using these two isomorphisms, from the perfect pairing of Corollary 4.61 we get the perfect pairing

$$\begin{aligned}(\cdot,\cdot) : \mathbb{Z}/m\mathbb{Z} \times \mu_m &\to \mu_m,\\ (a,\zeta) &\to \zeta^a.\end{aligned}$$

The explicit description follows from Corollary 4.60.

Corollary 4.62. *The norm-residue symbol induces the perfect pairing*

$$(\cdot,\cdot)^{-1} : (\overline{K^*} \cap \overline{U})/\overline{\mathbb{F}^*} \times \overline{J^0}/(\overline{K^*} \cdot \overline{U}) \to \mu_m(\mathbb{F}). \tag{4.63}$$

Proof. Since the annihilator of $\overline{K^*} \cap \overline{U}$ is $\overline{K^*} \cdot \overline{U}$ and by Corollary 4.61 the annihilator of $\overline{J^0}$ is $\overline{\mathbb{F}^*}$, the pairing induced by the norm-residue symbol is perfect. □

Definition 4.64 (Divisor class groups)**.** Let $\mathbb{F}$ be a finite field, let K be a function field with exact field of constants $\mathbb{F}$, let Div_K and Div_K^0 be the group of divisors of K and the group of degree zero divisors of K, respectively, and let Pr_K be the group of principal divisors of K. The *divisor class group* Pic_K of K is the group $\mathrm{Div}_K \,/\, \mathrm{Pr}_K$ and the *divisor class group of degree zero divisors* Pic_k^0 is the group $\mathrm{Div}_K^0 \,/\, \mathrm{Pr}_K$.

The surjective map $\overline{K^*} \cap \overline{U} \to \mathrm{Pic}^0[m]$ that maps an element $a = uj^m$, with $a \in K^*$, $u \in U$, $j \in J$, to $\mathrm{div}(j)$ is well-defined by Lemma 4.51 and fits into the short exact sequence

$$1 \longrightarrow \overline{\mathbb{F}^*} \longrightarrow \overline{K^*} \cap \overline{U} \longrightarrow \mathrm{Pic}^0[m] \longrightarrow 0.$$

Hence, we have an isomorphism

$$(\overline{K^*} \cap \overline{U})/\overline{\mathbb{F}^*} \cong \mathrm{Pic}^0[m]. \tag{4.65}$$

Furthermore, from the exact sequence

$$1 \longrightarrow U \longrightarrow J^0 \xrightarrow{\text{div}} \text{Div}^0 \longrightarrow 0,$$

where Div^0 is the group of divisors of degree zero, we get an isomorphism

$$\overline{J^0}/(\overline{K^*} \cdot \overline{U}) \cong \text{Pic}^0/m\,\text{Pic}^0. \tag{4.66}$$

Corollary 4.67. *The norm-residue symbol induces the perfect pairing*

$$\begin{aligned} \{\cdot,\cdot\} : \text{Pic}^0[m] \times \text{Pic}^0/m\,\text{Pic}^0 &\to \mu_m(\mathbb{F}), \\ \{[D],[E] \bmod m\,\text{Pic}^0\} &\mapsto f(E)^{\frac{q-1}{m}}, \end{aligned}$$

where D and E are divisors with disjoint supports and $f \in K^*$ has divisor mD.

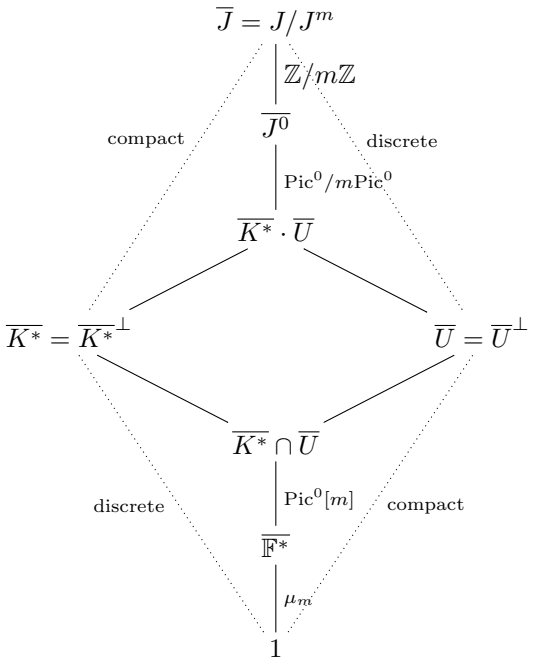
Proof. Combining isomorphisms 4.65 and 4.66 with the perfect pairing 4.63 gives the perfect pairing $\{\cdot,\cdot\} : \text{Pic}^0[m] \times \text{Pic}^0/m\,\text{Pic}^0 \to \mu_m(\mathbb{F})$.

Consider elements $[D] \in \text{Pic}^0[m]$ and $[E] \in \text{Pic}^0$ represented by divisors D and $E = \sum_v n_v v$ of K with disjoint supports. Let f be a nonzero rational function with divisor mD. By isomorphism 4.65 we can write f as ui^m with $u \in U$ and $i \in J$. Hence, we have $\text{div}(i) = D$. Moreover, by isomorphism 4.66 we can choose $j \in J^0$ with $\text{div}(j) = E$. Using Theorem 4.59 we get

$$\{[D],[E] \bmod m\,\text{Pic}^0\} = (f,j)^{-1} = f(\text{div}(j))^{\frac{q-1}{m}} = f(E)^{\frac{q-1}{m}}.$$

□

The present situation can be summarized in the following diagram.



Note that taking the annihilators reflects the diagram upside down.

4.6 The Tate pairing

The norm-residue symbol induces perfect pairings on subgroups and quotient groups of the group of ideles of a global field. Two very famous and commonly used pairings in the case of function fields are the Weil pairing and the Tate pairing. Hence, it is natural to look for relations between the norm-residue symbol and these pairings. In 1995, Howe [26] showed that Kummer theory and class field theory provide a way to obtain the Weil pairing from the norm-residue symbol. Here we show that the Tate pairing is given by the norm-residue symbol on certain groups of ideles and that it is even possible to extend this pairing to larger groups. The Tate pairing has been generalized by Bruin [8] to a pairing associated to an isogeny between abelian varieties over a finite field and it has been explicitly related to the Weil pairing.

The Tate pairing was constructed in 1994 by Frey and Rück [17] in order to reduce the discrete logarithm problem in the m-torsion part of the divisor class group of degree zero divisors on a projective irreducible nonsingular curve

over a finite field to the corresponding problem in the multiplicative group of the finite field. More recently it has been noticed by Boneh and Franklin that pairings can be used for identity-based cryptography [5]. Nowadays pairings are studied in some of the most active research fields in elliptic curve cryptography, but they are also of theoretical interest.

Definition 4.68 (Tate pairing)**.** Let K be a function field as in the previous section. Consider elements $[D] \in \mathrm{Pic}^0[m]$ and $[E] \in \mathrm{Pic}^0$ represented by divisors D and E of K with disjoint supports. Let f be a non-zero rational function with divisor mD. The *Tate pairing* of K is the map

$$\begin{aligned}\{\cdot,\cdot\} : \mathrm{Pic}^0[m] \times \mathrm{Pic}^0 / m\,\mathrm{Pic}^0 &\to \mu_m(\mathbb{F}),\\ \{[D], [E] \bmod m\,\mathrm{Pic}^0\} &\mapsto f(E)^{\frac{q-1}{m}},\end{aligned}$$

where

$$f(E) = \prod_v \mathrm{N}_{(\mathcal{O}_v/\mathfrak{P}_v)/\mathbb{F}}(f^{n_v} \bmod \mathfrak{P}_v) \text{ if } E = \sum_v n_v v.$$

Theorem 4.69. *The Tate pairing is a perfect pairing.*

Proof. The Tate pairing equals the pairing in Corollary 4.67. □

The proof by Frey and Rück uses a pairing introduced by Lichtenbaum [42], which comes from a duality result of Tate [70] on cohomology groups of an abelian variety. For this reason the Tate pairing is also called 'Tate–Lichtenbaum pairing' or 'Frey–Rück pairing'. Nowadays there are proofs by Hess [25] and by Schaefer [61] that do not use the results by Lichtenbaum and Tate.

Remark 4.70. If we consider the Tate pairing in the form of Corollary 4.62, the perfect pairing

$$(\cdot,\cdot)^{-1} : (\overline{K^*} \cap \overline{U}) \times \overline{J}/(\overline{K^*} \cdot \overline{U}) \to \mu_m(\mathbb{F})$$

in Theorem 4.59 is an extension of the Tate pairing to larger groups. In this way we increase the size of the groups involved by a factor of m. This might be useful for cryptographic applications. Note that the same formula still holds for this perfect pairing.

The group $\overline{J}/(\overline{K^*} \cdot \overline{U})$ has an interpretation in terms of groups of divisors similar to that of the group $\overline{J^0}/(\overline{K^*} \cdot \overline{U})$. From the short exact sequence

$$1 \longrightarrow U \longrightarrow J \xrightarrow{\mathrm{div}} \mathrm{Div} \longrightarrow 0$$

we get the isomorphism

$$\overline{J}/(\overline{K^*} \cdot \overline{U}) \cong \mathrm{Pic}\,/m\,\mathrm{Pic}\,.$$

4.7 The Arakelov class group

Given a number field K, we define the Arakelov class group of K. It is a group that is analogous to the divisor class group of degree zero divisors of a function field over a finite field. The main reference is [64] by Schoof.

Definition 4.71 (Group of Arakelov divisors)**.** Let K be a number field and let S and S_∞ be the sets of places of K and of Archimedean places of K, respectively. The *group of Arakelov divisors* Div_K of K is the set

$$\mathrm{Div}_K = \left\{ \sum_{v \in S \setminus S_\infty} n_v v + \sum_{v \in S_\infty} x_v v : n_v \in \mathbb{Z}, x_v \in \mathbb{R} \right\}$$

of finite formal sums with componentwise addition.

We will often write Div when the field K is understood.

The degree d_v of a non-Archimedean place v of K is $\log |\mathcal{O}_v/\mathfrak{P}_v|$, where $|\mathcal{O}_v/\mathfrak{P}_v|$ denotes the order of the residue field $\mathcal{O}_v/\mathfrak{P}_v$ of the completion K_v of K at v. The degree d_v of an Archimedean place v of K equals 1 or 2 depending on whether the place v is real or complex. The degree extends by linearity to the surjective group homomorphism

$$\begin{aligned} \deg : \mathrm{Div} &\to \mathbb{R} \\ \sum_{v \in S \setminus S_\infty} n_v v + \sum_{v \in S_\infty} x_v v &\mapsto \sum_{v \in S \setminus S_\infty} n_v d_v + \sum_{v \in S_\infty} x_v d_v, \end{aligned}$$

where d_v is the degree of the place v. The kernel of this map is the group of degree zero Arakelov divisors of K, which we denote by Div^0. There is a natural surjective continuous group homomorphism

$$\begin{aligned} \mathrm{div} : J &\to \mathrm{Div}, \\ j = (j_v)_v \mapsto \mathrm{div}(j) &= \sum_{v \in S \setminus S_\infty} \mathrm{v}_v(j_v) \cdot v + \sum_{v \in S_\infty} -\log |j_v| \cdot v, \end{aligned}$$

where the map $|\cdot| : \mathbb{C} \to \mathbb{R}_{\geq 0}$ is the ordinary absolute value and for each non-Archimedean place v of K the map $\mathrm{v}_v : K_v \to \mathbb{Z} \cup \{+\infty\}$ denotes the normalized valuation on K_v.

Definition 4.72 (Group of principal Arakelov divisors)**.** Let K be a number field. The *group of principal Arakelov divisors* Pr of K is the image of $K^* \subseteq J$ in Div under the map $\mathrm{div} : J \to \mathrm{Div}$.

Following the analogy to the function fields, we define Pic as the quotient group $\mathrm{Div} \,/\, \mathrm{Pr}$. For each $a \in K^*$ the principal Arakelov divisor $\mathrm{div}(a)$ is zero

if and only if a is a unit of $\mathcal{O}_K$ all of whose conjugates of a have absolute value equal to 1. Hence $\operatorname{div}(a)$ is zero if and only if a is contained in the group μ of roots of unity of K. We get the exact sequence

$$1 \to \mu \to K^* \xrightarrow{\operatorname{div}} \operatorname{Div} \to \operatorname{Pic} \to 0.$$

The product formula [Theorem 4.28] gives the inclusion $\operatorname{Pr} \subseteq \operatorname{Div}^0$.

Definition 4.73 (Arakelov class group)**.** Let K be a number field, let Div^0 be the group of degree zero Arakelov divisors of K, and let Pr be the group of principal Arakelov divisors of K. The *Arakelov class group* Pic^0 of K is the quotient group $\operatorname{Div}^0 / \operatorname{Pr}$.

Theorem 4.74. *Let K be a number field, let $(\bigoplus_{v\in S_\infty} \mathbb{R})^0$ be the subgroup of Arakelov divisors of K in $\bigoplus_{v\in S_\infty} \mathbb{R}$ that have degree zero, and let T^0 be the cokernel of the group homomorphism $\mathcal{O}_K^* \to (\bigoplus_{v\in S_\infty} \mathbb{R})^0$ obtained by composing the map $\operatorname{div} : \mathcal{O}_K \to \operatorname{Div}_K$ with the projection on the components corresponding to the Archimedean places of K. Then there is a group isomorphism*

$$T^0 \cong (\mathbb{R}/\mathbb{Z})^{|S_\infty|-1},$$

where S_∞ is the set of Archimedean place of K.

Proof. This follows from Dirichlet's unit theorem. □

Theorem 4.75. *Let K be a number field, let* Id *be the group of fractional ideals of its ring of integers, and let* Cl *be the ideal class group of K. Let* Div *be the group of Arakelov divisors of K, let* Pic^0 *be the Arakelov class group of K, and let T^0 be as in* Theorem 4.74*. For each non-Archimedean place v of K let $\mathfrak{P}_v$ be the prime ideal of the ring of integers of K associated to v. Then the group homomorphism*

$$\begin{aligned} \operatorname{Div} &\to \operatorname{Id} \\ \sum_{v\in S\setminus S_\infty} n_v v + \sum_{v\in S_\infty} x_v v &\mapsto \prod_{v\in S\setminus S_\infty} \mathfrak{P}_v^{-n_v} \end{aligned}$$

induces a natural split short exact sequence

$$0 \to T^0 \to \operatorname{Pic}^0 \to \operatorname{Cl} \to 1.$$

Proof. See Proposition 2.2 in [64] by Schoof. □

Corollary 4.76. *Let m be a positive integer and let K be a number field. Let* Cl *and* Pic^0 *be the ideal class group of K and the Arakelov class group of K, respectively. Then the exact sequence in* Theorem 4.75 *induces a group isomorphism*

$$\operatorname{Pic}^0 / m \operatorname{Pic}^0 \xrightarrow{\sim} \operatorname{Cl} / \operatorname{Cl}^m .$$

Proof. Since by Theorem 4.74 the group T^0 is divisible, the results follows from the split short exact sequence in Theorem 4.75. □

Composing the map $\mathrm{div} : J \to \mathrm{Div}$ with the degree map $\deg : \mathrm{Div} \to \mathbb{R}$ we obtain the map $-\log \circ c : J \to \mathbb{R}$, where $c : J \to \mathbb{R}$, $j = (j_v)_v \mapsto \prod_v |j_v|_v$, is the content map. This composite map gives rise to the split short exact sequence

$$1 \to J^0 \to J \xrightarrow{\deg \circ \mathrm{div}} \mathbb{R} \to 0, \tag{4.77}$$

where J^0 is the group of ideles of K of degree zero, which is also the kernel of the content map. The splitting of this exact sequence follows from the splitting of the exact sequence 4.26.

Let U' be the kernel of the map $\mathrm{div} : J \to \mathrm{Div}$. Hence U' is the group

$$U' = \prod_{v \in S} \ker(|\cdot|_v) = \{(j_v)_v \in J : \forall v \in S : |j_v|_v = 1\}.$$

From the short exact sequence

$$1 \to U' \to J^0 \xrightarrow{\mathrm{div}} \mathrm{Div}^0 \to 0$$

we get a group isomorphism

$$J^0/(K^* \cdot U') \xrightarrow{\sim} \mathrm{Pic}^0\,. \tag{4.78}$$

Let m be a positive integer. Now we assume that K contains a primitive m-th root of unity. Let $\overline{} : J \to J/J^m$ be the canonical projection of J onto J/J^m. Given a subgroup A of J we will write $\overline{A}$ for the group $(A \cdot J^m)/J^m$. Note that we have the equality $\overline{U'} = \overline{U}$, where U is the group of unit ideles of K. Combining the split exact sequence 4.77 and the group isomorphism 4.78 gives a group isomorphism

$$\overline{J}/(\overline{K^*} \cdot \overline{U}) \xrightarrow{\sim} \mathrm{Pic}^0/m\,\mathrm{Pic}^0.$$

The surjective map $\overline{K^*} \cap \overline{U'} \to \mathrm{Pic}^0[m]$ that maps an element $a = uj^m$, with $a \in K^*$, $u \in U'$, $j \in J$, to $\mathrm{div}(j)$ fits into the short exact sequence

$$1 \longrightarrow \overline{\mu} \longrightarrow \overline{K^*} \cap \overline{U'} \longrightarrow \mathrm{Pic}^0[m] \longrightarrow 0. \tag{4.79}$$

Hence, we get an isomorphism

$$(\overline{K^*} \cap \overline{U})/\overline{\mu} \xrightarrow{\sim} \mathrm{Pic}^0[m].$$

4.8 Number fields

Given a positive integer m and a number field K containing a primitive m-th root of unity, we reproduce the construction of the Tate pairing in this setting. Using the norm-residue symbol we define some natural pairings on subgroups and quotient groups of J/J^m, where J denotes the group of ideles of K. These pairings do not deviate much from a naturally defined perfect pairing $\mathrm{Cl}[m] \times \mathrm{Cl}\,/\,\mathrm{Cl}^m \to \mu_m$, where Cl is the ideal class group of K and μ_m is the group of m-th roots of unity in K. The m-th virtual group V of K [Definition 5.15], which is a subgroup of the m-th unit residue group of K [Definition 5.3], provides an upper bound for this deviation, which is mathematically expressed by Theorem 4.84 and Theorem 4.86.

Notation 4.80. Let m be a positive integer and let K be a number field containing a primitive m-th root of unity ζ_m, which generates the multiplicative group μ_m. The ring of integers of K, its group of units, the set of places of K, and the set of Archimedean places of K are $\mathcal{O}_K$, E, S, and S_∞, respectively. For a place v of K, we denote by K_v the completion of K at v, by $\mathcal{O}_v$ the ring of integers of K_v, and by U_v the unit group of $\mathcal{O}_v$ if v is non-Archimedean and K_v^* if v is Archimedean. Let Cl and Pic^0 be the ideal class group of K and the Arakelov class group of K, respectively.

We denote the group of ideles of K by J and the unit idele group of K by U. For definitions see Definition 4.19 and Definition 4.21. Let $\overline{} : J \to J/J^m$ be the canonical projection of J onto J/J^m. Given a subgroup A of J, we write $\overline{A}$ for the group $(A \cdot J^m)/J^m$. For any subgroup $H \subseteq \overline{J}$ we denote by $H^\perp$ its annihilator in $\overline{J}$ with respect to the norm-residue symbol $(\cdot,\cdot) : \overline{J} \times \overline{J} \to \mu_m$. Let V be the subgroup

$$V = (\overline{K^*} \cap \overline{U}) \cdot \overline{U}^\perp / \overline{U}^\perp$$

of the m-th unit residue group $\overline{U}/\overline{U}^\perp$ of K. It will be called the 'm-th virtual group' of K [Definition 5.15].

Similarly to the function fields case, we have two short exact sequences

$$1 \longrightarrow U \cdot K^* \longrightarrow J \longrightarrow \mathrm{Cl} \longrightarrow 1 \tag{4.81}$$

and

$$1 \longrightarrow \overline{E} \longrightarrow \overline{K^*} \cap \overline{U} \longrightarrow \mathrm{Cl}[m] \longrightarrow 1. \tag{4.82}$$

Let G be the group of automorphisms of K over $\mathbb{Q}$. We also remark that the two sequences are G-linear.

We consider the pairing $(\cdot,\cdot) : \overline{J} \times \overline{J} \to \mu_m$ induced by the norm-residue symbol in Theorem 4.49. The annihilator of $\overline{K^*}$ in $\overline{J}$ is $\overline{K^*}$ itself but, differently

from the function field case, the annihilator $\overline{U}^{\perp}$ of $\overline{U}$ in $\overline{J}$ is not $\overline{U}$. This is due to the presence of ramified places and Archimedean places. By Theorem 3.89 and by Section 3.7 we only have the inclusion $\overline{U}^{\perp} \subset \overline{U}$. See Theorem 5.1 for more details. We will call the quotient group $\overline{U}/\overline{U}^{\perp}$ the 'm-th unit residue group' of K [Definition 5.3].

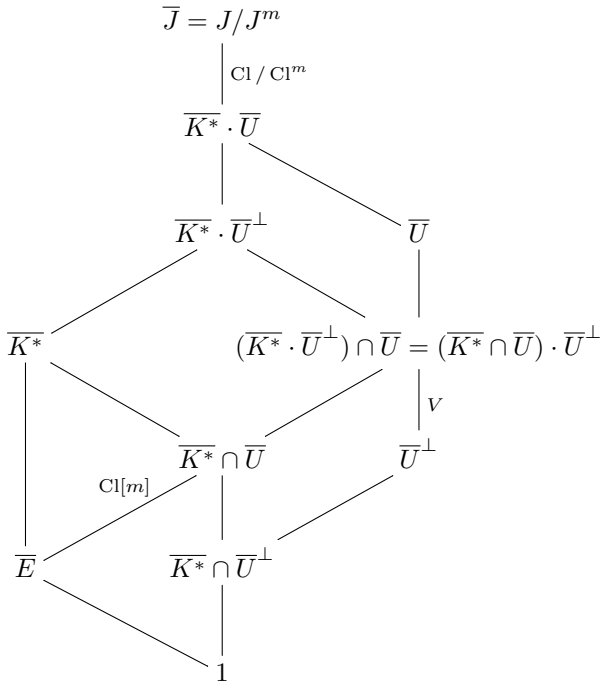
Theorem 4.83. *Let the notation be as in* Notation 4.80. *Then one has the equality*

$$(\overline{K^*} \cdot \overline{U}^{\perp}) \cap \overline{U} = (\overline{K^*} \cap \overline{U}) \cdot \overline{U}^{\perp}.$$

Proof. Since by Theorem 5.1 we have the inclusion $\overline{U}^{\perp} \subset \overline{U}$, we get

$$(\overline{K^*} \cdot \overline{U}^{\perp}) \cap \overline{U} = (\overline{K^*} \cap \overline{U}) \cdot (\overline{U}^{\perp} \cap \overline{U}) = (\overline{K^*} \cap \overline{U}) \cdot \overline{U}^{\perp}. \qquad \square$$

The following diagram summarizes the situation.



Theorem 4.84. *Let the notation be as in* Notation 4.80. *Then one has the following.*

(a) *The norm-residue symbol induces a perfect pairing of finite abelian groups*

$$(\cdot, \cdot) : (\overline{K^*} \cap \overline{U}) \times \overline{J}/(\overline{K^*} \cdot \overline{U}^{\perp}) \to \mu_m.$$

(b) *The short exact sequences* 4.82 *and* 4.81 *induce surjective canonical group homomorphisms*

$$\varphi_1 : \overline{K^*} \cap \overline{U} \twoheadrightarrow \mathrm{Cl}[m]$$
$$\varphi_2 : \overline{J}/(\overline{K^*} \cdot \overline{U}^{\perp}) \twoheadrightarrow \mathrm{Cl}\,/\,\mathrm{Cl}^m$$

such that

$$\ker \varphi_1 \cong (\mathbb{Z}/m\mathbb{Z})^{|S_\infty|} \quad \textit{and} \quad \ker \varphi_2 \cong V \textit{ with } |V| = m^{|S_\infty|}.$$

Proof. Since the annihilator of $\overline{K^*} \cap \overline{U}$ with respect to the norm-residue symbol is $\overline{K^*} \cdot \overline{U}^{\perp}$, the norm-residue symbol induces a perfect pairing

$$(\cdot,\cdot) : (\overline{K^*} \cap \overline{U}) \times \overline{J}/(\overline{K^*} \cdot \overline{U}^{\perp}) \to \mu_m.$$

The surjective canonical group homomorphism $\varphi_1 : \overline{K^*} \cap \overline{U} \twoheadrightarrow \mathrm{Cl}[m]$ is given by the short exact sequence (4.82). By Dirichlet's unit theorem we have $\overline{E} \cong (\mathbb{Z}/m\mathbb{Z})^{|S_\infty|}$ and therefore $\ker \varphi_1 \cong (\mathbb{Z}/m\mathbb{Z})^{|S_\infty|}$. The surjective canonical group homomorphism $\varphi_2 : \overline{J}/(\overline{K^*} \cdot \overline{U}^{\perp}) \twoheadrightarrow \mathrm{Cl}\,/\,\mathrm{Cl}^m$ follows from the short exact sequence (4.81) and we have $\ker \varphi_2 = (\overline{K^*} \cdot \overline{U})/(\overline{K^*} \cdot \overline{U}^{\perp})$. By duality and the second group isomorphism theorem we get

$$(\overline{K^*} \cdot \overline{U})/(\overline{K^*} \cdot \overline{U}^{\perp}) \cong (\overline{K^*} \cap \overline{U})/(\overline{K^*} \cap \overline{U}^{\perp}) \cong V.$$

Since we have

$$|\,\mathrm{Cl}[m]| \cdot |\overline{E}| = |\overline{K^*} \cap \overline{U}| = |\overline{K^*} \cap \overline{U}^{\perp}| \cdot |V| = |\overline{J}/(\overline{K^*} \cdot \overline{U})| \cdot |V| = |\,\mathrm{Cl}\,/\,\mathrm{Cl}^m\,| \cdot |V|,$$

the equality $|V| = m^{|S_\infty|}$ follows. □

Theorem 4.85. *Let the notation be as in* Notation 4.80. *Then one has the following.*

(a) *The norm-residue symbol induces a perfect pairing of finite abelian groups*

$$(\cdot,\cdot) : (\overline{K^*} \cap \overline{U}) \times \overline{J}/(\overline{K^*} \cdot \overline{U}^{\perp}) \to \mu_m.$$

(b) *The short exact sequences* 4.79 *and* 4.81 *induce surjective canonical group homomorphisms*

$$\varphi_1 : \overline{K^*} \cap \overline{U} \twoheadrightarrow \mathrm{Pic}^0[m]$$
$$\varphi_2 : \overline{J}/(\overline{K^*} \cdot \overline{U}^{\perp}) \twoheadrightarrow \mathrm{Pic}^0/m\,\mathrm{Pic}^0$$

such that

$$\ker \varphi_1 \cong \mathbb{Z}/m\mathbb{Z} \quad \textit{and} \quad \ker \varphi_2 \cong V \textit{ with } |V| = m^{|S_\infty|}.$$

Proof. By Theorem 4.84 the norm-residue symbol induces a perfect pairing

$$(\cdot,\cdot) : (\overline{K^*} \cap \overline{U}) \times \overline{J}/(\overline{K^*} \cdot \overline{U}^{\perp}) \to \mu_m.$$

The surjective canonical group homomorphism $\varphi_1 : \overline{K^*} \cap \overline{U} \twoheadrightarrow \mathrm{Pic}^0[m]$ is given by the short exact sequence (4.79). We have $\ker \varphi_1 \cong \mathbb{Z}/m\mathbb{Z}$, because K contains a primitive m-th root of unity. By Corollary 4.76 the surjective canonical group homomorphism $\varphi_2 : \overline{J}/(\overline{K^*} \cdot \overline{U}^{\perp}) \twoheadrightarrow \mathrm{Pic}^0/m\,\mathrm{Pic}^0$ is obtained from the surjective canonical group homomorphism $\varphi_2 : \overline{J}/(\overline{K^*} \cdot \overline{U}^{\perp}) \twoheadrightarrow \mathrm{Cl}\,/\,\mathrm{Cl}^m$ in Theorem 4.84. □

Theorem 4.86. *Let the notation be as in* Notation 4.80. *Then there are canonical subgroups* $A \subseteq \mathrm{Cl}\,/\,\mathrm{Cl}^m$ *and* $B \subseteq \mathrm{Cl}[m]$ *with the following properties.*

(a) *The norm-residue symbol induces a perfect pairing of finite abelian groups*

$$(\cdot,\cdot) : A \times B \to \mu_m.$$

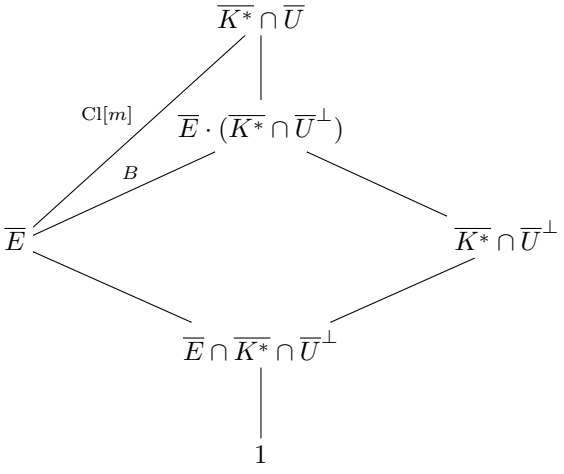
(b) *There are surjective group homomorphisms*

$$(\mathbb{Z}/m\mathbb{Z})^{|S_\infty|} \twoheadrightarrow (\mathrm{Cl}\,/\,\mathrm{Cl}^m)/A,$$
$$V \twoheadrightarrow \mathrm{Cl}[m]/B \text{ with } |V| = m^{|S_\infty|}.$$

Proof. Let B be the group $\overline{E} \cdot (\overline{K^*} \cap \overline{U}^{\perp})/\overline{E}$. By the second group isomorphism theorem we get

$$B \cong (\overline{K^*} \cap \overline{U}^{\perp})/(\overline{K^*} \cap \overline{U}^{\perp} \cap \overline{E}).$$

The situation is visualized in the following diagram.



Since the annihilator of $\overline{K^*} \cap \overline{U}^{\perp}$ with respect to the norm-residue symbol is $\overline{K^*} \cdot \overline{U}$, the norm-residue symbol induces a perfect pairing

$$(\cdot, \cdot) : J/(\overline{K^*} \cdot \overline{U}) \times (\overline{K^*} \cap \overline{U}^{\perp}) \to \mu_m.$$

Let A be the annihilator in $\overline{J}/(\overline{K^*} \cdot \overline{U})$ of $\overline{E} \cap \overline{K^*} \cap \overline{U}^{\perp}$ with respect to the induced pairing. The norm-residue symbol induces a perfect pairing

$$(\cdot, \cdot) : A \times B \to \mu_m.$$

Using the inclusions

$$A \hookrightarrow \overline{J}/(\overline{K^*} \cdot \overline{U}) \cong \mathrm{Cl} \,/\, \mathrm{Cl}^m$$

and

$$B \hookrightarrow (\overline{K^*} \cap \overline{U})/\overline{E} \cong \mathrm{Cl}[m]$$

we may consider A and B as subgroups of $\mathrm{Cl} \,/\, \mathrm{Cl}^m$ and $\mathrm{Cl}[m]$, respectively.

By Dirichlet's unit theorem we get a group isomorphism $\overline{E} \cong (\mathbb{Z}/m\mathbb{Z})^{|S_\infty|}$. Since by duality we have a group isomorphism

$$(\mathrm{Cl} \,/\, \mathrm{Cl}^m)/A \cong \overline{E} \cap \overline{K^*} \cap \overline{U}^{\perp},$$

the existence of a surjective homomorphism

$$(\mathbb{Z}/m\mathbb{Z})^{|S_\infty|} \twoheadrightarrow (\mathrm{Cl} \,/\, \mathrm{Cl}^m)/A$$

follows from the inclusion $\overline{E} \cap \overline{K^*} \cap \overline{U}^{\perp} \hookrightarrow \overline{E}$.

By the second group isomorphism theorem we get a group isomorphism

$$V = ((\overline{K^*} \cap \overline{U}) \cdot \overline{U}^{\perp})/\overline{U}^{\perp} \cong (\overline{K^*} \cap \overline{U})/(\overline{K^*} \cap \overline{U}^{\perp}).$$

This group maps surjectively to

$$(\overline{K^*} \cap \overline{U})/(\overline{E} \cdot (\overline{K^*} \cap \overline{U}^{\perp})) \cong \mathrm{Cl}[m]/B,$$

as required.

For a proof of the equality $|V| = m^{|S_\infty|}$ see Theorem 4.84. □

CHAPTER 5

The unit residue group

Given a positive integer m and a global field K containing a primitive m-th root of unity, we define the m-th unit residue group of K [Definition 5.3]. Corollary 5.2 shows that it is a skew abelian group, where the pairing is given by the m-th power norm-residue symbol. We refer to Chapter 2 for definitions and results on skew abelian groups. The m-th unit residue group is isomorphic to an orthogonal sum of skew abelian groups that are defined locally at the wild non-Archimedean places of K and at the real Archimedean places of K [Theorem 5.6]. Hence, it is the trivial group when K is a function field. This result is strongly related to the existence of the Tate pairing, as we will explain later in this introduction. As an abelian group, the m-th unit residue group of K is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^{2\cdot|S_\infty|}$, where S_∞ denotes the set of Archimedean places of K [Theorem 5.10].

The structure of the m-th unit residue group as an orthogonal sum of local components [Theorem 5.1] is reminiscent of the structure of the group $\overline{J} = J/J^m$ with respect to the pairing induced by the idelic m-th power norm-residue symbol, where J is the group of ideles of K. The group $\overline{J}$ has the subgroup $\overline{K^*} = (K^* \cdot J^m)/J^m$, which we can consider as the global contribution to $\overline{J}$. We could say that it lies halfway in $\overline{J}$, because $\overline{K^*}$ is its own annihilator in $\overline{J}$ with respect to the pairing induced by the idelic m-th power norm-residue symbol [Theorem 4.52]. The m-th unit residue group of K has a similar subgroup: the m-th virtual group of K [Definition 5.15]. The m-th virtual group is defined globally and is a maximal self-annihilating subgroup of the m-th unit residue group, of order $m^{|S_\infty|}$ [Theorem 5.17]. In particular,

its order equals its index in the m-th unit residue group. We remark that the m-th virtual group is not necessarily isomorphic, as an abelian group, to $(\mathbb{Z}/m\mathbb{Z})^{|S_\infty|}$ [Theorem 6.31].

The m-th virtual group naturally arises when one tries to extend the Tate pairing to number fields. It provides an upper bound for how far the groups $\mathrm{Cl}[m]$ and $\mathrm{Cl}\,/\,\mathrm{Cl}^m$ are from having a similar canonically defined perfect pairing $\mathrm{Cl}[m] \times \mathrm{Cl}\,/\,\mathrm{Cl}^m \to \mu_m$, where Cl is the ideal class group of K and μ_m is the group of m-th roots of unity in K [Theorem 4.84 and Theorem 4.86]. Note that this bound can be very small even for large ideal class groups, because the m-th virtual group has order $m^{|S_\infty|}$. For example, the 2-nd virtual group of any imaginary quadratic number field has order 2.

We want to describe the m-th virtual group in a more explicit way that is amenable to computation. Remark 5.28 gives a natural surjective group homomorphism from the m-Selmer group of K [Definition 5.25] to the m-th virtual group and links the m-th virtual group to the field extensions of K that are obtained by adjoining m-th roots of m-virtual units of K, which are the elements in K that have normalized valuation divisible by m at every place of K. These extensions can ramify only at the wild non-Archimedean places of K and at the real Archimedean places of K.

In this chapter we present definitions and general results on unit residue groups and virtual groups. As a first example we compute the 2-nd unit residue group of the field $\mathbb{Q}$ of rational numbers by identifying its local components and, in there, the 2-nd virtual group of $\mathbb{Q}$ [Theorem 5.32]. In later chapters we will compute unit residue groups of other number fields.

5.1 Definitions and general results

Theorem 5.1. *Let the notation be as in* Notation 4.80. *Then the subgroup $\overline{U}$ of J/J^m contains its own annihilator $\overline{U}^\perp$ in J/J^m with respect to the norm-residue symbol and the projection $\overline{} : J \to J/J^m$ induces a group isomorphism of finite abelian groups*

$$\prod_{v|m} U_v/U_v^\perp \times \prod_{v \text{ real}} U_v/U_v^\perp \xrightarrow{\sim} \overline{U}/\overline{U}^\perp,$$

where v ranges over the places of K dividing m and the real Archimedean places of K.

Proof. Let S be the set of places of K. By Remark 4.22 we get the equality

$$\overline{U} = \prod_{v \in S} U_v/U_v^m.$$

Section 3.7 and Theorem 3.89 imply that for every place $v \in S$ the group U_v/U_v^m contains its own annihilator in $K_v^*/(K_v^*)^m$ with respect to the local norm-residue symbol. Hence, we obtain the inclusion

$$\overline{U}^{\perp} \subseteq \overline{U}.$$

By Corollary 3.90 for non-Archimedean places and by Section 3.7 for Archimedean places, for each place $v \in S$ we have the equality $(U_v/U_v^m)^{\perp} = U_v^{\perp}/U_v^m$. Hence, we get a group isomorphism

$$\prod_{v \in S} U_v/U_v^{\perp} \xrightarrow{\sim} \overline{U}/\overline{U}^{\perp}.$$

Theorem 3.89 implies that for each non-Archimedean place $v \in S$ the group $U_v/U_v^{\perp}$ has order $|m|^{-1}$ and therefore is trivial for all but the finitely many places dividing m. By Section 3.7 for each Archimedean place $v \in S$ the group $U_v/U_v^{\perp}$ has order dividing 2 and is trivial when v is complex. Hence, the group $\overline{U}/\overline{U}^{\perp}$ is finite and the group isomorphism in the statement follows. □

Corollary 5.2. *Let the notation be as in* Notation 4.80. *Then the triple* $(\overline{U}/\overline{U}^{\perp}, (\cdot,\cdot)_{K,m}, \mu_m)$ *is a skew abelian group.*

Proof. The result follows from Theorem 4.49 and Theorem 5.1. □

Definition 5.3 (m-th unit residue group)**.** Let m be a positive integer, let K be a global field containing a primitive m-th root of unity, and let μ_m be the group of m-th roots of unity in K. Let J be the group of ideles of K and let U be the group of unit ideles of K. Denote by $\overline{U}$ the group UJ^m/J^m and let $\overline{U}^{\perp}$ be the annihilator of $\overline{U}$ in J/J^m with respect to pairing $J/J^m \times J/J^m \to \mu_m$ induced the idelic m-th power norm-residue symbol. Let $(\cdot,\cdot)_{K,m} : \overline{U}/\overline{U}^{\perp} \times \overline{U}/\overline{U}^{\perp} \to \mu_m$ be the pairing induced by the idelic m-th power norm-residue symbol. The *m-th unit residue group* of the global field K is the skew abelian group $(\overline{U}/\overline{U}^{\perp}, \mu_m, (\cdot,\cdot)_{K,m})$.

We will write only 'unit residue group' when m is understood.

Theorem 5.4. *Let m be a positive integer, let K be a global field containing a primitive m-th root of unity, and let $(\overline{U}/\overline{U}^{\perp}, \mu_m, (\cdot,\cdot)_{K,m})$ be the m-th unit residue group of K. The skew element of the m-th unit residue group of K is $\overline{-1} \cdot \overline{U}^{\perp}$.*

Proof. Let $(a_v)_v \in U$. By Corollary 3.75 for each place v of K we have

$$(-1, a_v)_v = (a_v, a_v)_v .$$

Taking the product over all places of K concludes the proof. □

Theorem 5.5. *Let m be a positive integer and let K be a global field containing a primitive m-th root of unity. Then the following are equivalent.*
(i) *The m-th unit residue group of K is a symplectic abelian group.*
(ii) *The extension $K(\sqrt[m]{-1})/K$ is unramified at all places of K.*

Proof. By Theorem 5.4 the skew element of the m-th unit residue group of K is $-1\cdot\overline{U}^{\perp}$. Now the equivalence follows from Theorem 2.15 and Theorem 3.86. □

Theorem 5.6. *Let the notation be as in* Notation 4.80. *Then the group isomorphism*

$$\prod_{v|m} U_v/U_v^{\perp} \times \prod_{v \text{ real}} U_v/U_v^{\perp} \xrightarrow{\sim} \overline{U}/\overline{U}^{\perp}$$

induced by the canonical projection $J \to J/J^m$ is an isomorphism

$$\bigsqcup_{v\in S_m} (U_v/U_v^{\perp}, \mu_m, (\cdot,\cdot)_{K_v,m}) \xrightarrow{\sim} (\overline{U}/\overline{U}^{\perp}, \mu_m, (\cdot,\cdot)_{K,m})$$

of skew abelian groups, where S_m denotes the set of the places of K dividing m and the real Archimedean places of K.

Proof. The result follows from the definition of the global norm-residue symbol as the product of all local norm-residue symbols. □

Theorem 5.7. *Let the notation be as in* Notation 4.80 *and let the triple $(\overline{U}/\overline{U}^{\perp}, \mu_m, (\cdot,\cdot)_{K,m})$ be the m-th unit residue group of K. For each prime p dividing m let $n_p = p^{\mathrm{v}_p(m)}$ and let $(\overline{U_p}/\overline{U_p}^{\perp}, \mu_{n_p}, (\cdot,\cdot)_{K,n_p})$ be the n_p-th unit residue group of K. Then the projection*

$$J/J^m \to \bigoplus_{p|m} J/J^{n_p}$$

induces a group isomorphism

$$\varphi : \overline{U}/\overline{U}^{\perp} \xrightarrow{\sim} \bigoplus_{p|m} \overline{U_p}/\overline{U_p}^{\perp},$$

which is an isomorphism

$$(\overline{U}/\overline{U}^{\perp}, \mu_m, (\cdot,\cdot)_{K,m}) \xrightarrow{\sim} \bigsqcup_{p|m} (\overline{U_p}/\overline{U_p}^{\perp}, \mu_{n_p}, (\cdot,\cdot)_{K,n_p})$$

of skew abelian groups, where for each $p \mid m$ the injective group homomorphism used in defining the orthogonal sum is $\psi_p : \mu_{n_p} \to \mu_m$, $\zeta \mapsto \zeta^{m/n_p}$.

Proof. Theorem 5.1 and Corollary 3.93 imply that φ is a group isomorphism. Using the orthogonal sum in Theorem 5.6 and the similarity in Corollary 3.93 we conclude that φ is also an isomorphism of skew abelian groups. □

Remark 5.8. Theorem 5.7 implies that the structure of the m-th unit residue group can be determined by only studying the cases when m is a prime power.

Lemma 5.9. *Let p be a prime, let n be a positive integer, and let $m = p^n$. Let K be a number field containing a primitive m-th root of unity and let μ_m be the group of m-th roots of unity in K. For each place v of K above p, let U_v be the unit group of the ring of integers of the completion K_v of K at v and let $U_v^\perp$ be the annihilator in U_v of U_v with respect to the norm-residue symbol $(\cdot,\cdot)_{K_v,m} : K_v^* \times K_v^* \to \mu_m$. Then there is a group isomorphism*

$$\prod_{v|m} U_v/U_v^\perp \xrightarrow{\sim} (\mathbb{Z}/m\mathbb{Z})^{[K:\mathbb{Q}]}.$$

Proof. By Corollary 3.91 for each place v of K above p we have a group isomorphism

$$U_v/U_v^\perp \xrightarrow{\sim} (\mathbb{Z}/m\mathbb{Z})^{[K_v:\mathbb{Q}_p]}.$$

Since the sum of the local degrees

$$\sum_{v|p} [K_v : \mathbb{Q}_p] = [K : \mathbb{Q}]$$

equals the global degree, the desired group isomorphism follows. □

Theorem 5.10. *Let m be a positive integer, let K be a number field containing a primitive m-th root of unity, let S_∞ be the set of Archimedean places of K, and let $(\overline{U}/\overline{U}^\perp, \mu_m, (\cdot,\cdot)_{K,m})$ be the m-th unit residue group of K. Then there is a group isomorphism*

$$\overline{U}/\overline{U}^\perp \xrightarrow{\sim} (\mathbb{Z}/m\mathbb{Z})^{2\cdot|S_\infty|}.$$

Proof. The case $m = 1$ is trivial. By Theorem 5.7 we may suppose that m is a prime power. Let p be a prime and n be a positive integer satisfying $m = p^n$. Because of the group isomorphism

$$\prod_{v|m} U_v/U_v^\perp \times \prod_{v \text{ real}} U_v/U_v^\perp \xrightarrow{\sim} \overline{U}/\overline{U}^\perp,$$

in Theorem 5.1, we can combine the results we have locally. Lemma 5.9 gives a group isomorphism

$$\prod_{v|m} U_v/U_v^\perp \xrightarrow{\sim} (\mathbb{Z}/m\mathbb{Z})^{[K:\mathbb{Q}]}.$$

Firstly, we suppose $m > 2$. In this case there are no real places and therefore we have $[K : \mathbb{Q}] = 2 \cdot |S_\infty|$. The desired group isomorphism follows.

Now we consider the case $m = 2$. Let r_1 and r_2 be the numbers of real and complex places of K, respectively. By Section 3.7 for each real place v of K we have a group isomorphism $U_v/U_v^\perp \xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z}$. Hence, we get a group isomorphism

$$\overline{U}/\overline{U}^\perp \xrightarrow{\sim} (\mathbb{Z}/2\mathbb{Z})^{[K:\mathbb{Q}]} \times (\mathbb{Z}/2\mathbb{Z})^{r_1}.$$

Since we have $[K : \mathbb{Q}] = r_1 + 2r_2$, we obtain again

$$\overline{U}/\overline{U}^\perp \xrightarrow{\sim} (\mathbb{Z}/m\mathbb{Z})^{2\cdot|S_\infty|}. \qquad \square$$

We classify the m-th unit residue group as a skew abelian group.

Theorem 5.11. *Let m be a positive integer and let K be a number field containing a primitive m-th root of unity. Then the m-th unit residue group is a skew abelian group of even 2-rank and its class in* Theorem 2.28 *is the class of the pair $((\mathbb{Z}/m\mathbb{Z})^{|S_\infty|}, g)$, where g is the zero element if the extension $K(\sqrt[m]{-1})/K$ is unramified at all places of K and is any element of order 2 otherwise.*

Proof. By Theorem 5.10 the 2-rank of the m-th unit residue group is even. Theorem 5.5 and Remark 2.32 imply that the class of the m-th unit residue group in Theorem 2.28 is the class of the pair $((\mathbb{Z}/m\mathbb{Z})^{|S_\infty|}, 0)$ if the extension $K(\sqrt[m]{-1})/K$ is unramified at all places of K. Since the m-th unit residue group is a free $\mathbb{Z}/m\mathbb{Z}$-module, all nonzero elements in $(\mathbb{Z}/m\mathbb{Z})^{|S_\infty|}[2]$ have the same 2-height. Using Lemma 2.30 concludes the proof. $\square$

Theorem 5.12. *Let p be a prime, let n be a positive integer, and let $m = p^n$. Let K be a number field containing a primitive m-th root of unity, let $\mathcal{O}_K$ be its ring of integers, let μ_m be the group of m-th roots of unity in K, let ζ_p be a primitive p-th root of unity in K, and let $\lambda = 1 - \zeta_p$. For each place v of K above p, let U_v be the unit group of the ring of integers of the completion K_v of K at v and let $U_v^\perp$ be the annihilator in U_v of U_v with respect to the norm-residue symbol $(\cdot,\cdot)_{K_v,m} : K_v^* \times K_v^* \to \mu_m$. Then there is a surjective group homomorphism*

$$\varphi : (\mathcal{O}_K/p^n\lambda\mathcal{O}_K)^*/(\mathcal{O}_K/p^n\lambda\mathcal{O}_K)^{*m} \twoheadrightarrow \prod_{v|p} U_v/U_v^\perp$$

that is characterized by (a) *and also has the properties* (b), (c), *and* (d).

(a) *For each $a \in \mathcal{O}_K$ coprime to p one has*

$$(a + p^n\lambda\mathcal{O}_K) \cdot (\mathcal{O}_K/p^n\lambda\mathcal{O}_K)^{*m} \overset{\varphi}{\mapsto} (aU_v^\perp)_v.$$

(b) *For each $a \in \mathcal{O}_K$ coprime to p the following are equivalent.*
(i) *The extension $K(\sqrt[m]{a})/K$ is unramified at all places of K above p.*
(ii) *The element $(a + p^n\lambda\mathcal{O}_K) \cdot (\mathcal{O}_K/p^n\lambda\mathcal{O}_K)^{*m}$ is in* $\ker\varphi$.
(c) *There is a group isomorphism*

$$\ker\varphi \cong \bigoplus_{v|p} \mathbb{Z}/p^{n-1}\mathbb{Z}.$$

(d) *If one has $n > 1$, then for each $a \in \mathcal{O}_K$ coprime to p the following are equivalent.*
(i) *The extension $K(\sqrt[m]{a})/K$ is unramified at all places of K above p and there is a place v of K above p such that the extension $K_v(\sqrt[m]{a})/K_v$ is unramified of degree m.*
(ii) *The element $(a+p^n\lambda\mathcal{O}_K)\cdot(\mathcal{O}_K/p^n\lambda\mathcal{O}_K)^{*m}$ is in* $\ker\varphi$ *and has order p^{n-1}.*

Proof. Theorem 3.86 and Lemma 3.98 imply that the group homomorphism φ is well-defined, is characterized by (a), and has the property (b). It is surjective by the weak approximation theorem. By the Chinese remainder theorem it induces for each place v of K the map

$$\begin{aligned}\varphi_v : (\mathcal{O}_K/\mathfrak{P}_v^t)^*/(\mathcal{O}_K/\mathfrak{P}_v^t)^{*m} &\twoheadrightarrow U_v/U_v^{\perp},\\ (a + \mathfrak{P}_v^t) \cdot (\mathcal{O}_K/\mathfrak{P}_v^t)^{*m} &\mapsto aU_v^{\perp},\end{aligned}$$

where $\mathfrak{P}_v$ is the prime ideal of $\mathcal{O}_K$ associated to v and t is the normalized valuation on K_v of $p^n\lambda$, and is uniquely determined by the set $\{\varphi_v : v \mid p\}$ of maps. Hence, to prove (c) and (d), it suffices to prove that for each place v of K above p the kernel of the map φ_v is isomorphic to the cyclic group $\mathbb{Z}/p^{n-1}\mathbb{Z}$ and, if one has $n > 1$, then being a generator of this kernel is equivalent to having an m-th root that gives an unramified extension of K_v of degree m.

Now we fix a place v of K above p. Let $U^{(1)}$ be the first higher unit group of the ring of integers $\mathcal{O}_v$ of K_v. Note that the inclusion $U^{(1)} \hookrightarrow U_v$ induces a group isomorphism $U^{(1)}/{U^{(1)}}^m \xrightarrow{\sim} U_v/U_v^m$, because m is a power of p and therefore is coprime to the order of $U_v/U^{(1)}$. Hence, we get the commutative diagram

$$\begin{array}{ccc} U^{(1)}/{U^{(1)}}^m & & \\ \downarrow{\scriptstyle \chi} & \searrow^{\pi} & \\ (\mathcal{O}_K/\mathfrak{P}_v^t)^*/(\mathcal{O}_K/\mathfrak{P}_v^t)^{*m} & \xrightarrow{\varphi_v} & U_v/U_v^{\perp} \end{array}$$

where

$$\chi : U^{(1)}/{U^{(1)}}^m \twoheadrightarrow (\mathcal{O}_K/\mathfrak{P}_v^t)^*/(\mathcal{O}_K/\mathfrak{P}_v^t)^{*m}$$

is the map induced by the weak approximation theorem on U_v/U_v^m and

$$\pi : U^{(1)}/{U^{(1)}}^m \twoheadrightarrow U_v/U_v^{\perp}$$

is the map induced by the natural projection $U_v/U_v^m \to U_v/U_v^\perp$.

Let $\delta \in K_v$ be such that the extension $K_v(\sqrt[m]{\delta})/K_v$ is unramified of degree m. By Lemma 3.87 we can assume $\delta \in U_v$. Since every root of unity of order coprime to p is an m-th power, we can assume $\delta \in U^{(1)}$. Theorem 3.86 implies that $\delta \cdot {U^{(1)}}^m$ is contained in the kernel of π. By Corollary 3.91 this kernel is cyclic of order m and therefore is the cyclic subgroup of ${U^{(1)}}/{U^{(1)}}^m$ generated by $\delta \cdot {U^{(1)}}^m$.

The kernel of χ is the group $U^{(t)} \cdot {U^{(1)}}^m/{U^{(1)}}^m$, where $U^{(t)}$ is the t-th higher unit group of the ring of integers $\mathcal{O}_v$ of K_v. It is a cyclic group, because it is a subgroup of the kernel of π, which is a cyclic group. The second group isomorphism theorem gives a group isomorphism

$$U^{(t)} \cdot {U^{(1)}}^m/{U^{(1)}}^m \xrightarrow{\sim} U^{(t)}/(U^{(t)} \cap {U^{(1)}}^m).$$

The equality

$$U^{(t)}/(U^{(t)} \cap {U^{(1)}}^m) = U^{(t)}/(U^{(t)} \cap K_v^m)$$

follows from Theorem 3.37. By Kummer theory the group $U^{(t)} \cdot K_v^m/K_v^m$, which is isomorphic to the group $U^{(t)}/(U^{(t)} \cap K_v^m)$, is dual to the Galois group $\mathrm{Gal}(K_v(\sqrt[m]{U^{(t)}})/K_v)$. Since the kernel of χ is a cyclic group, the Galois group $\mathrm{Gal}(K_v(\sqrt[m]{U^{(t)}})/K_v)$ is cyclic. By Lemma 3.98 the extension $K_v(\sqrt[m]{U^{(t)}})/K_v$ is an unramified cyclic extension of degree dividing p. Theorem 3.95 implies that there is $b \in 1 + p\lambda\mathcal{O}_v$ such that the extension $K_v(\sqrt[p]{b})/K_v$ is unramified of degree p. Since an explicit computation shows $b^{m/p} \in U^{(t)}$, the kernel of χ contains $b^{m/p} \cdot {U^{(1)}}^m$. Thus, it has order p. Since the kernel of π is cyclic of order m and we have the identity $m/p = p^{n-1}$, the kernel of φ_v is a cyclic group of order p^{n-1}. This proves (c). Now (d) follows from the explicit description of the kernel of π. □

Remark 5.13. Note that for $n = 1$ the surjective group homomorphism φ in Theorem 5.12 is a group isomorphism

$$\varphi : (\mathcal{O}_K/p\lambda\mathcal{O}_K)^*/(\mathcal{O}_K/p\lambda\mathcal{O}_K)^{*p} \xrightarrow{\sim} \prod_{v|p} U_v/U_v^\perp$$

given by

$$(a + p\lambda\mathcal{O}_K) \cdot (\mathcal{O}_K/p\lambda\mathcal{O}_K)^{*p} \xmapsto{\varphi} (aU_v^\perp)_v.$$

Theorem 5.14. *Let the notation be as in* Notation 4.80 *with $m = 2$ and let K_+^* be the group of totally positive elements in K^*. Then there is a group isomorphism*

$$\varphi : K^*/K_+^* \xrightarrow{\sim} \prod_{v \text{ real}} U_v/U_v^\perp$$

given by

$$aK_+^* \xmapsto{\varphi} (aU_v^\perp)_v.$$

Proof. By Section 3.7 the map is a well-defined and injective group homomorphism. The surjectivity follows from the weak approximation theorem. □

5.2 The virtual group

Definition 5.15 (m-th virtual group)**.** Let m be a positive integer, let K be a number field containing a primitive m-th root of unity, and let the triple $(\overline{U}/\overline{U}^{\perp}, \mu_m, (\cdot,\cdot)_{K,m})$ be the m-th unit residue group of K. The *m-th virtual group* V of the number field K is the subgroup

$$V = (\overline{K^*} \cap \overline{U}) \cdot \overline{U}^{\perp}/\overline{U}^{\perp}$$

of the m-th unit residue group of K.

We will write only 'virtual group' when m is understood.

Remark 5.16. By definition the m-th virtual group of K is the image of the natural group homomorphism $\overline{K^*} \cap \overline{U} \to \overline{U}/\overline{U}^{\perp}$. This group homomorphism gives rise to a short exact sequence

$$1 \longrightarrow \overline{K^*} \cap \overline{U}^{\perp} \longrightarrow \overline{K^*} \cap \overline{U} \longrightarrow V \longrightarrow 1.$$

Theorem 5.17. *Let m be a positive integer and let K be a number field containing a primitive m-th root of unity. Then the m-th virtual group V of K is a maximal self-annihilating subgroup of the m-th unit residue group of K and has order $m^{|S_\infty|}$.*

Proof. By Theorem 4.52 we have the identity $\overline{K^*}^{\perp} = \overline{K^*}$. Using the equality

$$(\overline{K^*} \cdot \overline{U}^{\perp}) \cap \overline{U} = (\overline{K^*} \cap \overline{U}) \cdot \overline{U}^{\perp}$$

in Theorem 4.83, we obtain

$$V^{\perp} = \left((\overline{K^*} \cap \overline{U}) \cdot \overline{U}^{\perp}/\overline{U}^{\perp}\right)^{\perp} = ((\overline{K^*} \cdot \overline{U}^{\perp}) \cap \overline{U})/\overline{U}^{\perp} = (\overline{K^*} \cap \overline{U}) \cdot \overline{U}^{\perp}/\overline{U}^{\perp} = V.$$

Hence, the annihilator of V in $\overline{U}/\overline{U}^{\perp}$ is itself. By Theorem 5.10 we conclude that V is a maximal self-annihilating subgroup of the m-th unit residue group and has order $m^{|S_\infty|}$. □

Corollary 5.18. *Let m be a positive integer and let K be a number field containing a primitive m-th root of unity. If m is square-free, then the m-th virtual group of K is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^{|S_\infty|}$.*

Proof. By Theorem 5.17 the m-th virtual group of K has order $m^{|S_\infty|}$. Since by Theorem 5.10 the m-th unit residue group of K is isomorphic, as an abelian group, to $(\mathbb{Z}/m\mathbb{Z})^{2\cdot|S_\infty|}$, the result follows from the structure theorem for finite abelian groups. □

Remark 5.19. If m is not square-free, then an isomorphism as in Corollary 5.18 does not necessarily exist. As an example, see Theorem 6.31, where m equals 4, the number field K is $\mathbb{Q}(\mathrm{i}, \sqrt{30})$, and the 4-th virtual group of K is isomorphic, as an abelian group, to $(\mathbb{Z}/2\mathbb{Z})^4$.

Theorem 5.20. *Let m be a positive integer, let K be a number field containing a primitive m-th root of unity, let S be the set of places of K, and let V be the m-th virtual group of K. For each subset $T \subseteq S$ let π_T be the canonical projection*

$$\pi_T : \prod_{v\in S} U_v/U_v^\perp \twoheadrightarrow \prod_{v\in T} U_v/U_v^\perp$$

of the m-th unit residue group of K on the product of its local components at the places in T. Then for each subset $T \subseteq S$ one has

$$|\pi_T(V)|^2 \geq \prod_{v\in T} |U_v/U_v^\perp|.$$

Proof. We have the inclusion

$$V \subseteq \left(\prod_{v\in S\setminus T} U_v/U_v^\perp\right) \times \pi_T(V).$$

Denote $\prod_{v\in T} U_v/U_v^\perp$ by W. Taking the annihilators in the m-th unit residue group of K gives

$$V^\perp \supseteq \{1\} \times \pi_T(V)^\perp,$$

where $\pi_T(V)^\perp$ denotes the annihilator of $\pi_T(V)$ in W. The equality $V = V^\perp$ of Theorem 5.17 implies the inclusion

$$\pi_T(V)^\perp \subseteq \pi_T(V).$$

Hence, we get

$$|W| = |W/\pi_T(V)^\perp| \cdot |\pi_T(V)^\perp| \leq |W/\pi_T(V)^\perp| \cdot |\pi_T(V)|.$$

Since by duality we have $|W/\pi_T(V)^\perp| = |\pi_T(V)|$, we obtain the inequality $|W| \leq |\pi_T(V)|^2$. □

Corollary 5.21. *Let m be a positive integer, let K be a number field containing a primitive m-th root of unity, let S be the set of places of K, and let V be the m-th virtual group of K. Let w be a place in S such that $U_w/U_w^\perp$ is not the trivial group and let π_w be the canonical projection*

$$\pi_w : \prod_{v\in S} U_v/U_v^\perp \twoheadrightarrow U_w/U_w^\perp$$

of the m-th unit residue group of K on its w-component. Then the image $\pi_w(V)$ of V in $U_w/U_w^\perp$ is not trivial.

Proof. The result follows from Theorem 5.20. □

Corollary 5.22. *Let K be a number field, let S be the set of places of K, let π_2 be the canonical projection*

$$\pi_2 : \prod_{v\in S} U_v/U_v^\perp \twoheadrightarrow \prod_{v|2} U_v/U_v^\perp$$

of the 2-nd unit residue group of K on the product of its local components at the places dividing 2, and let V be the 2-nd virtual group of K. Then one has

$$\operatorname{rk}_2 \pi_2(V) \geq \left\lceil \frac{[K:\mathbb{Q}]}{2} \right\rceil.$$

Proof. The 2-nd virtual group of K is an elementary abelian 2-group, because it is a subgroup of the 2-nd unit residue group of K, which is an elementary abelian 2-group by Theorem 5.10. Lemma 5.9 states that there is a group isomorphism

$$\prod_{v|2} U_v/U_v^\perp \xrightarrow{\sim} (\mathbb{Z}/2\mathbb{Z})^{[K:\mathbb{Q}]}.$$

The desired inequality follows from Theorem 5.20. □

Cohen introduced the notion of virtual unit in Definition 5.2.4 in [10].

Definition 5.23 (m-virtual unit)**.** Let m be a positive integer, let L be a number field, and let $\mathcal{O}_L$ be its ring of integers. An element $a \in L$ is an *m-virtual unit* if there exists a fractional ideal $\mathfrak{a}$ of $\mathcal{O}_L$ such that $a\mathcal{O}_L = \mathfrak{a}^m$.

Theorem 5.24. *Let m be a positive integer and let L be a number field. Then the set of m-virtual units of L forms a group under multiplication.*

Proof. The result follows directly from Definition 5.23. □

Definition 5.25 (m-Selmer group)**.** Let L be a number field. The *m-Selmer group* of L is the quotient group $\{m\text{-virtual units of } L\}/L^{*m}$.

Theorem 5.26. *Let the notation be as in* Notation 4.80. *Then the projection* $\overline{} : J \to J/J^m$ *gives rise to a short exact sequence*

$$1 \longrightarrow K^{*m} \longrightarrow \{m\text{-virtual units of } K\} \longrightarrow \overline{K^*} \cap \overline{U} \longrightarrow 1.$$

Proof. By definition any m-virtual unit has normalized valuation divisible by m at every finite place. Hence, the m-virtual units of K are the elements $a \in K^*$ with $\overline{a} \in \overline{U}$. The exactness of the sequence follows from the equality $K^* \cap J^m = K^{*m}$ in Lemma 4.51. □

Corollary 5.27. *Let the notation be as in* Notation 4.80. *Then the projection* $\overline{} : J \to J/J^m$ *induces a group isomorphism from the m-Selmer group of K to the group* $\overline{K^*} \cap \overline{U}$.

Proof. The group isomorphism follows from the short exact sequence in Theorem 5.26. □

Remark 5.28. Composing the projection $J \to J/J^m$ with the group homomorphism $\overline{K^*} \cap \overline{U} \to \overline{U}/\overline{U}^{\perp}$, by Theorem 5.26 and Remark 5.16 we get a surjective group homomorphism

$$\{m\text{-virtual units of } K\} \twoheadrightarrow V.$$

Note that an m-virtual unit $a \in K^*$ is in the kernel if and only if the extension $K(\sqrt[m]{a})/K$ is unramified at all places of K. Hence, there is an induced surjective group homomorphism from the m-Selmer group of K to V. In some cases we will compute the m-th virtual group V of K by explicitly specifying a set of m-virtual units of K of which the image in V generates V, as well as the relations among those generators.

Theorem 5.29. *Let the notation be as in* Notation 4.80. *Then the group homomorphism* $\{m\text{-virtual units of } K\}/K^{*m} \to \mathrm{Cl}[m]$ *that sends the class* $a \cdot K^{*m}$ *of an m-virtual unit $a \in K^*$ to the ideal class of the ideal $\mathfrak{a}$ such that* $a\mathcal{O}_K = \mathfrak{a}^m$ *gives rise to a split short exact sequence*

$$1 \longrightarrow E/E^m \longrightarrow \{m\text{-virtual units of } K\}/K^{*m} \longrightarrow \mathrm{Cl}[m] \longrightarrow 1.$$

Proof. By definition of m-virtual unit the group homomorphism in the statement is well-defined and surjective. Since its kernel is the group E/E^m, we get the short exact sequence in the statement. This sequence of $\mathbb{Z}/m\mathbb{Z}$-modules splits, because the group E/E^m is a free $\mathbb{Z}/m\mathbb{Z}$-module and each free $\mathbb{Z}/m\mathbb{Z}$-module is injective. □

Corollary 5.30. *Let the notation be as in* Notation 4.80. *Then the m-Selmer group* $\{m\text{-virtual units of } K\}/K^{*m}$ *of K is a finite abelian group.*

Proof. Since the abelian groups E/E^m and $\mathrm{Cl}[m]$ are finite, the result follows from Theorem 5.29. □

Remark 5.31. Theorem 5.29 implies that as soon as we know generators for the groups E and $\mathrm{Cl}[m]$, we also have generators for the m-Selmer group.

5.3 The field of rational numbers

Let $\mathbb{Q}$ be the field of rational numbers. It contains -1, a primitive 2-nd root of unity, and does not contain any primitive m-th root of unity for any integer $m > 2$. Hence, there are only two unit residue groups of $\mathbb{Q}$: the 1-st unit residue group and the 2-nd unit residue group. Since the 1-st unit residue group of $\mathbb{Q}$ is the trivial group, we restrict our attention to the 2-nd unit residue group.

Theorem 5.32. *Let $(\overline{U}/\overline{U}^{\perp}, \{\pm 1\}, (\cdot,\cdot)_{\mathbb{Q},2})$ be the 2-nd unit residue group of $\mathbb{Q}$. Then there is a natural isomorphism*

$$\overline{U}/\overline{U}^{\perp} \xrightarrow{\sim} (\mathbb{Z}/4\mathbb{Z})^* \perp (\mathbb{R}^*/\mathbb{R}_{>0})$$

of skew abelian groups, where each of the order 2 groups $(\mathbb{Z}/4\mathbb{Z})^*$ and $\mathbb{R}^*/\mathbb{R}_{>0}$ is equipped with its unique antisymmetric perfect pairing to $\{\pm 1\}$, and the image of the 2-nd virtual group of $\mathbb{Q}$ equals the image of the class of -1 in the 2-nd unit residue group of $\mathbb{Q}$ and is the graph of the unique group isomorphism

$$(\mathbb{Z}/4\mathbb{Z})^* \xrightarrow{\sim} \mathbb{R}^*/\mathbb{R}_{>0}.$$

Proof. By Theorem 5.1 the projection $J \to J/J^2$ induces a group isomorphism

$$\prod_{v|2} U_v/U_v^{\perp} \times \prod_{v \text{ real}} U_v/U_v^{\perp} \xrightarrow{\sim} \overline{U}/\overline{U}^{\perp},$$

where v ranges over all places of $\mathbb{Q}$ dividing 2 and over all real Archimedean places of $\mathbb{Q}$. There is only one place of $\mathbb{Q}$ dividing 2 and there is only one Archimedean place of $\mathbb{Q}$, which is real. Using the natural group isomorphisms

$$U_\infty/U_\infty^{\perp} \cong \mathbb{R}^*/\mathbb{R}_{>0}$$

in Section 3.7 for real Archimedean local fields and

$$U_2/U_2^{\perp} \cong (\mathbb{Z}/4\mathbb{Z})^*$$

in Section 3.10 for the local field $\mathbb{Q}_2$, the completion of $\mathbb{Q}$ at 2, we get a group isomorphism

$$(\mathbb{Z}/4\mathbb{Z})^* \oplus \mathbb{R}^*/\mathbb{R}_{>0} \xrightarrow{\sim} \overline{U}/\overline{U}^{\perp}.$$

Considered as a map on $((\mathbb{Z}/4\mathbb{Z})^* \oplus \mathbb{R}^*/\mathbb{R}_{>0}) \times ((\mathbb{Z}/4\mathbb{Z})^* \oplus \mathbb{R}^*/\mathbb{R}_{>0})$, the norm-residue symbol is the antisymmetric pairing

$$\begin{aligned}((\mathbb{Z}/4\mathbb{Z})^* \oplus \mathbb{R}^*/\mathbb{R}_{>0}) \times ((\mathbb{Z}/4\mathbb{Z})^* \oplus \mathbb{R}^*/\mathbb{R}_{>0}) &\to \{\pm 1\},\\ ((a_1, b_1), (a_2, b_2)) &\mapsto (-1)^{\frac{a_1-1}{2}\frac{a_2-1}{2} + \frac{b_1-|b_1|}{2b_1}\frac{b_2-|b_2|}{2b_2}}.\end{aligned}$$

The skew element is given by $(-1 \bmod 4, -1 \cdot \mathbb{R}_{>0})$, which is the element corresponding to the class of -1 in $\overline{U}/\overline{U}^{\perp}$, as also stated in Theorem 5.4. The 2-nd unit residue group of $\mathbb{Q}$ is isomorphic, as a skew abelian group, to a direct sum of two skew abelian groups of order 2. Its isomorphism class in Theorem 2.28 is the class of the pair $((\mathbb{Z}/2\mathbb{Z})^2, (1, 1))$.

Let V be the 2-nd virtual group of $\mathbb{Q}$. By Theorem 5.17 it is a subgroup of the 2-nd unit residue group of $\mathbb{Q}$ of order 2. The group of 2-virtual units of $\mathbb{Q}$ is $\{\pm 1\} \cdot {\mathbb{Q}^*}^2$, because the class number of $\mathbb{Q}$ is 1. Since V is generated by the images of 2-virtual units under the surjective group homomorphism $\{\text{2-virtual units of } \mathbb{Q}\} \twoheadrightarrow V$ in Remark 5.28 and is not trivial, the image of -1 cannot be trivial. In particular, the image of -1 is not trivial, because the extension $\mathbb{Q}(\mathrm{i})/\mathbb{Q}$ is ramified at 2 and at infinity. Hence V is the graph of the unique group isomorphism

$$(\mathbb{Z}/4\mathbb{Z})^* \xrightarrow{\sim} \mathbb{R}^*/\mathbb{R}_{>0}$$

and is generated by the skew element. □

CHAPTER 6

Quadratic number fields and a biquadratic example

6.1 Introduction

Let m be a positive integer. The m-th unit residue group of a number field K [Definition 5.3] is defined when K contains a primitive m-th root of unity. Since the minimal polynomial over $\mathbb{Q}$ of a primitive m-th root of unity has degree $\varphi(m)$, where φ denotes the Euler's totient function, for any positive integer $n \notin \{1, 2, 3, 4, 6\}$ no quadratic number field contains a primitive n-th root of unity. Every quadratic number field contains 1 and -1, which are a primitive 1-st root of unity and a 2-nd primitive root of unity, respectively. The only quadratic number fields that contain a primitive n-th root of unity for an integer $n > 2$ are $\mathbb{Q}(\mathrm{i})$ and $\mathbb{Q}(\sqrt{-3})$. The number field $\mathbb{Q}(\mathrm{i})$ contains a primitive 4-th root of unity and the number field $\mathbb{Q}(\sqrt{-3})$ contains a primitive 6-th root of unity and therefore a primitive 3-rd root of unity too. Hence, every quadratic number field has its own 1-st unit residue group and 2-nd unit residue group, there is the 4-th unit residue group of the number field $\mathbb{Q}(\mathrm{i})$, and the number field $\mathbb{Q}(\sqrt{-3})$ has its own 3-rd unit residue group and 6-th unit residue group.

Let m be a positive integer, let K be a quadratic number field containing a primitive m-th root of unity, and let G be the Galois group $\mathrm{Gal}(K/\mathbb{Q})$. We recall that the m-th unit residue group of K is a skew abelian group [Corollary 5.2], where the pairing is given by the m-th power norm-residue symbol, and is isomorphic to an orthogonal sum of skew abelian groups that

are defined locally at the places of K dividing m and at the real Archimedean places of K [Theorem 5.6]. We refer to Chapter 2 for definitions and results on skew abelian groups. Theorem 5.1 implies that the m-th unit residue group of K has trivial components at the places not dividing m. Using the group homomorphism in Theorem 5.12 and the group isomorphism in Theorem 5.14 we study the nontrivial components of the m-th unit residue group of K and the action of G on them. Moreover, we describe the m-th virtual group V of K explicitly by specifying a set of m-virtual units of K such that its image in V under the surjective group homomorphism $\{m\text{-virtual units of } K\} \twoheadrightarrow V$ in Remark 5.28 generates V.

The 1-st unit residue group of any number field is trivial. The 2-nd unit residue group of a quadratic number field has a nontrivial 2-adic component, which is the subject of study in Section 6.4. This component is a Klein four-group [Definition 6.7] and a $(\mathbb{Z}/2\mathbb{Z})[G]$-module [Theorem 6.10]. The Galois action depends on the residue class modulo 8 of the discriminant of the quadratic number field [Theorem 6.12 and Corollary 6.13].

Let K be an imaginary quadratic number field. The only nontrivial component of the 2-nd unit residue group of K is the 2-adic component. The natural $(\mathbb{Z}/2\mathbb{Z})[G]$-module isomorphism 6.16 in Theorem 6.15 shows it is enough to consider the $(\mathbb{Z}/2\mathbb{Z})[G]$-module $(\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2}$, where $\mathcal{O}_K$ is the ring of integers of K. According to the case distinction given by Theorem 6.1, we give an explicit $(\mathbb{Z}/2\mathbb{Z})[G]$-module isomorphism for this module and describe the 2-nd virtual group of K in Theorem 6.17, Theorem 6.18, and Theorem 6.19.

Let K be a real quadratic number field. The 2-nd unit residue group of K has also a nontrivial component at infinity [Theorem 6.24]. Each of Theorem 6.26, Theorem 6.27, Theorem 6.28, and Theorem 6.29 describes the 2-nd virtual group V of K in one of the four separate cases of Theorem 6.3. Corollary 6.30 shows that the Galois module structure of V depends on whether the discriminant of K can be written as the sum of two squares of integers or not.

The results about the 3-rd unit residue group of the number field $\mathbb{Q}(\sqrt{-3})$ and the 6-rd unit residue group of $\mathbb{Q}(\sqrt{-3})$ are presented in Theorem 6.20 and Theorem 6.22, respectively. Theorem 6.21 describes the 4-th unit residue group of $\mathbb{Q}(\mathrm{i})$.

Given a positive integer m and a global field K containing a primitive m-th root of unity, Theorem 5.10 states that the m-th unit residue group of K is a free module over $\mathbb{Z}/m\mathbb{Z}$. One may wonder whether there is a similar result for the m-th virtual group of K. The answer is negative. Theorem 6.31 gives an example of a number field whose 4-th virtual group is not a free module over $\mathbb{Z}/4\mathbb{Z}$.

6.2 Discriminants of quadratic number fields

Theorem 6.1. *Let D be the set of discriminants of quadratic number fields. Then the following sets form a partition of D:*
(a) $\{\Delta \in \mathbb{Z} : \Delta \equiv 4 \bmod 8$ with $\Delta/4 \equiv 3 \bmod 4$ and squarefree$\}$,
(b) $\{\Delta \in \mathbb{Z} : \Delta \equiv 0 \bmod 8$ with $\Delta/4 \equiv 2 \bmod 4$ and squarefree$\}$,
(c) $\{\Delta \in \mathbb{Z} \setminus \{1\} : \Delta \equiv 1 \bmod 4$ with Δ squarefree$\}$.

Proof. See Proposition 13.1.2 in Section 1 of Chapter 13 in [27] by Ireland and Rosen. □

Theorem 6.2 (Euler)**.** *Let n be a positive integer. Then the following are equivalent.*
(i) *The integer n is the sum of two squares of integers.*
(ii) *Every prime congruent to 3 modulo 4 occurs with an even exponent in the prime factorization of n.*

Proof. See Corollary 1 in Section 6 of Chapter 17 in [27] by Ireland and Rosen. □

It is believed that the first proof of Theorem 6.2 was given by Euler in two letters to Goldbach in 1747 and 1749. For more details about the correspondence between Euler and Goldbach on this result see [39] by Lemmermeyer.

Theorem 6.3. *Let D^+ be the set of discriminants of real quadratic number fields. Then the following sets form a partition of D^+:*
(a) $\{\Delta \in D^+ : \Delta \equiv 4 \bmod 8\}$,
(b) $\{\Delta \in D^+ : \Delta \not\equiv 4 \bmod 8$ and there is a prime congruent to 3 modulo 4 that divides $\Delta\}$,
(c) $\{\Delta \in D^+ : \Delta \equiv 0 \bmod 8$ and there are $a, b \in \mathbb{Z}$ with $\Delta = 4(a^2 + b^2)\}$,
(d) $\{\Delta \in D^+ : \Delta \equiv 1 \bmod 4$ and there are $a, b \in \mathbb{Z}$ with $\Delta = 4a^2 + b^2\}$.

Proof. This follows from Theorem 6.1 and Theorem 6.2. □

6.3 Unramified extensions

Lemma 6.4. *Let F be a number field, let $\mathfrak{P}$ be a prime of the ring of integers of F, and let $\overline{F}$ be an algebraic closure of F. Let K/F and L/F be extensions of number fields with $K, L \subseteq \overline{F}$. If the extension L/F is unramified at $\mathfrak{P}$, then the extension KL/K is unramified at $\mathfrak{P}$.*

Proof. This follows from Lemma 4.6.3 in Section 4.6 of Chapter 4 in [29] by Koch. □

Lemma 6.5. *Let F be a number field and let $\overline{F}$ be an algebraic closure of F. Let K/F and L/F be extensions of number fields with $K, L \subseteq \overline{F}$. If a prime $\mathfrak{P}$ of F is unramified in both K and in L, then it is unramified in the compositum KL.*

Proof. This follows from Lemma 6.4. See also Theorem 31 of Chapter 4 in [44] by Marcus. □

Lemma 6.6. *Let n be a positive integer, let $K/\mathbb{Q}$ be a number field extension of degree n unramified at 2, and let $\mathcal{O}_K$ be the ring of integers of K. Then there is a group isomorphism*

$$\varphi : \mathcal{O}_K/2\mathcal{O}_K \xrightarrow{\sim} (\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2}$$

such that for each $a \in \mathcal{O}_K$ one has

$$a + 2\mathcal{O}_K \overset{\varphi}{\mapsto} (1 + 2a + 4\mathcal{O}_K) \cdot (\mathcal{O}_K/4\mathcal{O}_K)^{*2}.$$

Moreover, if $K/\mathbb{Q}$ is a Galois extension with Galois group G, then the group isomorphism φ is a $(\mathbb{Z}/2\mathbb{Z})[G]$-module isomorphism of free $(\mathbb{Z}/2\mathbb{Z})[G]$-modules of rank 1, where each of the groups $\mathcal{O}_K/2\mathcal{O}_K$ and $(\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2}$ is equipped with its natural G-action.

Proof. Let R be the ring $\mathcal{O}_K/4\mathcal{O}_K$ and let I be its ideal $2\mathcal{O}_K/4\mathcal{O}_K$. Since we have $I^2 = 0$, the map $I \to 1 + I$, $x \mapsto 1 + x$, is a group isomorphism. Hence, the group $1 + I$ is an elementary abelian 2-group and we get the short exact sequence

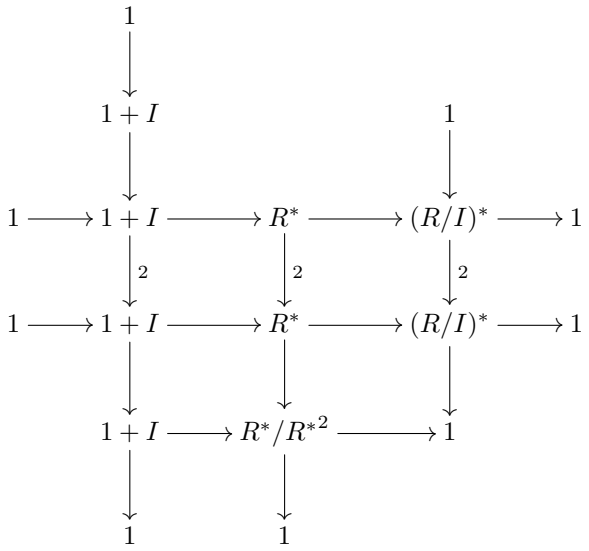
$$1 \to 1 + I \to R^* \to (R/I)^* \to 1.$$

Let $2\mathcal{O}_K = \prod_{i=1}^{r} \mathfrak{P}_i$ be the prime ideal factorization of $2\mathcal{O}_K$ in the ring of integers $\mathcal{O}_K$ of K. Since we have a natural group isomorphism $R/I \xrightarrow{\sim} \mathcal{O}_K/2\mathcal{O}_K$, the Chinese remainder theorem gives a group isomorphism

$$(R/I)^* \xrightarrow{\sim} \bigoplus_{i=1}^{r} (\mathcal{O}_K/\mathfrak{P}_i)^*.$$

The squaring map $(R/I)^* \to (R/I)^*$, $x \mapsto x^2$, is a group isomorphism, because for every prime ideal $\mathfrak{P}$ dividing $2\mathcal{O}_K$ the unit group of the residue field $\mathcal{O}_K/\mathfrak{P}$ has order coprime to 2. Hence, we get the following diagram of exact sequences,

where the arrows labelled with 2 are squaring maps.



The snake lemma gives the exact sequence

$$1 \to 1 + I \to R^*/{R^*}^2 \to 1.$$

By composing the group isomorphism $1 + I \xrightarrow{\sim} R^*/{R^*}^2$ given by this exact sequence with the group isomorphisms $\mathcal{O}_K/2\mathcal{O}_K \xrightarrow{\sim} I$, $x + 2\mathcal{O}_K \mapsto 2x + 4\mathcal{O}_K$, and $I \xrightarrow{\sim} 1 + I$, $x \mapsto 1 + x$, we get the group isomorphism

$$\begin{aligned} \varphi : \mathcal{O}_K/2\mathcal{O}_K &\xrightarrow{\sim} R^*/{R^*}^2, \\ a + 2\mathcal{O}_K &\mapsto (1 + 2a + 4\mathcal{O}_K) \cdot {R^*}^2, \end{aligned}$$

as stated in Lemma 6.6.

Now assume that $K/\mathbb{Q}$ is a Galois extension and let G be the Galois group $\mathrm{Gal}(K/\mathbb{Q})$. For each prime ideal $\mathfrak{P}$ dividing $2\mathcal{O}_K$ the decomposition group of $\mathfrak{P}$ is naturally isomorphic to the Galois group of the extension $(\mathcal{O}_K/\mathfrak{P})/(\mathbb{Z}/2\mathbb{Z})$ of residue fields. Since any finite Galois extension of fields has a normal basis and the group G acts transitively on the set of prime ideals of $\mathcal{O}_K$ above 2, the $(\mathbb{Z}/2\mathbb{Z})[G]$-module $\mathcal{O}_K/2\mathcal{O}_K$ is free of rank 1. The group isomorphism φ is a $(\mathbb{Z}/2\mathbb{Z})[G]$-module isomorphism, because it respects the natural G-actions. □

6.4 The two-adic component of the unit residue group

Definition 6.7 (Klein four-group)**.** A *Klein four-group* is a group isomorphic to $(\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z})$.

Lemma 6.8. *Let A be a Klein four-group. The map*

$$\{\text{skew abelian groups } (A, \{\pm 1\}, \beta)\} \to A$$

that sends a skew abelian group [Definition 2.7] *of the form $(A, \{\pm 1\}, \beta)$ to its skew element* [Definition 2.12] *is a bijection.*

Proof. Let $(A, \{\pm 1\}, \beta)$ be a skew abelian group and let g be its skew element. Since the antisymmetric pairing β takes values in $\{\pm 1\}$, giving the annihilator of each element in A is equivalent to giving the map β. For every nonzero element $a \in A$ the annihilator $a^\perp$ of a has order 2. We have $a + g \in a^\perp$ and $g \in g^\perp$. Since $a + g = 0$ is equivalent to $a = g$, we get an explicit description of the annihilator of any element in A that depends only on g. This shows that the map in the statement of Lemma 6.8 is injective. The classification of skew abelian groups [Theorem 2.28] implies that it is also surjective. □

Notation 6.9. Let K be a quadratic number field, let Δ be its discriminant, let $\mathcal{O}_K$ be the ring of integers of K, and let G be the Galois group $\mathrm{Gal}(K/\mathbb{Q})$.

Theorem 6.10. *Let the notation be as in* Notation 6.9. *For each place v of K above 2 let K_v be the completion of K at v, let U_v be the unit group of the ring of integers of K_v, and let $U_v^\perp$ be the annihilator in K_v^* of U_v with respect to the norm-residue symbol $(\cdot,\cdot)_{K_v,2} : K_v^* \times K_v^* \to \{\pm 1\}$. Then the groups $(\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2}$ and $\prod_{v|2} U_v/U_v^\perp$ are Klein four-groups and the natural group isomorphism*

$$(\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2} \xrightarrow{\sim} \prod_{v|2} U_v/U_v^\perp \tag{6.11}$$

given by Theorem 5.12 *is a $(\mathbb{Z}/2\mathbb{Z})[G]$-module isomorphism and is an isomorphism of skew abelian groups*

$$((\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2}, \{\pm 1\}, \beta) \xrightarrow{\sim} (\prod_{v|2} U_v/U_v^\perp, \{\pm 1\}, \prod_{v|2} (\cdot,\cdot)_{K_v,2}),$$

where β is the unique antisymmetric perfect pairing

$$\beta : (\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2} \times (\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2} \to \{\pm 1\}$$

that makes $((\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2}, \{\pm 1\}, \beta)$ into a skew abelian group with skew element $(-1 + 4\mathcal{O}_K) \cdot (\mathcal{O}_K/4\mathcal{O}_K)^{*2}$.

Proof. Since the group isomorphism given by Theorem 5.12 respects the natural actions of G on $(\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2}$ and on $\prod_{v|2} U_v/U_v^\perp$, we get a natural $(\mathbb{Z}/2\mathbb{Z})[G]$-module isomorphism

$$(\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2} \xrightarrow{\sim} \prod_{v|2} U_v/U_v^\perp.$$

Corollary 3.91 gives a group isomorphism $\prod_{v|2} U_v/U_v^\perp \cong (\mathbb{Z}/2\mathbb{Z})^2$, because the sum of the local degrees $\sum_{v|2}[K_v : \mathbb{Q}_2]$, where $\mathbb{Q}_2$ is the field of 2-adic rationals, equals the global degree $[K : \mathbb{Q}]$. Since $\prod_{v|2}(\cdot,\cdot)_{K_v,2}$ is an antisymmetric perfect pairing, there is an antisymmetric perfect pairing

$$\beta : (\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2} \times (\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2} \to \{\pm 1\}$$

such that the group isomorphism 6.11 is an isomorphism of skew abelian groups

$$((\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2}, \{\pm 1\}, \beta) \xrightarrow{\sim} (\prod_{v|2} U_v/U_v^\perp, \{\pm 1\}, \prod_{v|2}(\cdot,\cdot)_{K_v,2}).$$

Let β be such an antisymmetric perfect pairing. Corollary 3.92 and Lemma 6.8 imply that β is the unique antisymmetric perfect pairing

$$\beta : (\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2} \times (\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2} \to \{\pm 1\}$$

that makes $((\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2}, \{\pm 1\}, \beta)$ into a skew abelian group with skew element $(-1 + 4\mathcal{O}_K) \cdot (\mathcal{O}_K/4\mathcal{O}_K)^{*2}$. □

Theorem 6.12. *Let the notation be as in* Notation 6.9. *Then one has the following.*

(a) *For* $\Delta \equiv 1 \bmod 4$ *there is a* $(\mathbb{Z}/2\mathbb{Z})[G]$*-module isomorphism*

$$(\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2} \xrightarrow{\sim} \mathcal{O}_K/2\mathcal{O}_K$$

of free $(\mathbb{Z}/2\mathbb{Z})[G]$*-modules of rank* 1 *such that for each* $a \in \mathcal{O}_K$ *one has*

$$(1 + 2a + 4\mathcal{O}_K) \cdot (\mathcal{O}_K/4\mathcal{O}_K)^{*2} \mapsto a + 2\mathcal{O}_K.$$

(b) *For* $\Delta \equiv 0 \bmod 8$ *there is a* $(\mathbb{Z}/2\mathbb{Z})[G]$*-module isomorphism*

$$(\mathbb{Z}/2\mathbb{Z})[G] \xrightarrow{\sim} (\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2}$$

of free $(\mathbb{Z}/2\mathbb{Z})[G]$*-modules of rank* 1 *such that for each pair* $(a_0, a_1) \in (\mathbb{Z}/2\mathbb{Z})^2$ *one has*

$$a_0 + a_1\sigma \mapsto (1 + \sqrt{\Delta/4} + 4\mathcal{O}_K)^{a_0}(1 - \sqrt{\Delta/4} + 4\mathcal{O}_K)^{a_1} \cdot (\mathcal{O}_K/4\mathcal{O}_K)^{*2},$$

where σ *is the generator of* G.

(c) *For* $\Delta \equiv 4 \bmod 8$ *there is a* $(\mathbb{Z}/2\mathbb{Z})[G]$*-module isomorphism*

$$(\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2} \xrightarrow{\sim} (\mathcal{O}_K/2\mathcal{O}_K)^* \times \langle 5 \bmod 8 \rangle$$

of $(\mathbb{Z}/2\mathbb{Z})[G]$*-modules with trivial* G*-actions such that for each* $a \in \mathcal{O}_K$ *coprime to* 2 *one has*

$$(a + 4\mathcal{O}_K) \cdot (\mathcal{O}_K/4\mathcal{O}_K)^{*2} \mapsto (a + 2\mathcal{O}_K, \mathrm{N}_{K/\mathbb{Q}}\, a \bmod 8),$$

where $\mathrm{N}_{K/\mathbb{Q}} : K \to \mathbb{Q}$ *denotes the norm map from* K *to* $\mathbb{Q}$.

Proof. We prove each case separately.

(a) Since the rational prime 2 does not divide Δ, the extension $K/\mathbb{Q}$ is unramified at 2. The result follows from Lemma 6.6.

(b) By Theorem 6.10 the group $(\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2}$ is a Klein four-group. We have

$$\mathrm{N}_{K/\mathbb{Q}}(1 + \sqrt{\Delta/4}) = \mathrm{N}_{K/\mathbb{Q}}(1 - \sqrt{\Delta/4}) = 1 - \Delta/4 \equiv -1 \bmod 4.$$

Since by direct computation $-1 + 4\mathcal{O}_K$ is not a square in $(\mathcal{O}_K/4\mathcal{O}_K)^*$, the residue classes of $1 + \sqrt{\Delta/4}$ and $1 - \sqrt{\Delta/4}$ in $(\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2}$ are different. The nontrivial action of σ on the set $\{1 + \sqrt{\Delta/4}, 1 - \sqrt{\Delta/4}\}$ implies that these residue classes are both different from the residue class of 1. The $(\mathbb{Z}/2\mathbb{Z})[G]$-module isomorphism in the statement of (b) in Theorem 6.12 follows.

(c) Let σ be the generator of G. Since for every $b \in \mathcal{O}_K$ we have

$$\mathrm{N}_{K/\mathbb{Q}}(1 + 4b) = 1 + 4(b + \sigma(b)) + 16b\sigma(b) \equiv 1 \bmod 8$$

and for each $a \in \mathcal{O}_K$ coprime to 2 we have

$$\mathrm{N}_{K/\mathbb{Q}}(a^2) = (a\sigma(a))^2 \equiv 1 \bmod 8,$$

the map in the statement of (c) in Theorem 6.12 is well-defined. It is surjective, because it is a group homomorphism, it is surjective on the first component, and we have

$$\mathrm{N}_{K/\mathbb{Q}}(1 + 2\sqrt{\Delta/4}) = 1 - \Delta \equiv 5 \bmod 8.$$

The injectivity follows from the fact that by Theorem 6.10 it is a surjective group homomorphism between two finite groups of the same order. This map is a $(\mathbb{Z}/2\mathbb{Z})[G]$-module isomorphism of $(\mathbb{Z}/2\mathbb{Z})[G]$-modules with trivial G-actions, because it respects the natural G-actions on both groups and the natural G-action is trivial on $(\mathcal{O}_K/2\mathcal{O}_K)^* \times \langle 5 \bmod 8 \rangle$. □

Corollary 6.13. *Let the notation be as in* Notation 6.9. *For each place v of K above 2 let K_v be the completion of K at v, let U_v be the unit group of the ring of integers of K_v, and let $U_v^\perp$ be the annihilator in K_v^* of U_v with respect to the norm-residue symbol $(\cdot,\cdot)_{K_v,2} : K_v^* \times K_v^* \to \{\pm 1\}$. Then the following are equivalent.*

(i) *The skew abelian group $(\prod_{v|2} U_v/U_v^\perp, \{\pm 1\}, \prod_{v|2}(\cdot,\cdot)_{K_v,2})$ is a symplectic abelian group* [Definition 2.6].

(ii) *The action of the Galois group G on $\prod_{v|2} U_v/U_v^\perp$ is trivial.*

(iii) *The discriminant of K is congruent to 4 modulo 8.*

Proof. Using the group isomorphism 6.11 in Theorem 6.10, Theorem 6.12 implies that (ii), (iii) and $-1+4\mathcal{O}_K$ being a square in $(\mathcal{O}_K/4\mathcal{O}_K)^*$ are equivalent. Now the result follows from Theorem 2.15 and Theorem 6.10. □

6.5 Imaginary quadratic number fields

Notation 6.14. Let K be an imaginary quadratic number field, let Δ be its discriminant, let $\mathcal{O}_K$ be the ring of integers of K, and let G be the Galois group $\mathrm{Gal}(K/\mathbb{Q})$.

Theorem 6.15. *Let the notation be as in* Notation 6.14. *Then the 2-nd unit residue group $(\overline{U}/\overline{U}^\perp, \{\pm 1\}, (\cdot,\cdot)_{K,2})$ of K is a Klein four-group, there is a natural $(\mathbb{Z}/2\mathbb{Z})[G]$-module isomorphism*

$$(\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2} \xrightarrow{\sim} \overline{U}/\overline{U}^\perp \tag{6.16}$$

that is an isomorphism of skew abelian groups

$$((\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2}, \{\pm 1\}, \beta) \xrightarrow{\sim} (\overline{U}/\overline{U}^\perp, \{\pm 1\}, (\cdot,\cdot)_{K,2}),$$

where β is the unique antisymmetric perfect pairing

$$\beta : (\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2} \times (\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2} \to \{\pm 1\}$$

that makes $((\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2}, \{\pm 1\}, \beta)$ into a skew abelian group with skew element $(-1+4\mathcal{O}_K)\cdot(\mathcal{O}_K/4\mathcal{O}_K)^{*2}$, and the 2-nd virtual group of K has order 2 and is a submodule of Galois invariant elements of the 2-nd unit residue group of K.

Proof. Theorem 5.10 gives a group isomorphism $\overline{U}/\overline{U}^\perp \cong (\mathbb{Z}/2\mathbb{Z})^2$. The natural $(\mathbb{Z}/2\mathbb{Z})[G]$-module isomorphism 6.16 follows from Theorem 6.10 and Theorem 5.6. Theorem 5.17 implies that the 2-nd virtual group of K has order 2. Since by definition it is a Galois submodule of the 2-nd unit residue group of K, it is a submodule of Galois invariant elements of the 2-nd unit residue group of K. □

Each of Theorem 6.17, Theorem 6.18, and Theorem 6.19 describes the 2-nd unit residue group and the 2-nd virtual group of an imaginary quadratic number field in one of the three separate cases of Theorem 6.1.

Theorem 6.17. *Let the notation be as in* Notation 6.14 *and suppose one has* $\Delta \equiv 4 \bmod 8$. *Then there is a* $(\mathbb{Z}/2\mathbb{Z})[G]$*-module isomorphism*

$$(\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2} \xrightarrow{\sim} (\mathcal{O}_K/2\mathcal{O}_K)^* \times \langle 5 \bmod 8 \rangle$$

of $(\mathbb{Z}/2\mathbb{Z})[G]$*-modules with trivial* G*-actions such that for each* $a \in \mathcal{O}_K$ *coprime to* 2 *one has*

$$(a + 4\mathcal{O}_K) \cdot (\mathcal{O}_K/4\mathcal{O}_K)^{*2} \mapsto (a + 2\mathcal{O}_K, \mathrm{N}_{K/\mathbb{Q}}\, a \bmod 8),$$

the 2*-nd virtual group* V *of* K *is generated, under the surjective group homomorphism* $\{2\text{-virtual units of } K\} \twoheadrightarrow V$ *in* Remark 5.28*, by the image of* 2*, and the preimage of* V *under the natural* $(\mathbb{Z}/2\mathbb{Z})[G]$*-module isomorphism* 6.16 *is the kernel of the map*

$$\begin{aligned}(\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2} &\to \langle 5 \bmod 8 \rangle,\\ (a + 4\mathcal{O}_K) \cdot (\mathcal{O}_K/4\mathcal{O}_K)^{*2} &\mapsto \mathrm{N}_{K/\mathbb{Q}}\, a \bmod 8,\end{aligned}$$

where a *denotes any element in* $\mathcal{O}_K$ *coprime to* 2 *and* $\mathrm{N}_{K/\mathbb{Q}} : K \to \mathbb{Q}$ *is the norm map from* K *to* $\mathbb{Q}$.

Proof. The $(\mathbb{Z}/2\mathbb{Z})[G]$-module isomorphism of $(\mathbb{Z}/2\mathbb{Z})[G]$-modules with trivial G-action is given by (c) in Theorem 6.12. Theorem 5.17 implies that V has order 2. Hence, it is generated by one element. The extension $K(\sqrt{2})/\mathbb{Q}$ has three subextensions of degree 2 over $\mathbb{Q}$ and they are all ramified at 2. Thus, the extension $K(\sqrt{2})/K$ is ramified at the place v dividing 2. Since $2\mathcal{O}_K$ is the square of an ideal of $\mathcal{O}_K$, the integer 2 is a 2-virtual unit of K. Remark 5.28 shows that V is generated, under the surjective group homomorphism $\{2\text{-virtual units of } K\} \twoheadrightarrow V$, by the image of 2, because by Theorem 3.86 the residue class of 2 in the 2-nd unit-residue group of K is not the identity element. Multiplying 2 by squares of elements in K^*, which are in the kernel of the map $\{2\text{-virtual units of } K\} \to V$, we can get a 2-virtual unit coprime to 2. The norm of any 2-virtual unit coprime to 2 equals the square of an odd integer in $\mathbb{Z}$. Hence, it cannot be congruent to 5 modulo 8. This proves the statement about the preimage of V. □

Theorem 6.18. *Let the notation be as in* Notation 6.14 *and suppose one has* $\Delta \equiv 0 \bmod 8$. *Then there is a* $(\mathbb{Z}/2\mathbb{Z})[G]$*-module isomorphism*

$$(\mathbb{Z}/2\mathbb{Z})[G] \xrightarrow{\sim} (\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2}$$

of free $(\mathbb{Z}/2\mathbb{Z})[G]$*-modules of rank* 1 *such that for each pair* $(a_0, a_1) \in (\mathbb{Z}/2\mathbb{Z})^2$ *one has*

$$a_0 + a_1\sigma \mapsto (1 + \sqrt{\Delta/4})^{a_0}(1 - \sqrt{\Delta/4})^{a_1} \cdot (\mathcal{O}_K/4\mathcal{O}_K)^{*2},$$

where σ *is the generator of* G*, and the* 2*-nd virtual group of* K *is the submodule of Galois invariant elements of the* 2*-nd unit residue group of* K*, has order* 2*, and is generated by the residue class of* -1*.*

Proof. The $(\mathbb{Z}/2\mathbb{Z})[G]$-module isomorphism of free $(\mathbb{Z}/2\mathbb{Z})[G]$-modules of rank 1 in the statement of Theorem 6.18 is given by (b) in Theorem 6.12. Note that the residue class of -1 in $(\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2}$ is not trivial, because it is the image of $1+\sigma$ under this isomorphism. Since in a free $(\mathbb{Z}/2\mathbb{Z})[G]$-module of rank 1 the set of Galois invariant elements forms the unique submodule of order 2, Theorem 6.15 implies that the 2-nd virtual group of K is the submodule of Galois invariant elements of the 2-nd unit residue group of K and has order 2. Hence, it must be generated by the residue class of -1. □

Theorem 6.19. *Let the notation be as in* Notation 6.14 *and suppose one has* $\Delta \equiv 1 \bmod 4$*. Then there is a* $(\mathbb{Z}/2\mathbb{Z})[G]$*-module isomorphism*

$$(\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2} \xrightarrow{\sim} \mathcal{O}_K/2\mathcal{O}_K$$

of free $(\mathbb{Z}/2\mathbb{Z})[G]$*-modules of rank* 1 *such that for each* $a \in \mathcal{O}_K$ *one has*

$$(1 + 2a + 4\mathcal{O}_K) \cdot (\mathcal{O}_K/4\mathcal{O}_K)^{*2} \mapsto a + 2\mathcal{O}_K$$

and the 2*-nd virtual group of* K *is the submodule of Galois invariant elements of the* 2*-nd unit residue group of* K*, has order* 2*, and is generated by the residue class of* -1*.*

Proof. The $(\mathbb{Z}/2\mathbb{Z})[G]$-module isomorphism of free $(\mathbb{Z}/2\mathbb{Z})[G]$-modules of rank 1 in the statement of Theorem 6.19 is given by (a) in Theorem 6.12. Note that the residue class of -1 in $(\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2}$ is not trivial, because its image under this isomorphism is $1+2\mathcal{O}_K$. Since in a free $(\mathbb{Z}/2\mathbb{Z})[G]$-module of rank 1 the set of Galois invariant elements forms the unique submodule of order 2, Theorem 6.15 implies that the 2-nd virtual group of K is the submodule of Galois invariant elements of the 2-nd unit residue group of K and has order 2. Hence, it must be generated by the residue class of -1. □

Theorem 6.20. *Let* K *be the number field* $\mathbb{Q}(\sqrt{-3})$*, let* $\mathcal{O}_K$ *be the ring of integers of* K*, and let* G *be the Galois group* $\mathrm{Gal}(K/\mathbb{Q})$*. Let* ζ_3 *be a primitive* 3*-rd root of unity in* K *and let* $(\overline{U}/\overline{U}^{\perp}, \langle\zeta_3\rangle, (\cdot,\cdot)_{K,3})$ *be the* 3*-rd unit residue group of* K*. Then there is a natural* $(\mathbb{Z}/3\mathbb{Z})[G]$*-module isomorphism*

$$(\mathcal{O}_K/(1-\zeta_3)^3\mathcal{O}_K)^*/(\mathcal{O}_K/(1-\zeta_3)^3\mathcal{O}_K)^{*3} \xrightarrow{\sim} \overline{U}/\overline{U}^{\perp}$$

of free $(\mathbb{Z}/3\mathbb{Z})[G]$*-modules of rank* 1 *and the* 3*-rd virtual group of* K *is a cyclic submodule of order* 3 *with nontrivial* G*-action of the* 3*-rd unit residue group of* K *and is generated by the residue class of* ζ_3 *both as a group and as a* $(\mathbb{Z}/3\mathbb{Z})[G]$*-module.*

Proof. Let M be the group $(\mathcal{O}_K/(1-\zeta_3)^3\mathcal{O}_K)^*$. Since the group isomorphism given by Theorem 5.12 respects the natural actions of G on both groups, Theorem 5.6 implies the existence of a natural $(\mathbb{Z}/3\mathbb{Z})[G]$-module isomorphism

$$M/M^3 \xrightarrow{\sim} \overline{U}/\overline{U}^{\perp},$$

as stated in Theorem 6.20. Since the order of the group M is 18 and Theorem 5.10 gives a group isomorphism $\overline{U}/\overline{U}^{\perp} \xrightarrow{\sim} (\mathbb{Z}/3\mathbb{Z})^2$, the kernel of the canonical surjective group homomorphism

$$M \twoheadrightarrow M/M^3$$

is generated by the residue class of -1. Hence, the residue class of every element $a \in \mathcal{O}_K$ with $a \equiv 1 \bmod (1-\zeta_3)\mathcal{O}_K$ and $a \not\equiv 1 \bmod (1-\zeta_3)^3\mathcal{O}_K$ in the quotient group M/M^3 is not the identity. Since the $(\mathbb{Z}/3\mathbb{Z})[G]$-module $1+(1-\zeta_3)^2\mathcal{O}_K/(1-\zeta_3)^3\mathcal{O}_K$ is generated by $1+3$, which is a Galois invariant element, the cyclic submodule of the $(\mathbb{Z}/3\mathbb{Z})[G]$-module M/M^3 generated by the residue class of $1+(1-\zeta_3)^2$ is a $(\mathbb{Z}/3\mathbb{Z})[G]$-module of order 3 with trivial G-action. Let $\sigma \in G$ be the generator of G. Since we have $\sigma(\zeta_3) = \zeta_3^2$, the cyclic submodule generated by the residue class of ζ_3 is a $(\mathbb{Z}/3\mathbb{Z})[G]$-module of order 3 with nontrivial G-action. This proves that the G-action makes the group M/M^3 into a free $(\mathbb{Z}/3\mathbb{Z})[G]$-module of rank 1.

The cyclotomic extension $K(\zeta_9)/K$ is totally ramified at 3. Theorem 3.86 implies $\zeta_3 \notin U^{\perp}$. Since by Theorem 5.17 the 3-rd virtual group of K has order 3, the residue class of the unit ζ_3 generates the 3-rd virtual group of K both as a group and as a $(\mathbb{Z}/3\mathbb{Z})[G]$-module. □

Theorem 6.21. *Let* K *be the number field* $\mathbb{Q}(\mathrm{i})$*, let* $\mathcal{O}_K$ *be the ring of integers of* K*, and let* $(\overline{U}/\overline{U}^{\perp}, \langle \mathrm{i} \rangle, (\cdot,\cdot)_{K,4})$ *be the* 4*-th unit residue group of* K*. Then the* 4*-th unit residue group of* K *is isomorphic, as an abelian group, to* $(\mathbb{Z}/4\mathbb{Z})^2$*, there is a natural surjective group homomorphism*

$$(\mathcal{O}_K/2^3\mathcal{O}_K)^*/(\mathcal{O}_K/2^3\mathcal{O}_K)^{*4} \twoheadrightarrow \overline{U}/\overline{U}^{\perp}$$

with kernel of order 2 *generated by* $(1+4\mathrm{i}+2^3\mathcal{O}_K)\cdot(\mathcal{O}_K/2^3\mathcal{O}_K)^{*4}$*, and the* 4*-th virtual group of* K *is a cyclic subgroup of order* 4 *of the* 4*-th unit residue group of* K *and is generated by the residue class of* i.

Proof. By Theorem 5.10 we have a group isomorphism $\overline{U}/\overline{U}^{\perp} \xrightarrow{\sim} (\mathbb{Z}/4\mathbb{Z})^2$. Let F be the completion of K at the prime $1+\mathrm{i}$ above 2 and identify K with its image under the natural field homomorphism $K \to F$. Let $a \in K$ be such that the extension $F(\sqrt[4]{a})/F$ is unramified of degree 4. By Lemma 3.99 we can assume $\mathrm{v}_F(a-1) = \mathrm{v}_F(4)$, where $\mathrm{v}_F : F \to \mathbb{Z} \cup \{+\infty\}$ is the normalized valuation on F. Theorem 5.12 implies that there is a natural surjective group homomorphism

$$(\mathcal{O}_K/2^3\mathcal{O}_K)^*/(\mathcal{O}_K/2^3\mathcal{O}_K)^{*4} \twoheadrightarrow \overline{U}/\overline{U}^{\perp}$$

with kernel of order 2 generated by $(a+2^3\mathcal{O}_K)\cdot(\mathcal{O}_K/2^3\mathcal{O}_K)^{*4}$. Hence, this kernel is generated by the residue class of one of the following two elements:

$$5 = 1+4 \quad \text{and} \quad 9+4\mathrm{i} = 1+4(1+(1+\mathrm{i})).$$

The field $F(\sqrt[4]{a})$ is the compositum of F with the unique unramified extension of degree 4 of the field $\mathbb{Q}_2$ of 2-adic rationals and is Galois over $\mathbb{Q}_2$ with Galois group isomorphic to $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$. If we had $a = 5$, then $F(\sqrt[4]{a})$ would be the splitting field of the polynomial $X^4 - 5$ over $\mathbb{Q}_2$, of which the Galois group is a subgroup of the dihedral group of order 8, which is not abelian. Thus, we have $a \equiv 1+4\mathrm{i} \bmod 2^3\mathcal{O}_K$.

The cyclotomic extension $K(\zeta_{16})/K$ is totally ramified at 2. Theorem 3.86 implies $-1 \notin U^{\perp}$. Since by Theorem 5.17 the 4-th virtual group of K has order 4, it is generated by the residue class of the unit i and is a cyclic subgroup of order 4 of the 4-th unit residue group of K. □

Theorem 6.22. *Let K be the field $\mathbb{Q}(\sqrt{-3})$ and let ζ_6 be a primitive 6-th root of unity in K. Then the 6-th unit residue group of K is isomorphic, as an abelian group, to $(\mathbb{Z}/6\mathbb{Z})^2$ and the 6-th virtual group of K is a cyclic subgroup of order 6 of the 6-th unit residue group of K and is generated by the residue class of ζ_6.*

Proof. By Theorem 5.7 this follows from Theorem 6.15 and Theorem 6.20. □

6.6 Real quadratic number fields

Notation 6.23. Let K be a real quadratic number field, let Δ be its discriminant, let $\mathcal{O}_K$ be the ring of integers of K, and let G be the Galois group $\mathrm{Gal}(K/\mathbb{Q})$.

Theorem 6.24. *Let the notation be as in* Notation 6.23. *Then the 2-nd unit residue group $(\overline{U}/\overline{U}^{\perp}, \{\pm 1\}, (\cdot,\cdot)_{K,2})$ of K is isomorphic, as an abelian group,*

to $(\mathbb{Z}/2\mathbb{Z})^4$*, there is a natural* $(\mathbb{Z}/2\mathbb{Z})[G]$*-module isomorphism*

$$(\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2} \times \left(\bigoplus_{v \text{ real}} \mathbb{R}^*/\mathbb{R}_{>0}\right) \xrightarrow{\sim} \overline{U}/\overline{U}^{\perp} \tag{6.25}$$

that is an isomorphism of skew abelian groups from

$$((\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2}, \{\pm 1\}, \beta) \perp (\bigoplus_{v \text{ real}} \mathbb{R}^*/\mathbb{R}_{>0}, \{\pm 1\}, \gamma)$$

to 2*-nd unit residue group of* K*, where* β *is the unique antisymmetric perfect pairing*

$$\beta : (\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2} \times (\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2} \to \{\pm 1\}$$

that makes $((\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2}, \{\pm 1\}, \beta)$ *into a skew abelian group with skew element* $(-1 + 4\mathcal{O}_K) \cdot (\mathcal{O}_K/4\mathcal{O}_K)^{*2}$ *and* γ *is the antisymmetric perfect pairing*

$$\gamma : \bigoplus_{v \text{ real}} \mathbb{R}^*/\mathbb{R}_{>0} \times \bigoplus_{v \text{ real}} \mathbb{R}^*/\mathbb{R}_{>0} \to \{\pm 1\},$$
$$((a_v \cdot \mathbb{R}_{>0})_v, (b_v \cdot \mathbb{R}_{>0})_v) \mapsto \prod_{v \text{ real}} (-1)^{\frac{a_v - |a_v|_v}{2a_v} \frac{b_v - |b_v|_v}{2b_v}},$$

and the 2*-nd virtual group of* K *is a Galois-stable submodule of the* 2*-nd unit residue group of* K *isomorphic, as an abelian group, to a Klein four-group.*

Proof. Theorem 5.10 gives a group isomorphism $\overline{U}/\overline{U}^{\perp} \xrightarrow{\sim} (\mathbb{Z}/2\mathbb{Z})^4$. The natural $(\mathbb{Z}/2\mathbb{Z})[G]$-module isomorphism 6.25 follows from Theorem 6.10, Theorem 3.81, and Theorem 5.6. By definition the 2-nd virtual group of K is a Galois-stable submodule of the 2-nd unit residue group of K. Theorem 5.17 implies that it has order 4. It is a Klein four-group, because it is a subgroup of order 4 of a group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^4$. □

Each of Theorem 6.26, Theorem 6.27, Theorem 6.28, and Theorem 6.29 describes the 2-nd virtual group of a real quadratic number field in one of the four separate cases of Theorem 6.3.

Theorem 6.26. *Let the notation be as in* Notation 6.23 *and suppose one has* $\Delta \equiv 4 \bmod 8$*. Then the preimage under the natural* $(\mathbb{Z}/2\mathbb{Z})[G]$*-module isomorphism* 6.25 *of the* 2*-nd virtual group* V *of* K *is the direct sum of the submodule of elements of norm congruent to* 1 *modulo* 8 *in* $(\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2}$ *given by* (c) *in* Theorem 6.12 *and the submodule of Galois invariant elements of* $\bigoplus_{v \text{ real}} \mathbb{R}^*/\mathbb{R}_{>0}$*, and* V *is generated, under the surjective group homomorphism* $\{2\text{-virtual units of } K\} \twoheadrightarrow V$ *in* Remark 5.28*, by the images of* -1 *and* 2*.*

Proof. Since 2 divides Δ, the ideal $2\mathcal{O}_K$ is the square of an ideal of the ring of integers $\mathcal{O}_K$ of K. Hence, the integer 2 is a 2-virtual unit of K. All three subextensions of $K(\sqrt{2})/\mathbb{Q}$ of degree 2 over $\mathbb{Q}$ are ramified at 2. Hence, the extension $K(\sqrt{2})/K$ is also ramified at 2. Theorem 3.86 and Remark 5.28 imply that the integer 2 is not in the kernel of the group homomorphism $\{\text{2-virtual units of } K\} \to V$. Looking at the real components of the 2-nd unit residue group of K shows that the group generated by the image of 2 does not contain the image of -1. Since by Theorem 6.24 the 2-nd virtual group V of K is a Klein four-group, the images of -1 and 2 generate V.

Now we consider the $(\mathbb{Z}/2\mathbb{Z})[G]$-module isomorphism given by (c) in Theorem 6.12. Multiplying 2 by squares of elements in K^*, which are in the kernel of the group homomorphism $\{\text{2-virtual units of } K\} \to V$, we can get a 2-virtual unit coprime to 2. Its norm equals the square of an odd integer in $\mathbb{Z}$ and therefore it is congruent to 1 modulo 8. Hence, this 2-virtual unit generates the submodule of elements of norm congruent to 1 modulo 8 of $(\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2}$. Moreover, it is the identity element at the real components of the 2-nd unit residue group of K. Since -1 generates the submodule of Galois invariant elements of $\bigoplus_{v \text{ real}} \mathbb{R}^*/\mathbb{R}_{>0}$ and its norm equals 1, the statement about the preimage of V follows. □

Theorem 6.27. *Let the notation be as in* Notation 6.23. *Suppose one has* $\Delta \not\equiv 4 \bmod 8$ *and let* p *be a prime congruent to* 3 *modulo* 4 *that divides* Δ. *Then the preimage under the natural* $(\mathbb{Z}/2\mathbb{Z})[G]$*-module isomorphism* 6.25 *of the* 2*-nd virtual group* V *of* K *is the submodule of Galois invariant elements of the* 2*-nd unit residue group of* K*, and* V *is generated, under the surjective group homomorphism* $\{\text{2-virtual units of } K\} \twoheadrightarrow V$ *in* Remark 5.28*, by the images of* -1 *and* p.

Proof. The ideal $p\mathcal{O}_K$ is the square of an ideal of the ring of integers $\mathcal{O}_K$ of K, because p divides Δ. Hence, the integer p is a 2-virtual unit of K. When we have $\Delta \equiv 0 \bmod 8$, the three subextensions of $K(\sqrt{p})/\mathbb{Q}$ of degree 2 over $\mathbb{Q}$ are ramified at 2, whereas for $\Delta \equiv 1 \bmod 4$ the extension $\mathbb{Q}(\sqrt{\Delta})/\mathbb{Q}$ is unramified at 2 and $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$ is ramified at 2. In both cases, the extension $K(\sqrt{p})/K$ is ramified at 2. Theorem 3.86 and Remark 5.28 imply that the integer p is not in the kernel of the group homomorphism $\{\text{2-virtual units of } K\} \to V$. Looking at the real components of the 2-nd unit residue group of K shows that the group generated by the image of p does not contain the image of -1. By Theorem 6.24 the 2-nd virtual group V of K is a Klein four-group and therefore V is generated by the images of -1 and p.

Combining the natural $(\mathbb{Z}/2\mathbb{Z})[G]$-module isomorphism 6.25 with (a) and (b) in Theorem 6.12 shows that the submodule of Galois invariant elements of the 2-nd unit residue group of K has order 4. Since both p and -1 are Galois invariant and their images generate a submodule of order 4, the statement

about the preimage of V follows. □

Theorem 6.28. *Let the notation be as in* Notation 6.23. *Suppose one has* $\Delta \equiv 0 \bmod 8$ *and let* a *and* b *be integers that satisfy* $\Delta = 4(a^2+b^2)$. *Then the preimage of the* 2*-nd virtual group* V *of* K *under the natural* $(\mathbb{Z}/2\mathbb{Z})[G]$*-module isomorphism* 6.25 *is the graph of the group isomorphism*

$$(\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2} \xrightarrow{\sim} \bigoplus_{v \text{ real}} \mathbb{R}^*/\mathbb{R}_{>0}$$

that for each $\delta \in \mathcal{O}_K$ *satisfying* $\delta^2 = \Delta/4$ *sends* $(1+\delta+4\mathcal{O}_K)\cdot(\mathcal{O}_K/4\mathcal{O}_K)^{*2}$ *to* $(\delta_v \cdot \mathbb{R}_{>0})_v$, *and* V *is generated, under the surjective group homomorphism* $\{2\text{-virtual units of } K\} \twoheadrightarrow V$ *in* Remark 5.28, *by the images of the elements* -1 *and* $a - \sqrt{\Delta/4}$.

Proof. Let $d = \Delta/4$. Since d is squarefree, the integers d and b are coprime and both a and b are odd. We claim that the principal ideals of the ring of integers $\mathcal{O}_K$ of K generated by $a+\sqrt{d}$ and by $a-\sqrt{d}$ are coprime. Their sum ideal contains $4d$ and b^2, because we have

$$4d = (a+\sqrt{d}-(a-\sqrt{d}))^2 \quad \text{and} \quad b^2 = -(a+\sqrt{d})(a-\sqrt{d}).$$

Since the integers $4d$ and b^2 are coprime, it also contains 1. Hence, the ideals $(a+\sqrt{d})\mathcal{O}_K$ and $(a-\sqrt{d})\mathcal{O}_K$ are coprime. They are squares of coprime ideals, because their product is the square of an ideal. It follows that the element $a-\sqrt{d}$ is a 2-virtual unit of K. Let v be the real place of K with $(a-\sqrt{d})_v < 0$. The extension $K(\sqrt{a-\sqrt{d}})/K$ is ramified at v, because we have $(a-\sqrt{d})_v < 0$. Remark 5.28 implies that $a-\sqrt{d}$ is not in the kernel of the group homomorphism $\{2\text{-virtual units of } K\} \to V$. Looking at the real components of the 2-nd unit residue group of K shows that the group generated by the image of $a-\sqrt{d}$ does not contain the image of -1. Since by Theorem 6.24 the 2-nd virtual group V of K is a Klein four-group, it is generated by the images of -1 and $a-\sqrt{d}$. This argument is also used in the proof of Theorem 6.29 with d replaced by Δ.

A straightforward computation shows the congruence

$$1-\sqrt{d} \equiv (3-\sqrt{d})(1-\sqrt{d})^2 \bmod 4\mathcal{O}_K.$$

Since a is odd, the residue classes of the elements $a-\sqrt{d}$ and $1-\sqrt{d}$ in the group $(\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2}$ are equal. The statement about the preimage of V follows. □

Theorem 6.29. *Let the notation be as in* Notation 6.23. *Suppose one has* $\Delta \equiv 1 \bmod 4$ *and let* a *and* b *be integers that satisfy* $\Delta = 4a^2+b^2$. *Then the*

preimage of the 2*-nd virtual group* V *of* K *under the natural* $(\mathbb{Z}/2\mathbb{Z})[G]$*-module isomorphism* 6.25 *is the graph of the group isomorphism*

$$(\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2} \xrightarrow{\sim} \bigoplus_{v \text{ real}} \mathbb{R}^*/\mathbb{R}_{>0}$$

that for each $\delta \in \mathcal{O}_K$ *satisfying* $\delta^2 = \Delta$ *sends* $(\delta + 4\mathcal{O}_K) \cdot (\mathcal{O}_K/4\mathcal{O}_K)^{*2}$ *to* $((-1)^{\frac{\Delta-1}{4}}\delta_v \cdot \mathbb{R}_{>0})_v$*, and* V *is generated, under the surjective group homomorphism* {2-virtual units of K} $\twoheadrightarrow V$ *in* Remark 5.28*, by the images of* -1 *and* $2a - \sqrt{\Delta}$*.*

Proof. Since Δ is squarefree, the integers Δ and b are coprime. We claim that the principal ideals of the ring of integers $\mathcal{O}_K$ of K generated by $2a+\sqrt{\Delta}$ and by $2a-\sqrt{\Delta}$ are coprime. Their sum ideal contains 4Δ and b^2, because we have

$$4\Delta = (2a + \sqrt{\Delta} - (2a - \sqrt{\Delta}))^2 \quad \text{and} \quad b^2 = -(2a + \sqrt{\Delta})(2a - \sqrt{\Delta}).$$

Since the integers 4Δ and b^2 are coprime, it also contains 1. Hence, the ideals $(2a + \sqrt{\Delta})\mathcal{O}_K$ and $(2a - \sqrt{\Delta})\mathcal{O}_K$ are coprime. They are squares of coprime ideals, because their product is the square of an ideal. It follows that the element $2a - \sqrt{\Delta}$ is a 2-virtual unit of K. Let v be the real place of K with $(2a - \sqrt{\Delta})_v < 0$. The extension $K(\sqrt{2a - \sqrt{\Delta}})/K$ is ramified at v, because we have $(2a - \sqrt{\Delta})_v < 0$. Remark 5.28 implies that $2a - \sqrt{\Delta}$ is not in the kernel of the group homomorphism {2-virtual units of K} $\to V$. Looking at the real components of the 2-nd unit residue group of K shows that the group generated by the image of $2a - \sqrt{\Delta}$ does not contain the image of -1. Since by Theorem 6.24 the 2-nd virtual group V of K is a Klein four-group, it is generated by the images of -1 and $2a - \sqrt{\Delta}$. This argument is also used in the proof of Theorem 6.28 with Δ replaced by d, which equals $\Delta/4$.

From the congruence $(\sqrt{\Delta})^2 \equiv 1 \bmod 4\mathcal{O}_K$ we get $\sqrt{\Delta} \equiv 1 \bmod 2\mathcal{O}_K$. Moreover, the integer 2 divides a if and only if we have $\Delta \equiv 1 \bmod 8$. Hence, we have the congruence

$$2a + \sqrt{\Delta} \equiv (-1)^{\frac{\Delta-1}{4}}\sqrt{\Delta} \bmod 4\mathcal{O}_K.$$

Since the residue classes of the elements $2a - \sqrt{\Delta}$ and $-(-1)^{\frac{\Delta-1}{4}}\sqrt{\Delta}$ in the group $(\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2}$ are equal, the statement about the preimage of V follows. □

Corollary 6.30. *Let the notation be as in* Notation 6.23*. Then the following are equivalent.*

(i) *The* 2*-nd virtual group of* K *is a free* $(\mathbb{Z}/2\mathbb{Z})[G]$*-module of rank* 1*.*

(ii) *The action of* G *on the* 2*-nd virtual group of* K *is not trivial.*

(iii) *The discriminant of* K *is the sum of two squares of integers.*

Proof. Theorem 6.24 states that V is a Klein four-group. Hence (i) and (ii) are equivalent. Theorem 6.26, Theorem 6.27, Theorem 6.28, and Theorem 6.29 imply that (ii) and (iii) are equivalent. □

6.7 The number field $\mathbb{Q}(\mathrm{i}, \sqrt{30})$

Theorem 6.31. *Let K be the number field $\mathbb{Q}(\mathrm{i}, \sqrt{30})$. Then the 4-th virtual group of K* [Definition 5.15] *is the maximal subgroup of exponent 2 of the 4-th unit residue group of K* [Definition 5.3].

Proof. We fix an algebraic closure of K. Let V be the 4-th virtual group of K, let F be the number field

$$F = K(\sqrt[4]{\mathrm{i}}, \sqrt{1+\mathrm{i}}, \sqrt{1+2\mathrm{i}}, \sqrt[4]{11+2\sqrt{30}}),$$

and let L be the number field

$$L = \mathbb{Q}(\mathrm{i}, \sqrt{2}, \sqrt{3}, \sqrt{5}).$$

We will show that F and L are the field extensions of K we get by adjoining the fourth roots of all 4-virtual units of K [Definition 5.23] and of all elements in the kernel of the surjective group homomorphism $\{\text{4-virtual units of } K\} \twoheadrightarrow V$ in Remark 5.28, respectively. Moreover, we denote by M the number field

$$M = \mathbb{Q}(\mathrm{i})(\sqrt{\mathrm{i}}, \sqrt{1+\mathrm{i}}, \sqrt{3}, \sqrt{1+2\mathrm{i}}, \sqrt{1-2\mathrm{i}}).$$

We claim that L is the Hilbert class field of K. The extension L/K is unramified at infinity. The rational prime 2 is unramified in both $\mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(\sqrt{5})$. Hence, it is unramified in $\mathbb{Q}(\sqrt{-3}, \sqrt{5})$ by Lemma 6.5. Since L is the compositum of $\mathbb{Q}(\sqrt{-3}, \sqrt{5})$ and K, Lemma 6.4 shows that the extension L/K is unramified at the prime above 2. Lemma 6.5 implies that the rational prime 5 is unramified in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, because it is unramified in both $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$. Since L is the compositum of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ and K, by Lemma 6.4 the extension L/K is unramified at the primes above 5. A similar argument shows that L/K is also unramified at the prime above 3. For any other finite place v of $\mathbb{Q}$ it is sufficient to note that all quadratic subextensions of L over $\mathbb{Q}$ are unramified at v. By Lemma 6.5 the extension L/K is unramified at v. Since in [45] the ideal class group of K is proved to be isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, the number field L is the Hilbert class field of K.

We are going to prove the equality

$$L = K(\sqrt{\mathrm{i}}, \sqrt{11+2\sqrt{30}}).$$

The equality $\mathbb{Q}(\mathrm{i}, \sqrt{2}) = \mathbb{Q}(\mathrm{i})(\sqrt{\mathrm{i}})$ follows from the identities

$$\left(\frac{1+\mathrm{i}}{\sqrt{2}}\right)^2 = \mathrm{i} \quad \text{and} \quad \left(\frac{1+\mathrm{i}}{\sqrt{\mathrm{i}}}\right)^2 = 2.$$

Let $\varepsilon = 11 + 2\sqrt{30}$ and let $\mathcal{O}_K$ be the ring of integers of K. Since we have $\mathrm{N}_{\mathbb{Q}(\sqrt{30})/\mathbb{Q}}\,\varepsilon = 1$, the element ε is a unit in $\mathcal{O}_K$. The identities

$$(\sqrt{5}+\sqrt{6})^2 = \varepsilon, \quad \left(\frac{\sqrt{\varepsilon}^3 - 21\sqrt{\varepsilon}}{2}\right)^2 = 5, \quad \left(\frac{\sqrt{\varepsilon}^3 - 23\sqrt{\varepsilon}}{2}\right)^2 = 6$$

imply the equality $\mathbb{Q}(\sqrt{5}, \sqrt{6}) = \mathbb{Q}(\sqrt{30})(\sqrt{\varepsilon})$. Since the compositum of $\mathbb{Q}(\mathrm{i}, \sqrt{2})$ and $\mathbb{Q}(\sqrt{5}, \sqrt{6})$ is the number field L and the compositum of $\mathbb{Q}(\mathrm{i})(\sqrt{\mathrm{i}})$ and $\mathbb{Q}(\sqrt{30})(\sqrt{\varepsilon})$ is the number field $K(\sqrt{\mathrm{i}}, \sqrt{\varepsilon})$, we get the equality $L = K(\sqrt{\mathrm{i}}, \sqrt{\varepsilon})$, as claimed.

The inclusion $L \subseteq F$ follows from the equality $L = K(\sqrt{\mathrm{i}}, \sqrt{\varepsilon})$. Kummer theory shows that the subgroup of $\mathcal{O}_K^*/{\mathcal{O}_K^*}^2$ generated by the residue classes of i and ε has order 4, because the degree of the field extension L/K equals 4. Dirichlet's unit theorem implies that $\langle \mathrm{i}, \varepsilon \rangle$ is subgroup of $\mathcal{O}_K^*$ of odd index.

We claim that the Galois group $\mathrm{Gal}(M/\mathbb{Q}(\mathrm{i}))$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^5$. The number field $\mathbb{Q}(\mathrm{i})$ has class number 1. In the ring of integers of $\mathbb{Q}(\mathrm{i})$ we have the prime factorizations $2 = -\mathrm{i}(1+\mathrm{i})^2$, $3 = 3$, and $5 = (1+2\mathrm{i})(1-2\mathrm{i})$. They show that the subgroup of $\mathbb{Q}(\mathrm{i})^*/\mathbb{Q}(\mathrm{i})^{*2}$ generated by the residue classes of the elements in the set $\{\mathrm{i}, 1+\mathrm{i}, 3, 1+2\mathrm{i}, 1-2\mathrm{i}\}$ has order 32. Now the claim follows from Kummer theory. These prime factorizations also show the chain of inclusions $L \subseteq M \subseteq F$.

The Galois group $\mathrm{Gal}(M/K)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^4$, because the extension $K/\mathbb{Q}(\mathrm{i})$ has degree 2 and the Galois group $\mathrm{Gal}(M/\mathbb{Q}(\mathrm{i}))$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^5$. Since F can be obtained from K by adjoining two square roots and two fourth roots of elements in K^* and F contains M, the 2-rank of the Galois group $\mathrm{Gal}(F/K)$ equals 4. Kummer theory gives a group isomorphism

$$\mathrm{Gal}(F/K) \xrightarrow{\sim} (\mathbb{Z}/4\mathbb{Z})^2 \times (\mathbb{Z}/2\mathbb{Z})^2,$$

because the subgroup of K^*/K^{*4} generated by the residue classes of i and ε is isomorphic to $(\mathbb{Z}/4\mathbb{Z})^2$.

At each prime of $\mathcal{O}_K$ the elements i and $11 + 2\sqrt{30}$ have valuation zero, because they are units in $\mathcal{O}_K$. At each prime of $\mathcal{O}_K$ not dividing 2 the elements $1+\mathrm{i}$ and $1+2\mathrm{i}$ have even valuation, while at the prime above 2 the element $1+2\mathrm{i}$ has valuation zero and $1+\mathrm{i}$ has valuation two. Hence, we have the inclusion

$$\langle \mathrm{i}, 11 + 2\sqrt{30}, (1+\mathrm{i})^2, (1+2\mathrm{i})^2 \rangle \cdot K^{*4} \subseteq \{\text{4-virtual units of } K\}.$$

Consider the surjective group homomorphism

$$\{4\text{-virtual units of } K\}/K^{*4} \twoheadrightarrow V$$

in Remark 5.28. Since we have $L = K(\sqrt{\mathrm{i}}, \sqrt{11 + 2\sqrt{30}})$ and L/K is the maximal unramified abelian extension of K of exponent dividing 4, by Remark 5.28 and Kummer theory the kernel of this map is the group

$$\langle -1, (11 + 2\sqrt{30})^2 \rangle \cdot K^{*4}/K^{*4}$$

and has order the degree of the extension L/K, which equals 4. The group V has order 16 by Theorem 5.17. Hence, the group $\{4\text{-virtual units of } K\}/K^{*4}$ has order 64. Kummer theory gives the equality

$$\{4\text{-virtual units of } K\}/K^{*4} = \langle \mathrm{i}, 11 + 2\sqrt{30}, (1 + \mathrm{i})^2, (1 + 2\mathrm{i})^2 \rangle \cdot K^{*4}/K^{*4},$$

because the abelian extension F/K has degree 64. Since V has order 16 and is isomorphic to the quotient group

$$\langle \mathrm{i}, 11 + 2\sqrt{30}, (1 + \mathrm{i})^2, (1 + 2\mathrm{i})^2 \rangle \cdot K^{*4}/\langle -1, (11 + 2\sqrt{30})^2 \rangle \cdot K^{*4},$$

which has exponent 2, we get a group isomorphism

$$V \xrightarrow{\sim} (\mathbb{Z}/2\mathbb{Z})^4.$$

Since by Theorem 5.10 the 4-th unit residue group of K is isomorphic to $(\mathbb{Z}/4\mathbb{Z})^4$, the group V is the maximal subgroup of exponent 2 of the 4-th unit residue group of K. □

CHAPTER 7

Two-ranks of ideal class groups

7.1 Results

Let K be a number field. The 2-nd virtual group of K [Definition 5.15] is a subgroup of the 2-nd unit residue group of K [Definition 5.3], which is an elementary abelian 2-group [Theorem 5.10]. The projection of the 2-nd virtual group of K on the product of local components of the 2-nd unit residue group of K at the places dividing 2 measures the difference between the 2-ranks of the ideal class groups of K in the strict sense [Definition 7.1] and in the usual sense [Theorem 7.2]. A bound on the 2-rank of this projection is given in Corollary 5.22. Theorem 7.4 states the exact value of this 2-rank for quadratic number fields. Theorem 7.5, which is a classical result in genus theory for quadratic number fields, is obtained as a corollary of Theorem 7.2 and Theorem 7.4.

Theorem 7.2 and Corollary 5.22 are the main results. As corollaries, in Section 7.2 are presented the classical theorem of Armitage–Fröhlich [Theorem 7.8] and Oriat's theorem [Theorem 7.6].

Definition 7.1 (Strict ideal class group)**.** Let K be a number field and let $\mathcal{O}_K$ be its ring of integers. The *strict ideal class group* Cl^+ of K is the quotient group of the group of fractional ideals of $\mathcal{O}_K$ modulo the subgroup of principal ideals generated by totally positive elements.

Theorem 7.2. *Let K be a number field, let r_1 be the number of real embeddings $K \hookrightarrow \mathbb{R}$, and let r_2 be the number of conjugate pairs of complex embeddings*

$\sigma : K \hookrightarrow \mathbb{C}$ with $\sigma(K) \not\subseteq \mathbb{R}$. Let Cl *and* Cl^+ *be the ideal class group of K and the strict ideal class group of K, respectively. Let S be the set of places of K, let π_2 be the canonical projection*

$$\pi_2 : \prod_{v \in S} U_v / U_v^{\perp} \twoheadrightarrow \prod_{v \mid 2} U_v / U_v^{\perp}$$

of the 2-nd unit residue group of K [Definition 5.3] *on the product of its local components at the places dividing 2, and let V be the 2-nd virtual group of K* [Definition 5.15]. *Then one has*

$$\mathrm{rk}_2 \mathrm{Cl}^+ - \mathrm{rk}_2 \mathrm{Cl} = r_1 + r_2 - \mathrm{rk}_2 \pi_2(V).$$

Proof. See Section 7.3. □

Remark 7.3. Let the notation be as in Theorem 7.2. Corollary 5.22 states the inequality

$$\mathrm{rk}_2 \pi_2(V) \geq \left\lceil \frac{[K : \mathbb{Q}]}{2} \right\rceil .$$

In the case of quadratic number fields we compute $\mathrm{rk}_2 \pi_2(V)$ in Theorem 7.2 using the results about the 2-virtual group of quadratic number fields in Chapter 6.

Theorem 7.4. *Let the notation be as in* Theorem 7.2 *with K a quadratic number field. Then* $\mathrm{rk}_2 \pi_2(V)$ *equals either* 2 *or* 1*, according as the discriminant of K is or is not the sum of two squares of integers.*

Proof. Firstly, we consider the case when K is an imaginary quadratic field. Since there are no real Archimedean places of K, Theorem 5.1 implies that the 2-nd unit residue group of K has nontrivial components only at the places dividing 2. By Theorem 6.15 we get $\mathrm{rk}_2 \pi_2(V) = 1$.

Now we suppose that K is a real quadratic field. Theorem 6.26, Theorem 6.27, Theorem 6.28, and Theorem 6.29 imply that $\mathrm{rk}_2 \pi_2(V)$ equals either 2 or 1, according as the discriminant of K is or is not the sum of two squares of integers. □

As a corollary of Theorem 7.2 and Theorem 7.4 we get a classical result in genus theory for real quadratic number fields. As a reference see Proposition 2.12 in Section 2.2 of Chapter 2 in [37] by Lemmermeyer.

Theorem 7.5. *Let K be a real quadratic number field, let* Cl *be the ideal class group of K, and let* Cl^+ *be the strict ideal class group of K. Then the following are equivalent.*

(i) *One has* $\mathrm{Cl}^+ / {\mathrm{Cl}^+}^2 \xrightarrow{\sim} \mathrm{Cl} \,/\, \mathrm{Cl}^2$.

(ii) *The discriminant of K is the sum of two squares of integers.*

Proof. This follows from Theorem 7.2 and Theorem 7.4. □

7.2 Armitage–Fröhlich's theorem

In 1967, Armitage and Fröhlich [1] found a bound on the 2-rank of the ideal class group of a number field [Theorem 7.8]. A crucial fact in their proof follows from the functional equation of an L-function. Serre pointed out that it was possible to avoid bringing in analytic tools. The note added to the paper by Armitage and Fröhlich contains the proof by Serre.

In 1976, Oriat [53] proved a stronger result [Theorem 7.6] by an algebraic method that does not require the bilinear form introduced by Serre, but some groups that are subgroups of what is now called 2-Selmer group of a number field [Definition 5.25]. Lemmermeyer [38] gave a proof of Oriat's result, which he calls 'the theorem of Armitage–Fröhlich', using the 2-Selmer group of a number field. In his paper he claims that his proof is essentially due to Oriat. Another proof of the same result was given by Hayes [24]. His argument uses Galois groups of the Kummer extensions corresponding to elements in the 2-Selmer group of a number field.

The proof of Oriat's result presented here is a straightforward application of Theorem 7.2 and Corollary 5.22. The proof of Theorem 7.2 involves the 2-Selmer group of a number field and arguments similar to those used by Lemmermeyer, but it introduces the 2-virtual group of a number field. In this way, it is then possible to apply Corollary 5.22.

Theorem 7.6 (Oriat [53])**.** *Let K be a number field, let r_1 be the number of real embeddings $K \hookrightarrow \mathbb{R}$, let* Cl *and* Cl^+ *be the ideal class group of K and the strict ideal class group of K, respectively. Then one has*

$$\operatorname{rk}_2 \mathrm{Cl}^+ - \operatorname{rk}_2 \mathrm{Cl} \leq \left\lfloor \frac{r_1}{2} \right\rfloor .$$

Proof. Let V be the 2-nd virtual group of K and let r_2 be the number of conjugate pairs of complex embeddings $\sigma : K \hookrightarrow \mathbb{C}$ with $\sigma(K) \not\subseteq \mathbb{R}$. Theorem 7.2 states the equality

$$\operatorname{rk}_2 \mathrm{Cl}^+ - \operatorname{rk}_2 \mathrm{Cl} = r_1 + r_2 - \operatorname{rk}_2 \pi_2(V).$$

Since we have $[K : \mathbb{Q}] = r_1 + 2r_2$, Corollary 5.22 implies

$$\operatorname{rk}_2 \pi_2(V) \geq r_1 + r_2 - \left\lfloor \frac{r_1}{2} \right\rfloor .$$

The desired inequality follows. □

Lemma 7.7. *Let the notation be as in* Theorem 7.6 *and let E and E^+ be the group of units and the group of totally positive units, respectively, of the ring of integers of K. Then one has*

$$\operatorname{rk}_2 \mathrm{Cl}^+ \geq r_1 - \operatorname{rk}_2 E/E^+.$$

Proof. Let K_+^* be the group of totally positive elements in K^*. The natural map $\mathrm{Cl}^+ \to \mathrm{Cl}$ fits into the exact sequence

$$1 \longrightarrow E/E^+ \longrightarrow K^*/K_+^* \longrightarrow \mathrm{Cl}^+ \longrightarrow \mathrm{Cl} \longrightarrow 1.$$

Since E/E^+ and K^*/K_+^* are elementary abelian 2-groups and $\mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \cdot)$ is a left exact functor, we get an exact sequence

$$1 \longrightarrow E/E^+ \longrightarrow K^*/K_+^* \longrightarrow \mathrm{Cl}^+[2].$$

Hence, we have the inequality

$$\mathrm{rk}_2\,\mathrm{Cl}^+ + \mathrm{rk}_2\,E/E^+ \geq \mathrm{rk}_2\,K^*/K_+^*.$$

Theorem 5.14 implies that $\mathrm{rk}_2\,K^*/K_+^*$ equals r_1. The inequality in the statement of Lemma 7.7 follows. □

Theorem 7.8 (Armitage–Fröhlich [1])**.** *Let K be a number field, let r_1 be the number of real embeddings of K, let E and E^+ be the group of units and the group of totally positive units, respectively, of the ring of integers of K, and let* Cl *be the ideal class group of K. Then one has*

$$\mathrm{rk}_2\,\mathrm{Cl} \geq \left\lceil \frac{r_1}{2} \right\rceil - \mathrm{rk}_2\,E/E^+.$$

Proof. This follows from Theorem 7.6 and Lemma 7.7. □

7.3 Proof of the main theorem

Proof of Theorem 7.2. Let $\varphi_2 : \{\text{2-virtual units of } K\} \to \pi_2(V)$ be the composite map of the surjective group homomorphism $\{\text{2-virtual units of } K\} \twoheadrightarrow V$ in Remark 5.28 with the projection π_2. Note that a 2-virtual unit $a \in K^*$ is in $\ker\varphi_2$ if and only if the extension $K(\sqrt{a})/K$ is unramified outside infinity. In particular, we have $K^{*2} \subseteq \ker\varphi_2$. Let

$$\overline{\varphi_2} : \{\text{2-virtual units of } K\}/K^{*2} \to \pi_2(V)$$

be the natural map induced by φ_2 and consider the short exact sequence

$$1 \longrightarrow \ker\overline{\varphi_2} \longrightarrow \{\text{2-virtual units of } K\}/K^{*2} \xrightarrow{\overline{\varphi_2}} \pi_2(V) \longrightarrow 1.$$

Since all nontrivial groups in this exact sequence are elementary abelian 2-groups, we have the equality of 2-ranks

$$\mathrm{rk}_2\{\text{2-virtual units of } K\}/K^{*2} = \mathrm{rk}_2\ker\overline{\varphi_2} + \mathrm{rk}_2\,\pi_2(V).$$

Dirichlet's unit theorem and Theorem 5.29 give

$$\mathrm{rk}_2\{\text{2-virtual units of } K\}/{K^*}^2 = r_1 + r_2 + \mathrm{rk}_2\,\mathrm{Cl}\,.$$

Kummer theory and class field theory imply

$$\mathrm{rk}_2 \ker \overline{\varphi_2} = \mathrm{rk}_2\,\mathrm{Cl}^+\,.$$

The equality

$$\mathrm{rk}_2\,\mathrm{Cl}^+ - \mathrm{rk}_2\,\mathrm{Cl} = r_1 + r_2 - \mathrm{rk}_2\,\pi_2(V)$$

follows. □

CHAPTER 8

Three-ranks of ideal class groups of quadratic number fields

8.1 Introduction

Let $d \in \mathbb{Z}_{>1}$ be squarefree and let K be the number field $\mathbb{Q}(\sqrt{d},\sqrt{-3})$. The biquadratic number field K contains a primitive 3-rd root of unity and has its 3-rd unit residue group [Definition 5.3] and 3-rd virtual group [Definition 5.15]. The number field extension $K/\mathbb{Q}$ is Galois and the description of the Galois module structure of these two groups is one of the main results of the chapter [Theorem 8.1].

Theorem 8.1. *Let $d \in \mathbb{Z}_{>1}$ be squarefree, let K be the number field $\mathbb{Q}(\sqrt{d},\sqrt{-3})$, and let G be the Galois group of the extension $K/\mathbb{Q}$. Then the 3-rd unit residue group of K is a free $(\mathbb{Z}/3\mathbb{Z})[G]$-module of rank 1. Moreover, the 3-rd virtual group of K is a submodule of the 3-rd unit residue group of K and corresponds to exactly one of the following modules:*

(a) *the kernel of the natural map $(\mathbb{Z}/3\mathbb{Z})[G] \to (\mathbb{Z}/3\mathbb{Z})[\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})]$,*
(b) *the kernel of the natural map $(\mathbb{Z}/3\mathbb{Z})[G] \to (\mathbb{Z}/3\mathbb{Z})[\mathrm{Gal}(\mathbb{Q}(\sqrt{-3d})/\mathbb{Q})]$.*

Proof. This follows from Theorem 8.18 and Theorem 8.17. □

A classical theorem of Scholz [Theorem 8.19] states that the difference between the 3-rank of the ideal class group of $\mathbb{Q}(\sqrt{-3d})$ and the 3-rank of the ideal class group of $\mathbb{Q}(\sqrt{d})$ is either 0 or 1. Theorem 8.2 shows that these two cases can

be distinguished by looking at the Galois module structure of the 3-rd virtual group of K.

Theorem 8.2. *Let $d \in \mathbb{Z}_{>1}$ be squarefree, let r be the 3-rank of the ideal class group of $\mathbb{Q}(\sqrt{d})$, let s be the 3-rank of the ideal class group of $\mathbb{Q}(\sqrt{-3d})$, and let K be the number field $\mathbb{Q}(\sqrt{d},\sqrt{-3})$. Then in case* (a) *of* Theorem 8.1 *one has $s = r + 1$ and in case* (b) *of* Theorem 8.1 *one has $s = r$.*

Proof. This follows from the G-decompositions of the $(\mathbb{Z}/3\mathbb{Z})[G]$-modules in cases (a) and (b) of Theorem 8.1 and Theorem 8.17. □

As a byproduct we get a new proof of Scholz's theorem, but the ingredients are really the same as in earlier proofs. In Section 8.3 we show the G-decompositions of some $(\mathbb{Z}/3\mathbb{Z})[G]$-modules and use the duality given by the norm-residue symbol. In this way we simultaneously apply class field theory and Kummer theory, as is done more explicitly in the proof of Scholz's Theorem [Theorem 10.10 of Chapter 10 in [74]] by Washington.

In 1984 Dutarte [14] proposed a probabilistic model [Section 8.5] that leads to Conjecture 8.3 and studied the compatibility of the Cohen–Lenstra heuristics with Scholz's theorem. He showed that the Cohen–Lenstra heuristics for real quadratic fields, Scholz's theorem, and Conjecture 8.3 give the same result for the proportion of imaginary quadratic fields with prescribed 3-rank as the Cohen-Lenstra heuristics for imaginary quadratic fields.

Conjecture 8.3 (Dutarte [14])**.** *Let D^+ be the set of discriminants of real quadratic number fields. For each number field L let Cl_L be its ideal class group. Then for every nonnegative integer a one has*

$$\lim_{x\to+\infty} \frac{|\{\Delta \in D^+ : \Delta < x,\, \mathrm{rk}_3\, \mathrm{Cl}_{\mathbb{Q}(\sqrt{\Delta})} = a,\, \mathrm{rk}_3\, \mathrm{Cl}_{\mathbb{Q}(\sqrt{-3\Delta})} = a+1\}|}{|\{\Delta \in D^+ : \Delta < x,\, \mathrm{rk}_3\, \mathrm{Cl}_{\mathbb{Q}(\sqrt{\Delta})} = a\}|} = \frac{1}{3^{a+1}}.$$

In Dutarte's model Conjecture 8.3 is a statement about the existence and the value of a conditional probability: the probability that the 3-rank of the ideal class group of $\mathbb{Q}(\sqrt{-3\Delta})$ is the positive integer $a+1$ given that Δ is a discriminant of a real quadratic number field whose ideal class group has 3-rank a.

Following his model we state Conjecture 8.4.

Conjecture 8.4. *Let the notation be as in* Conjecture 8.3*. Then for every nonnegative integer a one has*

$$\lim_{x\to+\infty} \frac{|\{\Delta \in D^+ : \Delta < x,\, \mathrm{rk}_3\, \mathrm{Cl}_{\mathbb{Q}(\sqrt{\Delta})} = a,\, \mathrm{rk}_3\, \mathrm{Cl}_{\mathbb{Q}(\sqrt{-3\Delta})} = a\}|}{|\{\Delta \in D^+ : \Delta < x,\, \mathrm{rk}_3\, \mathrm{Cl}_{\mathbb{Q}(\sqrt{-3\Delta})} = a\}|} = \frac{1}{3^{a}}.$$

A natural assumption is Conjecture 8.5.

Conjecture 8.5. *Let the notation be as in* Conjecture 8.3. *Then for each pair* $(a, b) \in \mathbb{Z}^2$ *the limit*

$$\lim_{x \to +\infty} \frac{|\{\Delta \in D^+ : \Delta < x,\, \mathrm{rk}_3 \mathrm{Cl}_{\mathbb{Q}(\sqrt{\Delta})} = a,\, \mathrm{rk}_3 \mathrm{Cl}_{\mathbb{Q}(\sqrt{-3\Delta})} = b\}|}{|\{\Delta \in D^+ : \Delta < x\}|}$$

exists. Moreover, if one denotes its value by $\Pr^+(r = a, s = b)$, *then one has*

$$\sum_{(a,b) \in \mathbb{Z}^2} \Pr^+(r = a, s = b) = 1.$$

Theorem 8.6. *Let the notation be as in* Conjecture 8.3. *Assume* Conjecture 8.3, Conjecture 8.4, *and* Conjecture 8.5. *Then for each nonnegative integer* a *the limit*

$$\lim_{x \to +\infty} \frac{|\{\Delta \in D^+ : \Delta < x,\, \mathrm{rk}_3 \mathrm{Cl}_{\mathbb{Q}(\sqrt{\Delta})} = a\}|}{|\{\Delta \in D^+ : \Delta < x\}|}$$

equals

$$3^{-a(a+1)} \prod_{i=1}^{\infty} (1 - 3^{-i}) \prod_{i=1}^{a} (1 - 3^{-i})^{-1} \prod_{i=1}^{a+1} (1 - 3^{-i})^{-1}.$$

Proof. This follows from Theorem 8.31. □

Remark 8.7. The value of the limit in Theorem 8.6 is the value conjectured by Cohen and Lenstra [11].

Theorem 8.6 shows that Dutarte's assumption [Conjecture 8.3], an analogous assumption [Conjecture 8.4], and a natural assumption [Conjecture 8.5] are sufficient to compute the probability that a real quadratic number field has prescribed 3-rank. Moreover, the value of this probability is exactly the one predicted by the Cohen–Lenstra heuristics.

Under the same hypotheses we also get a similar result for complex quadratic number fields [Theorem 8.31], but the fields in our limit are ordered in a different way from the way they are ordered in the Cohen–Lenstra heuristics [Remark 8.35]. We are able to get the same order and again the values predicted by Cohen and Lenstra for both real and imaginary quadratic number fields, if we group together quadratic number fields according to the divisibility by 3 of their discriminants [Theorem 8.42 and Remark 8.44].

The idea of considering the divisibility by 3 in this context is not new. In 2010 Fouvry and Klüners [16] showed that Conjecture 8.3 follows from the Cohen–Lenstra heuristics for quadratic number fields grouped according to the divisibility by 3 of their discriminants.

Lee generalized Dutarte's results for the prime number 3 to every prime number. In Lee's papers Scholz's theorem is replaced by the Spiegelungssatz, which is a generalization of Scholz's theorem, and he works with both number fields [33] and function fields [34].

8.2 Two results on modules

Lemma 8.8. *Let p be a prime number, let G be a group of order coprime to p, and let A be a finite $\mathbb{Z}[G]$-module. Then the quotient A/pA and the p-torsion $A[p]$ are isomorphic $(\mathbb{Z}/p\mathbb{Z})[G]$-modules.*

Proof. The multiplication by p map $A \to A$, $a \mapsto pa$, gives rise to the exact sequence of $\mathbb{Z}[G]$-modules

$$0 \to A[p] \to A \to A \to A/pA \to 0.$$

It follows that the $\mathbb{Z}[G]$-modules $A[p] \oplus A$ and $A/pA \oplus A$ are Jordan–Hölder isomorphic and therefore so are the $\mathbb{Z}[G]$-modules $A[p]$ and A/pA. Since $A[p]$ and A/pA are $(\mathbb{Z}/p\mathbb{Z})[G]$-modules, they are also Jordan–Hölder isomorphic as $(\mathbb{Z}/p\mathbb{Z})[G]$-modules. By Maschke's Theorem the group ring $(\mathbb{Z}/p\mathbb{Z})[G]$ is semisimple. The existence of a $(\mathbb{Z}/p\mathbb{Z})[G]$-module isomorphism between $A[p]$ and A/pA follows from the semisimplicity of $(\mathbb{Z}/p\mathbb{Z})[G]$. □

Theorem 8.9. *Let L/K be a Galois extension of number fields and let G be its Galois group. Let p be a prime not dividing $|G|$ and let Cl_K and Cl_L be the ideal class groups of K and L, respectively. Then for each $m \in \mathbb{Z}_{\geq 0}$ the norm map $\mathrm{N}_{L/K} : L \to K$ induces the split exact sequence of $\mathbb{Z}[G]$-modules*

$$1 \to \ker(\mathrm{N}_{L/K} : \mathrm{Cl}_L[p^m] \to \mathrm{Cl}_K[p^m]) \to \mathrm{Cl}_L[p^m] \xrightarrow{\mathrm{N}_{L/K}} \mathrm{Cl}_K[p^m] \to 1$$

and the submodule of Galois invariant elements of $\mathrm{Cl}_L[p^m]$ is isomorphic to $\mathrm{Cl}_K[p^m]$.

Proof. Let $\mathrm{I}_{L/K} : \mathrm{Cl}_K \to \mathrm{Cl}_L$ be the group homomorphism induced by the natural injective map from the group of fractional ideals of K to the group of fractional ideals of L and let $\mathrm{N}_{L/K} : \mathrm{Cl}_L[p^m] \to \mathrm{Cl}_K[p^m]$ be the group homomorphism induced by the norm map. The composite map

$$\mathrm{N}_{L/K} \circ \mathrm{I}_{L/K} : \mathrm{Cl}_K[p^m] \to \mathrm{Cl}_K[p^m]$$

is the group automorphism $\mathrm{Cl}_K[p^m] \xrightarrow{\sim} \mathrm{Cl}_K[p^m]$, $a \mapsto a^{|G|}$. Hence, the map

$$\mathrm{N}_{L/K} : \mathrm{Cl}_L[p^m] \to \mathrm{Cl}_K[p^m]$$

is surjective and the map

$$\mathrm{I}_{L/K} : \mathrm{Cl}_K[p^m] \to \mathrm{Cl}_L[p^m]$$

is injective. We get the exact sequence of $\mathbb{Z}[G]$-modules

$$1 \to \ker(\mathrm{N}_{L/K} : \mathrm{Cl}_L[p^m] \to \mathrm{Cl}_K[p^m]) \to \mathrm{Cl}_L[p^m] \xrightarrow{\mathrm{N}_{L/K}} \mathrm{Cl}_K[p^m] \to 1.$$

This exact sequence splits, because up to an automorphism of $\mathrm{Cl}_K[p^m]$ the map $\mathrm{I}_{L/K} : \mathrm{Cl}_K[p^m] \to \mathrm{Cl}_L[p^m]$ is a section of the sequence.

Let $\mathrm{Cl}_L[p^m]^G$ be the submodule of Galois invariant elements of $\mathrm{Cl}_L[p^m]$. The map $\mathrm{I}_{L/K} \circ \mathrm{N}_{L/K}$ restricted to $\mathrm{Cl}_L[p^m]^G$ equals the group automorphism

$$\begin{aligned} \mathrm{Cl}_L[p^m]^G &\xrightarrow{\sim} \mathrm{Cl}_L[p^m]^G, \\ a &\mapsto a^{|G|}. \end{aligned}$$

Hence, the maps $\mathrm{I}_{L/K}$ and $\mathrm{N}_{L/K}$ induce $\mathbb{Z}[G]$-module isomorphisms between $\mathrm{Cl}_K[p^m]$ and $\mathrm{Cl}_L[p^m]^G$. □

8.3 Galois group decompositions of modules

Notation 8.10. Let $d \in \mathbb{Z}_{>1}$ be squarefree. Given a number field L, we denote by Cl_L its ideal class group. Let r and s be the 3-ranks of $\mathrm{Cl}_{\mathbb{Q}(\sqrt{d})}$ and $\mathrm{Cl}_{\mathbb{Q}(\sqrt{-3d})}$, respectively. Let K be the number field $\mathbb{Q}(\sqrt{d},\sqrt{-3})$, let E be the group of units of the ring of integers of K, and let G be the Galois group $\mathrm{Gal}(K/\mathbb{Q})$. The group G is isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Let σ and τ be the generators of the Galois groups $\mathrm{Gal}(K/\mathbb{Q}(\sqrt{-3d}))$ and $\mathrm{Gal}(K/\mathbb{Q}(\sqrt{d}))$, respectively. The group G has four characters $G \to \{\pm 1\}$. We denote the trivial character by ϵ. The three nontrivial characters of G factor through the quotient groups of G corresponding to the three quadratic fields $\mathbb{Q}(\sqrt{d})$, $\mathbb{Q}(\sqrt{-3d})$, and $\mathbb{Q}(\sqrt{-3})$. We denote these characters by φ, ψ, and ω, respectively. Since 3 does not divide the order of G, by Maschke's Theorem the group ring $(\mathbb{Z}/3\mathbb{Z})[G]$ is semisimple. Given a $(\mathbb{Z}/3\mathbb{Z})[G]$-module M, we write it as direct sum of its G-components

$$M = M^{(\varepsilon)} \oplus M^{(\varphi)} \oplus M^{(\psi)} \oplus M^{(\omega)},$$

where on each component G acts by the corresponding character.

Let J be the group of ideles of K [Definition 4.19] and U be the group of unit ideles of K [Definition 4.21]. Given a subgroup S of J, we will write $\overline{S}$ for the quotient group $(S \cdot J^3)/J^3$. For any subgroup $H \subseteq \overline{J}$ we will denote by $H^\perp$ its annihilator in $\overline{J}$ with respect to the norm-residue symbol $(\cdot,\cdot) : \overline{J} \times \overline{J} \to \mu_3$, where μ_3 is the group of 3-rd roots of unity in K.

Theorem 8.11. *Let the notation be as in* Notation 8.10. *Then there is a natural* $(\mathbb{Z}/3\mathbb{Z})[G]$*-module isomorphism*

$$E/E^3 \xrightarrow{\sim} \overline{E}$$

and the four groups in the direct sum of the G*-decomposition of the* $(\mathbb{Z}/3\mathbb{Z})[G]$*-module* $\overline{E}$

$$\overline{E} = \overline{E}^{(\varepsilon)} \oplus \overline{E}^{(\varphi)} \oplus \overline{E}^{(\psi)} \oplus \overline{E}^{(\omega)}$$

have 3*-ranks* 0, 1, 0, *and* 1, *respectively.*

Proof. By Lemma 4.51 we get a natural $(\mathbb{Z}/3\mathbb{Z})[G]$-module isomorphism

$$E/E^3 \xrightarrow{\sim} \overline{E}.$$

Let L be a subfield of K, let E_L the group of units of its ring of integers, and let H be the Galois of the extension K/L. Composing the natural inclusion $E_L \to E$ with the norm map $\mathrm{N}_{K/L} : K \to L$ induces the group automorphism

$$\begin{aligned} E_L/(E_L)^3 &\xrightarrow{\sim} E_L/(E_L)^3, \\ a &\mapsto a^{|H|}. \end{aligned}$$

Hence, the group homomorphism $E_L/(E_L)^3 \to E/E^3$ induced by the natural inclusion $E_L \to E$ is injective. Dirichlet's unit theorem implies the statement in Theorem 8.11. □

Theorem 8.12. *Let the notation be as in* Notation 8.10 *and let* M *one of the* $(\mathbb{Z}/3\mathbb{Z})[G]$*-modules* $\overline{J}/(\overline{K^*} \cdot \overline{U})$, $\mathrm{Cl}_K[3]$, *and* $\mathrm{Cl}_K \,/\, \mathrm{Cl}_K^3$. *Then the four groups in the direct sum of the* G*-decomposition of the* $(\mathbb{Z}/3\mathbb{Z})[G]$*-module* M

$$M = M^{(\varepsilon)} \oplus M^{(\varphi)} \oplus M^{(\psi)} \oplus M^{(\omega)}$$

have 3*-ranks* 0, r, s, *and* 0, *respectively.*

Proof. Theorem 8.9 applied to the extension $K/\mathbb{Q}$ states that the submodule of G-invariant elements of $\mathrm{Cl}_K[3]$ is isomorphic to $\mathrm{Cl}_{\mathbb{Q}}[3]$. The submodule of G-invariant elements of $\mathrm{Cl}_K[3]$ is $\mathrm{Cl}_K[3]^{(\varepsilon)}$ and therefore we have the $(\mathbb{Z}/3\mathbb{Z})[G]$-module isomorphism

$$\mathrm{Cl}_K[3]^{(\varepsilon)} \xrightarrow{\sim} \mathrm{Cl}_{\mathbb{Q}}[3].$$

Since $\mathbb{Q}$ has class number one, the submodule $\mathrm{Cl}_{\mathbb{Q}}[3]^{(\varepsilon)}$ is trivial. Hence $\mathrm{Cl}_K[3]^{(\varphi)}$ is the submodule of τ-invariant elements of $\mathrm{Cl}_K[3]$. Now applying Theorem 8.9 to the Galois extension $K/\mathbb{Q}(\sqrt{d})$, whose Galois group is generated by τ, gives a $(\mathbb{Z}/3\mathbb{Z})[G]$-module isomorphism

$$\mathrm{Cl}_K[3]^{(\varphi)} \xrightarrow{\sim} \mathrm{Cl}_{\mathbb{Q}(\sqrt{d})}[3].$$

Hence, we have $\operatorname{rk}_3 \operatorname{Cl}_K[3]^{(\varphi)} = r$. Similarly, we get the $(\mathbb{Z}/3\mathbb{Z})[G]$-module isomorphisms

$$\operatorname{Cl}_K[3]^{(\psi)} \xrightarrow{\sim} \operatorname{Cl}_{\mathbb{Q}(\sqrt{-3d})}[3] \quad \text{and} \quad \operatorname{Cl}_K[3]^{(\omega)} \xrightarrow{\sim} \operatorname{Cl}_{\mathbb{Q}(\sqrt{-3})}[3].$$

Hence, we have $\operatorname{rk}_3 \operatorname{Cl}_K[3]^{(\psi)} = s$. Since the ideal class group of $\mathbb{Q}(\sqrt{-3})$ is trivial, we have $\operatorname{rk}_3 \operatorname{Cl}_K[3]^{(\omega)} = 0$.

Lemma 8.8 implies the existence of a $(\mathbb{Z}/3\mathbb{Z})[G]$-module isomorphism

$$\operatorname{Cl}_K[3] \xrightarrow{\sim} \operatorname{Cl}_K / \operatorname{Cl}_K^3 .$$

By the short exact sequence 4.81 there is a $(\mathbb{Z}/3\mathbb{Z})[G]$-module isomorphism

$$\overline{J}/(\overline{K^*} \cdot \overline{U}) \xrightarrow{\sim} \operatorname{Cl}_K / \operatorname{Cl}_K^3 .$$

The statement in Theorem 8.12 follows. □

Lemma 8.13. *Let the notation be as in* Notation 8.10. *Then the norm-residue symbol*

$$(\cdot,\cdot) : \overline{J} \times \overline{J} \to \mu_3$$

splits into four perfect pairings

$$\overline{J}^{(\varepsilon)} \times \overline{J}^{(\omega)} \to \mu_3, \qquad \overline{J}^{(\omega)} \times \overline{J}^{(\varepsilon)} \to \mu_3,$$
$$\overline{J}^{(\varphi)} \times \overline{J}^{(\psi)} \to \mu_3, \qquad \overline{J}^{(\psi)} \times \overline{J}^{(\varphi)} \to \mu_3.$$

Proof. Let $\chi_1, \chi_2 \in \{\epsilon, \varphi, \psi, \omega\}$ and consider the pairing

$$\overline{J}^{(\chi_1)} \times \overline{J}^{(\chi_2)} \to \mu_3.$$

By Corollary 3.101 for each $g \in G$ we have $(ga, gb) = g\,(a, b)$. This implies that G acts on the image of the pairing through the character $\chi_1 \cdot \chi_2$. The group G acts on μ_3 through ω. If one has $\omega \neq \chi_1 \cdot \chi_2$, then the groups $\overline{J}^{(\chi_1)}$ and $\overline{J}^{(\chi_2)}$ are orthogonal. Since by Theorem 4.50 the norm-residue symbol is a perfect pairing, the statement in Lemma 8.13 follows. □

Lemma 8.14. *Let the notation be as in* Notation 8.10. *Then the norm-residue symbol induces a perfect pairing of finite abelian groups*

$$\overline{J}/(\overline{K^*} \cdot \overline{U}) \times \overline{K^*} \cap \overline{U}^{\perp} \to \mu_3$$

that splits into two perfect pairings of finite abelian groups

$$(\overline{J}/(\overline{K^*} \cdot \overline{U}))^{(\varphi)} \times (\overline{K^*} \cap \overline{U}^{\perp})^{(\psi)} \to \mu_3$$

and

$$(\overline{J}/(\overline{K^*} \cdot \overline{U}))^{(\psi)} \times (\overline{K^*} \cap \overline{U}^{\perp})^{(\varphi)} \to \mu_3.$$

Proof. The diagram in Section 4.8 shows that the annihilator of $\overline{K^*} \cap \overline{U}^{\perp}$ with respect to the norm-residue symbol is $\overline{K^*} \cdot \overline{U}$. Hence, the norm-residue symbol induces a perfect pairing of finite abelian groups

$$\overline{J}/(\overline{K^*} \cdot \overline{U}) \times \overline{K^*} \cap \overline{U}^{\perp} \to \mu_3.$$

The statement in Lemma 8.14 follows from Theorem 8.12 and Lemma 8.13. □

Theorem 8.15. *Let the notation be as in* Notation 8.10. *Then the four groups in the direct sum of the G-decomposition of the $(\mathbb{Z}/3\mathbb{Z})[G]$-module $\overline{K^*} \cap \overline{U}^{\perp}$*

$$\overline{K^*} \cap \overline{U}^{\perp} = (\overline{K^*} \cap \overline{U}^{\perp})^{(\varepsilon)} \oplus (\overline{K^*} \cap \overline{U}^{\perp})^{(\varphi)} \oplus (\overline{K^*} \cap \overline{U}^{\perp})^{(\psi)} \oplus (\overline{K^*} \cap \overline{U}^{\perp})^{(\omega)}$$

have 3-ranks 0, s, r, and 0, respectively.

Proof. By Theorem 8.12 we have

$$\overline{J}/(\overline{K^*} \cdot \overline{U}) = (\overline{J}/(\overline{K^*} \cdot \overline{U}))^{(\varphi)} \oplus (\overline{J}/(\overline{K^*} \cdot \overline{U}))^{(\psi)}$$

and the 3-ranks of $(\overline{J}/(\overline{K^*} \cdot \overline{U}))^{(\varphi)}$ and $(\overline{J}/(\overline{K^*} \cdot \overline{U}))^{(\psi)}$ equal r and s, respectively. Lemma 8.14 implies that by duality these 3-ranks are equal to the 3-ranks of $(\overline{K^*} \cap \overline{U}^{\perp})^{(\psi)}$ and $(\overline{K^*} \cap \overline{U}^{\perp})^{(\varphi)}$, respectively. □

Theorem 8.16. *Let the notation be as in* Notation 8.10. *Then the four groups in the direct sum of the G-decomposition of the $(\mathbb{Z}/3\mathbb{Z})[G]$-module $\overline{K^*} \cap \overline{U}$*

$$\overline{K^*} \cap \overline{U} = (\overline{K^*} \cap \overline{U})^{(\varepsilon)} \oplus (\overline{K^*} \cap \overline{U})^{(\varphi)} \oplus (\overline{K^*} \cap \overline{U})^{(\psi)} \oplus (\overline{K^*} \cap \overline{U})^{(\omega)}$$

have 3-ranks 0, $r+1$, s, and 1, respectively.

Proof. The group homomorphisms in Corollary 5.27 and Theorem 5.29 are $(\mathbb{Z}/3\mathbb{Z})[G]$-modules homomorphisms. Corollary 5.27 implies that the 3-Selmer group $\{3\text{-virtual units of } K\}/{K^*}^3$ of K and the group $\overline{K^*} \cap \overline{U}$ are isomorphic $(\mathbb{Z}/3\mathbb{Z})[G]$-modules. Using the short exact sequence of $(\mathbb{Z}/3\mathbb{Z})[G]$-modules

$$1 \longrightarrow E/E^3 \longrightarrow \{3\text{-virtual units of } K\}/{K^*}^3 \longrightarrow \mathrm{Cl}_K[3] \longrightarrow 1$$

given by Theorem 5.29, the statement in Theorem 8.16 follows from Theorem 8.11 and Theorem 8.12. □

Theorem 8.17. *Let the notation be as in* Notation 8.10 *and let V be the 3-rd virtual group of K* [Definition 5.15]. *Then the 3-ranks of the four groups in the direct sum of the G-decomposition of the $(\mathbb{Z}/3\mathbb{Z})[G]$-module V*

$$V = V^{(\varepsilon)} \oplus V^{(\varphi)} \oplus V^{(\psi)} \oplus V^{(\omega)}$$

are either 0, 1, 0, and 1, or 0, 0, 1, and 1, respectively. Moreover, in the first case one has $s = r$ and in the second case one has $s = r + 1$.

Proof. The G-decomposition of the short exact sequence of $(\mathbb{Z}/3\mathbb{Z})[G]$-modules

$$1 \longrightarrow \overline{K^*} \cap \overline{U}^{\perp} \longrightarrow \overline{K^*} \cap \overline{U} \longrightarrow V \longrightarrow 1$$

in Remark 5.16 gives rise to four short exact sequences of $(\mathbb{Z}/3\mathbb{Z})[G]$-modules. Theorem 8.15 and Theorem 8.16 imply that the 3-ranks of $V^{(\varepsilon)}$ and $V^{(\omega)}$ are 0 and 1, respectively. Since by Corollary 5.18 the 3-rank of V equals 2, the 3-ranks of $V^{(\varphi)}$ and $V^{(\psi)}$ are either 1 and 0 or 0 and 1, respectively. Using again Theorem 8.15 and Theorem 8.16 we get the following. If the 3-ranks of $V^{(\varphi)}$ and $V^{(\psi)}$ are 1 and 0, respectively, then one has $s = r$, otherwise one has $s = r + 1$. □

Theorem 8.18. *Let the notation be as in* Notation 8.10. *Then the* 3*-rd unit residue group of* K [Definition 5.3] *is a free* $(\mathbb{Z}/3\mathbb{Z})[G]$*-module of rank* 1.

Proof. By Theorem 5.10 the 3-rd unit residue group of K has 3-rank 4. Since it contains the 3-rd virtual group of K and is a skew abelian group by Corollary 5.2, the statement in Theorem 8.18 follows from Theorem 8.17 and Lemma 8.13. □

8.4 Scholz's theorem

A classical theorem in algebraic number theory about the 3-ranks of ideal class groups of quadratic number fields is Scholz's theorem [Theorem 8.19], which Scholz proved in 1932. It is often called the 'Mirror theorem' or the 'Reflection theorem'. These names are also used for Leopoldt's Spiegelungssatz [41], which is a generalization of Scholz's theorem.

Theorem 8.19 (Scholz [63])**.** *Let* $d \in \mathbb{Z}_{>1}$ *be squarefree, let* r *be the* 3*-rank of the ideal class group of* $\mathbb{Q}(\sqrt{d})$*, and let* s *be the* 3*-rank of the ideal class group of* $\mathbb{Q}(\sqrt{-3d})$*. Then one has*

$$r \leq s \leq r + 1.$$

Proof. This follows from Theorem 8.2. □

In our setting the proof of Scholz's theorem [Theorem 10.10 of Chapter 10 in [74]] by Washington gives rise to Theorem 8.20.

Theorem 8.20. *Let the notation be as in* Notation 8.10 *and let*

$$\overline{K^*} \cap \overline{U}^{\perp} \to \mathrm{Cl}_K[3] \tag{8.21}$$

be the $(\mathbb{Z}/3\mathbb{Z})[G]$*-module homomorphism obtained by composing the natural* $(\mathbb{Z}/3\mathbb{Z})[G]$*-module homomorphism*

$$\overline{K^*} \cap \overline{U}^{\perp} \to (\overline{K^*} \cap \overline{U})/\overline{E}$$

with the $(\mathbb{Z}/3\mathbb{Z})[G]$*-module isomorphism*

$$(\overline{K^*} \cap \overline{U})/\overline{E} \xrightarrow{\sim} \mathrm{Cl}_K[3]$$

given by the short exact sequence 4.82*. Then the* G*-decomposition of the* $(\mathbb{Z}/3\mathbb{Z})[G]$*-module homomorphism* 8.21 *gives rise to a group homomorphism with kernel of* 3*-rank at most* 1

$$(\overline{K^*} \cap \overline{U}^{\perp})^{(\varphi)} \to \mathrm{Cl}_K[3]^{(\varphi)}$$

from a group of 3*-rank* s *to a group of* 3*-rank* r *and an injective group homomorphism*

$$(\overline{K^*} \cap \overline{U}^{\perp})^{(\psi)} \to \mathrm{Cl}_K[3]^{(\psi)}$$

from a group of 3*-rank* r *to a group of* 3*-rank* s*.*

Proof. It follows from Theorem 8.12 and Theorem 8.15 that both the groups $\mathrm{Cl}_K[3]^{(\varphi)}$ and $(\overline{K^*} \cap \overline{U}^{\perp})^{(\psi)}$ have 3-rank r and both the groups $\mathrm{Cl}_K[3]^{(\psi)}$ and $(\overline{K^*} \cap \overline{U}^{\perp})^{(\varphi)}$ have 3-rank s. By Theorem 8.11 the 3-ranks of $\overline{E}^{(\varphi)}$ and $\overline{E}^{(\psi)}$ equal 1 and 0, respectively. Since the kernel of the $(\mathbb{Z}/3\mathbb{Z})[G]$-module homomorphism

$$\overline{K^*} \cap \overline{U}^{\perp} \to (\overline{K^*} \cap \overline{U})/\overline{E}$$

is contained in $\overline{E}$, the statement in Theorem 8.20 follows. □

Remark 8.22. The cases $s = r + 1$ and $s = r$ in Theorem 8.19 both occur. For instance, we have $r = 0$ and $s = 1$ for $d = 29$ and $r = s = 1$ for $d = 79$. Theorem 8.20 suggests distinguishing three cases.

(a) One has $s = r$ and the map $(\overline{K^*} \cap \overline{U}^{\perp})^{(\varphi)} \to \mathrm{Cl}_K[3]^{(\varphi)}$ is an isomorphism.

(b) One has $s = r$ and the map $(\overline{K^*} \cap \overline{U}^{\perp})^{(\varphi)} \to \mathrm{Cl}_K[3]^{(\varphi)}$ has both kernel and cokernel of dimension 1 over $\mathbb{Z}/3\mathbb{Z}$.

(c) One has $s = r + 1$.

Note that the last case occurs if and only if the injective group homomorphism

$$(\overline{K^*} \cap \overline{U}^{\perp})^{(\psi)} \to \mathrm{Cl}_K[3]^{(\psi)}$$

is not an isomorphism. We have examples of these three cases for $d = 142$, for $d = 79$, and for $d = 29$, respectively.

8.5 Dutarte's probabilistic model

Let $d \in \mathbb{Z}_{>1}$ be squarefree and let r be the 3-rank of the ideal class group of $\mathbb{Q}(\sqrt{d})$. Scholz's theorem [Theorem 8.19] states that the 3-rank of the ideal

class group of $\mathbb{Q}(\sqrt{-3d})$ is either r or $r+1$. These two cases are characterized in Theorem 8.2 using the Galois module structure of the 3-rd virtual group of the number field $\mathbb{Q}(\sqrt{d},\sqrt{-3})$. In 1984 Dutarte [14] proposed a probabilistic model, which we present in our setting.

Theorem 8.23. *Let the notation be as in* Notation 8.10. *Then the following are equivalent.*

(i) *The natural group homomorphism* $(\overline{K^*} \cap \overline{U})^{(\varphi)} \to (\overline{U}/\overline{U}^{\perp})^{(\varphi)}$ *is trivial.*
(ii) *One has* $s = r+1$.

Proof. By Remark 5.16 the kernel of the natural group homomorphism

$$(\overline{K^*} \cap \overline{U})^{(\varphi)} \to (\overline{U}/\overline{U}^{\perp})^{(\varphi)}$$

is $(\overline{K^*} \cap \overline{U}^{\perp})^{(\varphi)}$, which has 3-rank s by Theorem 8.15. The group $(\overline{K^*} \cap \overline{U})^{(\varphi)}$ has 3-rank $r+1$ by Theorem 8.16. The statement in Theorem 8.23 follows. □

Remark 8.24. By Theorem 8.18 the group $(\overline{U}/\overline{U}^{\perp})^{(\varphi)}$ in Theorem 8.23 has 3-rank 1. Hence, the natural group homomorphism in Theorem 8.23 is a group homomorphism from an elementary abelian 3-group of rank $r+1$ to a group of order 3.

Let a be a nonnegative integer and let D_a^+ be the set of discriminants of real quadratic number fields whose ideal class groups have 3-rank a. To each $\Delta \in D_a^+$ we associate the natural group homomorphism in Theorem 8.23 for the number field $K = \mathbb{Q}(\sqrt{\Delta},\sqrt{-3})$, which is a group homomorphism from an elementary abelian 3-group of rank $a+1$ to a group of order 3 by Remark 8.24. Since there are 3^{a+1} group homomorphisms from an elementary abelian 3-group of rank $a+1$ to a group of order 3, Dutarte assumes that the density in D_a^+ of the subset of discriminants with associated trivial group homomorphism is $1/3^{a+1}$. Hence, he writes that $1/3^{a+1}$ is the value of the probability that the 3-rank of the ideal class group of $\mathbb{Q}(\sqrt{-3\Delta})$ is the positive integer $a+1$ given that one has $\Delta \in D_a^+$. The formalization of this assumption is Conjecture 8.3.

Theorem 8.25. *Let the notation be as in* Notation 8.10. *Then the following are equivalent.*

(i) *The natural group homomorphism* $(\overline{K^*} \cap \overline{U})^{(\psi)} \to (\overline{U}/\overline{U}^{\perp})^{(\psi)}$ *is trivial.*
(ii) *One has* $s = r$.

Proof. By Remark 5.16 the kernel of the natural group homomorphism

$$(\overline{K^*} \cap \overline{U})^{(\psi)} \to (\overline{U}/\overline{U}^{\perp})^{(\psi)}$$

is $(\overline{K^*} \cap \overline{U}^{\perp})^{(\psi)}$, which has 3-rank r by Theorem 8.15. The group $(\overline{K^*} \cap \overline{U})^{(\psi)}$ has 3-rank s by Theorem 8.16. The statement in Theorem 8.25 follows. □

8.6 Some consequences

Notation 8.26. Let D^+ be the set of discriminants of real quadratic number fields. Given a number field L we denote by Cl_L its ideal class group. We define the maps

$$r : D^+ \to \mathbb{Z}_{\geq 0} \qquad \text{and} \qquad s : D^+ \to \mathbb{Z}_{\geq 0}$$
$$\Delta \mapsto \mathrm{rk}_3\, \mathrm{Cl}_{\mathbb{Q}(\sqrt{\Delta})} \qquad\qquad \Delta \mapsto \mathrm{rk}_3\, \mathrm{Cl}_{\mathbb{Q}(\sqrt{-3\Delta})}$$

in order to evaluate the 3-ranks of ideal class groups of quadratic number fields. Let A be a subset of D^+. We define the probability $\Pr^+(A)$ of A as being equal to the limit, if it exists,

$$\Pr^+(A) = \lim_{x \to +\infty} \frac{|\{\Delta \in A : \Delta < x\}|}{|\{\Delta \in D^+ : \Delta < x\}|}.$$

To shorten the notation, for each integer a we will write $\Pr^+(r = a)$ and $\Pr^+(s = a)$ for the probability of the subsets $\{\Delta \in D^+ : \mathrm{rk}_3\, \mathrm{Cl}_{\mathbb{Q}(\sqrt{\Delta})} = a\}$ and $\{\Delta \in D^+ : \mathrm{rk}_3\, \mathrm{Cl}_{\mathbb{Q}(\sqrt{-3\Delta})} = a\}$ of D^+, respectively. Moreover, we denote by D_0^+ and D_*^- the sets $\{\Delta \in D^+ : \Delta \equiv 0 \bmod 3\}$ and $\{\Delta \in D^- : \Delta \not\equiv 0 \bmod 3\}$, respectively.

Remark 8.27. The left-hand sides of the equalities in Conjecture 8.3 and Conjecture 8.4 can be thought of as conditional probabilities. We will denote them by $\Pr^+(s = a + 1 \mid r = a)$ and $\Pr^+(r = a \mid s = a)$, respectively.

In the proof of Theorem 8.31 we will use some identities of power series that come from the generating function for the number of partitions of positive integers.

Definition 8.28 (Durfee number)**.** The *Durfee number* of a partition of a positive integer is the largest integer i such that the partition contains at least i summands of size at least i.

Remark 8.29. The Durfee number of a partition of a positive integer is the size of the largest square that is contained within the Ferrers diagram of the partition.

Lemma 8.30 follows from Corollary 6.7 in [11] by Cohen and Lenstra, but it can also be proved directly, as we do here.

Lemma 8.30. *One has the identities of power series*

$$1 + \sum_{i>0} \frac{x^{i^2}}{\prod_{j=1}^{i} (1 - x^j)^2} = 1 + \sum_{i>0} x^i \prod_{j=1}^{i} \left(\frac{1}{1 - x^j} \right) = \prod_{i>0} \frac{1}{1 - x^i}.$$

Proof. We write the generating function for the number of partitions of positive integers. The first two expressions are obtained by grouping partitions according to their Durfee number and the size of their largest addend, respectively. The last one is the usual formula. □

Theorem 8.31. *Let the notation be as in* Notation 8.26. *Assume* Conjecture 8.3, Conjecture 8.4, *and* Conjecture 8.5. *Then for each nonnegative integer a one has*

$$\Pr^+(r = a) = 3^{-a(a+1)} \prod_{i=1}^{\infty}(1 - 3^{-i}) \prod_{i=1}^{a}(1 - 3^{-i})^{-1} \prod_{i=1}^{a+1}(1 - 3^{-i})^{-1}$$

and

$$\Pr^+(s = a) = 3^{-a^2} \prod_{i=1}^{\infty}(1 - 3^{-i}) \prod_{i=1}^{a}(1 - 3^{-i})^{-2}.$$

Proof. Let a be a nonnegative integer. Using the notation in Remark 8.27, Conjecture 8.3 states the equality

$$\Pr^+(s = a + 1 \mid r = a) = 1/3^{a+1}$$

and Scholz's theorem implies the equality

$$\Pr^+(s = a + 1 \mid r = a) + \Pr^+(s = a \mid r = a) = 1.$$

Hence, we have

$$\Pr^+(s = a \mid r = a) = 1 - 1/3^{a+1}.$$

Conjecture 8.5 states the existence of the probabilities $\Pr^+(r = a, s = a + 1)$ and $\Pr^+(r = a, s = a)$. From the equalities

$$\Pr^+(r = a, s = a + 1) = \Pr^+(s = a + 1 \mid r = a) \cdot \Pr^+(r = a)$$

and

$$\Pr^+(r = a, s = a) = \Pr^+(s = a \mid r = a) \cdot \Pr^+(r = a)$$

we get

$$\Pr^+(r = a, s = a + 1) = \Pr^+(s = a + 1 \mid r = a) \cdot \frac{\Pr^+(r = a, s = a)}{\Pr^+(s = a \mid r = a)}$$

and therefore

$$\Pr^+(r = a, s = a + 1) = \Pr^+(r = a, s = a)(3^{a+1} - 1)^{-1}. \tag{8.32}$$

Similarly, Conjecture 8.4 and Scholz's theorem imply for each nonnegative integer a the equality

$$\Pr^+(r = a+1, s = a+1) = \Pr^+(r = a, s = a+1)(3^{a+1} - 1)^{-1}. \tag{8.33}$$

The left-hand side of the equality

$$\sum_{(a,b)\in\mathbb{Z}^2} \Pr^+(r = a, s = b) = 1$$

in Conjecture 8.5 can be written as

$$\Pr^+(r = 0, s = 0) + \sum_{b=1}^{\infty} \sum_{a=b-1}^{b} \Pr^+(r = a, s = b).$$

Setting $y = \Pr^+(r = 0, s = 0)$ and using recursively (8.32) and (8.33) we get the equation in y

$$y\left(1 + \sum_{b=1}^{\infty}\left(\frac{3^b - 1}{\prod_{i=1}^{b}(3^i - 1)^2} + \frac{1}{\prod_{i=1}^{b}(3^i - 1)^2}\right)\right) = 1. \tag{8.34}$$

Since for all positive integers b we have

$$\frac{3^b - 1}{\prod_{i=1}^{b}(3^i - 1)^2} + \frac{1}{\prod_{i=1}^{b}(3^i - 1)^2} = \frac{3^b}{\prod_{i=1}^{b}(3^i - 1)^2} = \frac{(1/3)^{b^2}}{\prod_{i=1}^{b}(1 - (1/3)^i)^2},$$

we rewrite (8.34) as

$$y\left(1 + \sum_{b=1}^{\infty}\frac{(1/3)^{b^2}}{\prod_{i=1}^{b}(1 - (1/3)^i)^2}\right) = 1.$$

By Lemma 8.30 the solution is $y = \prod_{i=1}^{\infty}(1 - 3^{-i})$, which is the value predicted

by Cohen and Lenstra. Using (8.32) and (8.33), for all $a, b \in \mathbb{Z}_{\geq 0}$ we get

$$\Pr^+(r = a, s = b) = \begin{cases} 3^{-a(a+1)} \prod_{i=1}^{\infty}(1-3^{-i}) \prod_{i=1}^{a}(1-3^{-i})^{-2} & \text{if } b = a, \\ 3^{-(a+1)^2} \prod_{i=1}^{\infty}(1-3^{-i}) \prod_{i=1}^{a}(1-3^{-i})^{-1} \prod_{i=1}^{a+1}(1-3^{-i})^{-1} & \text{if } b = a+1, \\ 0 & \text{otherwise.} \end{cases}$$

Hence, for each nonnegative integer a from the equality

$$\Pr^+(r = a) = \Pr^+(r = a, s = a) + \Pr^+(r = a, s = a+1)$$

we get the value conjectured by Cohen and Lenstra

$$\Pr^+(r = a) = 3^{-a(a+1)} \prod_{i=1}^{\infty}(1-3^{-i}) \prod_{i=1}^{a}(1-3^{-i})^{-1} \prod_{i=1}^{a+1}(1-3^{-i})^{-1}.$$

Similarly, for each nonnegative integer a we get

$$\Pr^+(s = a) = 3^{-a^2} \prod_{i=1}^{\infty}(1-3^{-i}) \prod_{i=1}^{a}(1-3^{-i})^{-2}. \qquad \square$$

Remark 8.35. Let D^- be the set of discriminants of complex quadratic number fields. The value conjectured by Cohen and Lenstra [11] of the limit

$$\lim_{x \to +\infty} \frac{|\{\Delta \in D^- : |\Delta| < x,\ \mathrm{rk}_3\, \mathrm{Cl}_{\mathbb{Q}(\sqrt{\Delta})} = a\}|}{|\{\Delta \in D^- : |\Delta| < x\}|}$$

is the value of the probability

$$\Pr^+(s = a) = \lim_{x \to +\infty} \frac{|\{\Delta \in D^+ : \Delta < x,\ \mathrm{rk}_3\, \mathrm{Cl}_{\mathbb{Q}(\sqrt{-3\Delta})} = a\}|}{|\{\Delta \in D^+ : \Delta < x\}|}$$

in Theorem 8.31. Note that the complex quadratic number fields appear in different orders in the two limits. This is caused by the fact that D^- is not involved in any of the limits in Conjecture 8.3, Conjecture 8.4, and Conjecture 8.5.

Remark 8.36. Let D^- be the set of discriminants of complex quadratic number fields. The natural definition of the map s in Notation 8.26 is

$$\begin{aligned} s : D^- &\to \mathbb{Z}_{\geq 0}, \\ \Delta &\mapsto \mathrm{rk}_3\, \mathrm{Cl}_{\mathbb{Q}(\sqrt{\Delta})}\,. \end{aligned}$$

Similarly to the real case, given a subset A of D^-, we define the probability $\Pr^-(A)$ of A. Now the problem is the connection between $\Pr^+$ and $\Pr^-$, in particular the map between D^+ and D^-. A way of dealing with this problem is to restrict to subsets of D^+ and D^- that have an order-reversing bijection induced by the reflection map. For example, the maps

$$\begin{aligned} f : \{\Delta \in D^+ : \Delta \equiv 0 \bmod 3\} &\to \{\Delta \in D^- : \Delta \not\equiv 0 \bmod 3\}, \\ \Delta &\mapsto -\Delta/3, \end{aligned}$$

and

$$\begin{aligned} \{\Delta \in D^+ : \Delta \not\equiv 0 \bmod 3\} &\to \{\Delta \in D^- \setminus \{-3\} : \Delta \equiv 0 \bmod 3\}, \\ \Delta &\mapsto -3\Delta, \end{aligned}$$

are order-reversing bijections.

We restrict ourselves to considering the sets $\{\Delta \in D^+ : \Delta \equiv 0 \bmod 3\}$ and $\{\Delta \in D^- : \Delta \not\equiv 0 \bmod 3\}$. Conjecture 8.37, Conjecture 8.38, Conjecture 8.40, and Theorem 8.42. correspond to Conjecture 8.3, Conjecture 8.4, Conjecture 8.5, and Theorem 8.31, respectively. An analogous discussion can be given for the sets $\{\Delta \in D^+ : \Delta \not\equiv 0 \bmod 3\}$ and $\{\Delta \in D^- \setminus \{-3\} : \Delta \equiv 0 \bmod 3\}$ [Remark 8.44].

Conjecture 8.37. *Let the notation be as in* Notation 8.26. *Then for every nonnegative integer a one has*

$$\lim_{x\to+\infty} \frac{|\{\Delta \in D_0^+ : \Delta < x,\, \mathrm{rk}_3 \mathrm{Cl}_{\mathbb{Q}(\sqrt{\Delta})} = a,\, \mathrm{rk}_3 \mathrm{Cl}_{\mathbb{Q}(\sqrt{-3\Delta})} = a+1\}|}{|\{\Delta \in D_0^+ : \Delta < x,\, \mathrm{rk}_3 \mathrm{Cl}_{\mathbb{Q}(\sqrt{\Delta})} = a\}|} = \frac{1}{3^{a+1}}$$

Conjecture 8.38. *Let the notation be as in* Notation 8.26. *Then for every nonnegative integer a one has*

$$\lim_{x\to+\infty} \frac{|\{\Delta \in D_*^- : |\Delta| < x,\, \mathrm{rk}_3 \mathrm{Cl}_{\mathbb{Q}(\sqrt{\Delta})} = a,\, \mathrm{rk}_3 \mathrm{Cl}_{\mathbb{Q}(\sqrt{-3\Delta})} = a\}|}{|\{\Delta \in D_*^- : |\Delta| < x,\, \mathrm{rk}_3 \mathrm{Cl}_{\mathbb{Q}(\sqrt{\Delta})} = a\}|} = \frac{1}{3^{a}}$$

Remark 8.39. The left-hand sides of the equalities in Conjecture 8.37 and Conjecture 8.38 can be thought of as conditional probabilities. We will denote them by $\Pr_0^+(s \circ f = a+1 \mid r = a)$ and $\Pr_*^-(r \circ f^{-1} = a \mid s = a)$, respectively.

Conjecture 8.40. *Let the notation be as in* Notation 8.26. *Then for each pair $(a, b) \in \mathbb{Z}^2$ the limit*

$$\lim_{x\to+\infty} \frac{|\{\Delta \in D_0^+ : \Delta < x,\, \mathrm{rk}_3 \mathrm{Cl}_{\mathbb{Q}(\sqrt{\Delta})} = a,\, \mathrm{rk}_3 \mathrm{Cl}_{\mathbb{Q}(\sqrt{-3\Delta})} = b\}|}{|\{\Delta \in D_0^+ : \Delta < x\}|}$$

exists. Moreover, if one denotes its value by $\Pr_0^+(r = a, s \circ f = b)$*, then one has*

$$\sum_{(a,b)\in\mathbb{Z}^2} \Pr_0^+(r = a, s \circ f = b) = 1.$$

Remark 8.41. The limit in Conjecture 8.40 equals the limit

$$\lim_{x\to+\infty} \frac{|\{\Delta \in D_*^- : |\Delta| < x,\ \mathrm{rk}_3\,\mathrm{Cl}_{\mathbb{Q}(\sqrt{-3\Delta})} = a,\ \mathrm{rk}_3\,\mathrm{Cl}_{\mathbb{Q}(\sqrt{\Delta})} = b\}|}{|\{\Delta \in D_*^- : |\Delta| < x\}|},$$

because the map f is order-reversing. We will denote the equality of their values by

$$\Pr_0^+(r = a, s \circ f = b) = \Pr_*^-(r \circ f^{-1} = a, s = b).$$

Theorem 8.42. *Let the notation be as in* Notation 8.26*. For each nonnegative integer* a *let*

$$\Pr_0^+(r = a) = \lim_{x\to+\infty} \frac{|\{\Delta \in D_0^+ : \Delta < x,\ \mathrm{rk}_3\,\mathrm{Cl}_{\mathbb{Q}(\sqrt{\Delta})} = a\}|}{|\{\Delta \in D_0^+ : \Delta < x\}|}$$

and

$$\Pr_*^-(s = a) = \lim_{x\to+\infty} \frac{|\{\Delta \in D_*^- : |\Delta| < x,\ \mathrm{rk}_3\,\mathrm{Cl}_{\mathbb{Q}(\sqrt{\Delta})} = a\}|}{|\{\Delta \in D_*^- : |\Delta| < x\}|}.$$

Assume Conjecture 8.37*,* Conjecture 8.38*, and* Conjecture 8.40*. Then for each nonnegative integer* a *one has*

$$\Pr_0^+(r = a) = 3^{-a(a+1)} \prod_{i=1}^{\infty}(1 - 3^{-i}) \prod_{i=1}^{a}(1 - 3^{-i})^{-1} \prod_{i=1}^{a+1}(1 - 3^{-i})^{-1}$$

and

$$\Pr_*^-(s = a) = 3^{-a^2} \prod_{i=1}^{\infty}(1 - 3^{-i}) \prod_{i=1}^{a}(1 - 3^{-i})^{-2}.$$

Proof. Let a be a nonnegative integer. Conjecture 8.37 and Conjecture 8.38 state the equalities

$$\Pr_0^+(s \circ f = a + 1 \mid r = a) = \frac{1}{3^{a+1}}$$

and

$$\Pr_*^-(r \circ f^{-1} = a \mid s = a) = \frac{1}{3^a},$$

respectively. Conjecture 8.40 states the equality

$$\sum_{(a,b)\in\mathbb{Z}^2} \Pr_0^+(r = a, s \circ f = b) = 1.$$

Remark 8.41 states the equality

$$\Pr_0^+(r = a, s \circ f = b) = \Pr_*^-(r \circ f^{-1} = a, s = b).$$

Since the map f is order-reversing, we have

$$\Pr_*^-(s = a) = \lim_{x \to +\infty} \frac{|\{\Delta \in D_0^+ : \Delta < x, \operatorname{rk}_3 \operatorname{Cl}_{\mathbb{Q}(\sqrt{-3\Delta})} = a\}|}{|\{\Delta \in D_0^+ : \Delta < x\}|}.$$

We conclude by following the steps of the proof of Theorem 8.31 with $\Pr^+$ replaced by $\Pr_0^+$. □

Remark 8.43. The values of the limits in Theorem 8.42 are the values conjectured by Cohen and Lenstra [11].

Remark 8.44. Since the map

$$\begin{aligned} \{\Delta \in D^+ : \Delta \not\equiv 0 \bmod 3\} &\to \{\Delta \in D^- \setminus \{-3\} : \Delta \equiv 0 \bmod 3\}, \\ \Delta &\mapsto -3\Delta, \end{aligned}$$

is order-reversing, we can replace D_0^+ and D_*^- by $\{\Delta \in D^+ : \Delta \not\equiv 0 \bmod 3\}$ and $\{\Delta \in D^- \setminus \{-3\} : \Delta \equiv 0 \bmod 3\}$, respectively, in Conjecture 8.37, Conjecture 8.38, Conjecture 8.40, and Theorem 8.42.

CHAPTER 9

Cyclic number fields

9.1 Introduction

Let K be a real quadratic number field of discriminant congruent to 1 modulo 8. The rational prime 2 splits completely in the ring of integers of K. Hence, there are two prime ideals of the ring of integers of K dividing 2 and K has two real places. One may wonder whether there is a way of defining a natural bijection between the set of primes above 2 and the set of real places of K. An affirmative answer follows from Theorem 9.1 using the two square roots of the discriminant of K, which are conjugate under the action of the Galois group $\mathrm{Gal}(K/\mathbb{Q})$.

Theorem 9.1. *Let K be a real quadratic number field and let Δ be its discriminant. Suppose one has $\Delta \equiv 1 \bmod 8$ and let S_2 and S_∞ be the set of prime ideals of the ring of integers of K dividing 2 and the set of Archimedean places of K, respectively. Then for each $\delta \in K$ satisfying $\delta^2 = \Delta$ there is exactly one prime $\mathfrak{P} \in S_2$ satisfying the congruence $\delta \equiv 1 \bmod \mathfrak{P}^2$ and there is exactly one place $v \in S_\infty$ satisfying $\sigma(\delta) > 0$ where $\sigma : K \hookrightarrow \mathbb{R}$ is the field embedding corresponding to v.*

Proof. Let $\delta \in K$ satisfying $\delta^2 = \Delta$ and let $2 = \mathfrak{P}_1\mathfrak{P}_2$ be the prime ideal factorization of the rational prime 2 in the ring of integers of K. From the congruence

$$(\delta - 1)(\delta + 1) \equiv 0 \bmod 8$$

we get either $\delta \equiv 1 \bmod \mathfrak{P}_1^2$ or $\delta \equiv -1 \bmod \mathfrak{P}_1^2$. The action by the generator of the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ gives either $\delta \equiv -1 \bmod \mathfrak{P}_2^2$ or $\delta \equiv 1 \bmod \mathfrak{P}_2^2$ in the two respective cases. Since the two square roots of Δ have opposite signs, the statement of Theorem 9.1 follows. □

Let K be a real quadratic number field of discriminant congruent to 5 modulo 8. The rational prime 2 is inert in the ring of integers $\mathcal{O}_K$ of K, the residue field $\mathcal{O}_K/2\mathcal{O}_K$ has order 4, and the polynomial $X^2 + X + 1$ has two roots in this field. Theorem 9.2 shows that there is a way of defining a natural bijection between the set of the roots of the polynomial $X^2 + X + 1$ in $\mathcal{O}_K/2\mathcal{O}_K$ and the set of real places of K.

Theorem 9.2. *Let K be a real quadratic number field, let Δ be its discriminant, and let $\mathcal{O}_K$ be the ring of integers of K. Suppose one has $\Delta \equiv 5 \bmod 8$ and let S_∞ be the set of Archimedean places of K. Then for each $\delta \in K$ satisfying $\delta^2 = \Delta$ there is exactly one element $a \in \{x \in \mathcal{O}_K/2\mathcal{O}_K : x^2 + x + 1 = 0\}$ satisfying the congruence $\frac{\delta-1}{2} \equiv a \bmod \mathcal{O}_K/2\mathcal{O}_K$ and there is exactly one place $v \in S_\infty$ satisfying $\sigma(\delta) > 0$ where $\sigma : K \hookrightarrow \mathbb{R}$ is the field embedding corresponding to v.*

Proof. Since we have $\Delta \equiv 5 \bmod 8$, the rational prime 2 is inert in $\mathcal{O}_K$. The residue field $\mathcal{O}_K/2\mathcal{O}_K$ has order 4. Let $\delta \in K$ satisfying $\delta^2 = \Delta$. The element $\frac{\delta-1}{2}$ is a root of the polynomial $X^2 + X - \frac{\Delta-1}{4}$, which is irreducible over $\mathbb{Q}$, because its reduction modulo 2 is the irreducible polynomial $X^2 + X + 1$ in $(\mathbb{Z}/2\mathbb{Z})[X]$. Since the two square roots of Δ have opposite signs, the statement of Theorem 9.2 follows. □

The bijections obtained in Theorem 9.1 and Theorem 9.2 are suggested by the descriptions of 2-nd unit residue groups and 2-nd virtual groups of quadratic number fields. In particular, the bijection in Theorem 9.1, when Δ is the sum of two squares of integers, is induced by the 2-nd virtual group of K [Definition 5.15] as described in Theorem 6.29. The bijection in Theorem 9.2 follows from the group isomorphism in Lemma 6.6 which we use in studying unit residue groups.

Theorem 9.3 extends Theorem 9.1 for real quadratic number fields of discriminant congruent to 1 modulo 8 to cyclic extensions of number fields $K/\mathbb{Q}$ of degree either 3 or 5 for which the rational prime 2 splits completely in the ring of integers of K.

Theorem 9.3. *Let p be either 3 or 5 and let $K/\mathbb{Q}$ be a cyclic extension of number fields of degree p. Suppose that the rational prime 2 splits completely in the ring of integers of K. Then the 2-nd virtual group of K induces a natural bijection between the set of prime ideals of the ring of integers of K dividing 2 and the set of real Archimedean places of K.*

Proof. This follows from the isomorphism of permutation modules over the group ring $(\mathbb{Z}/2\mathbb{Z})[G]$ in Theorem 9.27. □

Lemma 9.24 implies that in a cyclic cubic or quintic field the rational prime 2 either splits completely or is inert. Natural bijections similar to the one in Theorem 9.3 are obtained in Theorem 9.4 and Theorem 9.5 for the cyclic extensions of number fields $K/\mathbb{Q}$ of degree either 3 or 5 for which the rational prime 2 is inert in the ring of integers of K. In these bijections the set of primes above 2 is replaced by the self-dual normal basis [Definition 9.16] of the finite field $\mathcal{O}_K/2\mathcal{O}_K$, where $\mathcal{O}_K$ is the ring of integers of K.

Theorem 9.4. *Let $K/\mathbb{Q}$ be a cyclic extension of number fields of degree 3, let $\mathcal{O}_K$ be the ring of integers of K, and let S_∞ be the set of Archimedean places of K. Suppose that the rational prime 2 is inert in $\mathcal{O}_K$. Then the 2-nd virtual group of K induces a natural bijection*

$$\{x \in \mathcal{O}_K/2\mathcal{O}_K : x^3 + x^2 + 1 = 0\} \to S_\infty.$$

Proof. This follows from Theorem 9.30. □

Theorem 9.5. *Let $K/\mathbb{Q}$ be a cyclic extension of number fields of degree 5, let $\mathcal{O}_K$ be the ring of integers of K, and let S_∞ be the set of real Archimedean places of K. Suppose that the rational prime 2 is inert in $\mathcal{O}_K$. Then the 2-nd virtual group of K induces a natural bijection*

$$\{x \in \mathcal{O}_K/2\mathcal{O}_K : x^5 + x^4 + x^2 + x + 1 = 0\} \to S_\infty.$$

Proof. This follows from Theorem 9.33. □

All these results follow from the description of 2-nd virtual groups, which are subgroups of the 2-nd unit residue groups. Every number field K has its 2-nd unit residue group [Definition 5.3] and its 2-nd virtual group of K [Definition 5.15]. We recall that the 2-nd unit residue group of K is a skew abelian group [Corollary 5.2], where the pairing is given by the quadratic norm-residue symbol, and is isomorphic to an orthogonal sum of skew abelian groups that are defined locally at the places of K dividing 2 and at the real Archimedean places of K [Theorem 5.6]. We refer to Chapter 2 for definitions and results on skew abelian groups. We also recall that the 2-nd virtual group of K is a maximal self-annihilating subgroup of the 2-nd unit residue group of K [Theorem 5.17].

Some general results on the 2-nd unit residue group and the 2-nd virtual group are presented in Section 9.3. When $K/\mathbb{Q}$ is a Galois extension unramified at 2 with Galois group G, Theorem 9.20 states that the 2-nd unit residue group of K is a free $(\mathbb{Z}/2\mathbb{Z})[G]$-module. Let D the set of positive integers that divide at least one of the integers in the set $\{2^n + 1 \mid n \in \mathbb{Z}_{>0}\}$. When $K/\mathbb{Q}$ is an

abelian extension of odd degree with Galois group G and the exponent of G is in D, Theorem 9.25 describes the 2-nd virtual group of K as a graph of a $(\mathbb{Z}/2\mathbb{Z})[G]$-module isomorphism of free $(\mathbb{Z}/2\mathbb{Z})[G]$-modules of rank 1 that is also an isomorphism of skew abelian groups. This description in the case of cyclic number field extensions of $\mathbb{Q}$ of degree either 3 or 5 is the essence of Theorem 9.27, Theorem 9.30 and Theorem 9.33.

9.2 Group rings

Lemma 9.6. *Let G be a finite group, let $^- : (\mathbb{Z}/2\mathbb{Z})[G] \to (\mathbb{Z}/2\mathbb{Z})[G]$ be the ring anti-automorphism that maps each element of G to its inverse, let $p_1 : (\mathbb{Z}/2\mathbb{Z})[G] \to \mathbb{Z}/2\mathbb{Z}$ be the nonzero additive group homomorphism that maps each element of G different from the identity to 0, and let α be the map*

$$\begin{aligned}\alpha : (\mathbb{Z}/2\mathbb{Z})[G] \times (\mathbb{Z}/2\mathbb{Z})[G] &\to \mathbb{Z}/2\mathbb{Z},\\ (f, g) &\mapsto p_1(f\overline{g}).\end{aligned}$$

Then the triple $((\mathbb{Z}/2\mathbb{Z})[G], \mathbb{Z}/2\mathbb{Z}, \alpha)$ is a skew abelian group.

Proof. Since α is an antisymmetric perfect pairing, the statement of Lemma 9.6 follows. □

Remark 9.7. Let the notation be as in Lemma 9.6. Then the underlying set of G is a basis of the $(\mathbb{Z}/2\mathbb{Z})$-vector space $(\mathbb{Z}/2\mathbb{Z})[G]$ and for all $\sigma, \tau \in G$ one has

$$\alpha(\sigma, \tau) = \begin{cases} 0 & \text{if } \sigma \neq \tau,\\ 1 & \text{if } \sigma = \tau.\end{cases}$$

Lemma 9.8. *Let the notation be as in* Lemma 9.6. *Let Φ be the group of $(\mathbb{Z}/2\mathbb{Z})[G]$-module isomorphisms $(\mathbb{Z}/2\mathbb{Z})[G] \xrightarrow{\sim} (\mathbb{Z}/2\mathbb{Z})[G]$ that are isomorphisms of skew abelian groups $((\mathbb{Z}/2\mathbb{Z})[G], \mathbb{Z}/2\mathbb{Z}, \alpha) \xrightarrow{\sim} ((\mathbb{Z}/2\mathbb{Z})[G], \mathbb{Z}/2\mathbb{Z}, \alpha)$. Then there is a group isomorphism*

$$\Phi \to \{u \in (\mathbb{Z}/2\mathbb{Z})[G]^* : u\overline{u} = 1\}$$

given by

$$\varphi \mapsto \overline{\varphi(1)}.$$

Proof. Let R be the ring $(\mathbb{Z}/2\mathbb{Z})[G]$. The opposite ring R^{op} of R is isomorphic to the endomorphism ring of the left R-module R by the mapping each element $r \in R^{\mathrm{op}}$ to the endomorphism given by right multiplication by r. Hence, there is a group isomorphism $\{R\text{-module isomorphisms } R \to R\} \to R^*$ given by $\varphi \mapsto \varphi(1)^{-1}$. Let φ be an R-module isomorphism $R \to R$. By definition

of isomorphism of skew abelian groups, we have $\varphi \in \Phi$ if and only if for all $f, g \in R$ we have $\alpha(f, g) = \alpha(\varphi(f), \varphi(g))$, that is $p_1(f\overline{g})$ and $p_1(f\varphi(1)\overline{\varphi(1)}\overline{g})$ are equal. Hence $\varphi \in \Phi$ is equivalent to $\varphi(1)\overline{\varphi(1)} = 1$. The statement of Lemma 9.8 follows. □

Remark 9.9. Let K be a field and let G be a group. The subgroup

$$\{u \in K[G]^* : u\overline{u} = 1\}$$

of the group of units of $K[G]$ is often called the *unitary subgroup*. See [69] by Szakács for a description of the structure of the unitary subgroup of the group of units of $K[G]$ when G is a finite abelian group.

Theorem 9.10. *Let G be a finite abelian group of odd order, let M be a free $(\mathbb{Z}/2\mathbb{Z})[G]$-module of rank 1, let $\delta : M \times M \to \mathbb{Z}/2\mathbb{Z}$ be an antisymmetric perfect pairing that for each $\sigma \in G$ and for all $x, y \in M$ satisfies $\delta(\sigma(x), \sigma(y)) = \delta(x, y)$, and let $((\mathbb{Z}/2\mathbb{Z})[G], \mathbb{Z}/2\mathbb{Z}, \alpha)$ be the skew abelian group defined as in* Lemma 9.6. *Then there exists a $(\mathbb{Z}/2\mathbb{Z})[G]$-module isomorphism $M \to (\mathbb{Z}/2\mathbb{Z})[G]$ that is an isomorphism of skew abelian groups from $(M, \mathbb{Z}/2\mathbb{Z}, \delta)$ to $((\mathbb{Z}/2\mathbb{Z})[G], \mathbb{Z}/2\mathbb{Z}, \alpha)$.*

Proof. Let R be the ring $(\mathbb{Z}/2\mathbb{Z})[G]$ and let $e \in M$ be a generator of M as an R-module. Since the $(\mathbb{Z}/2\mathbb{Z})$-dual of M is a free R-module of rank 1, there exists $u \in R$ that for each $z \in R$ satisfies $\delta(ze, e) = p_1(zu)$. Let $u \in R$ be such an element. For each $\sigma \in G$ and for each $w \in R$ we have

$$\delta(we, \sigma e) = \delta(\overline{\sigma}we, e) = p_1(\overline{\sigma}wu) = p_1(wu\overline{\sigma}).$$

By linearity of δ in the second argument, for all $w, z \in R$ we get

$$\delta(we, ze) = p_1(wu\overline{z}).$$

Since δ is a perfect pairing, we have $u \in R^*$. By symmetry of δ we get $u = \overline{u}$. Since by Maschke's Theorem the group ring R is semisimple, the Artin–Wedderburn theorem implies that it is isomorphic to a product of finite fields of characteristic 2. Hence u has odd order. Let d be the order of u and let $v = u^{\frac{d+1}{2}}$. Since we have $v\overline{v} = u$, for all $w, z \in R$ we get

$$\delta(we, ze) = \alpha(wv, zv).$$

Hence, the R-module isomorphism $M \to R$ that maps e to v is an isomorphism of skew abelian groups from $(M, \mathbb{Z}/2\mathbb{Z}, \delta)$ to $((\mathbb{Z}/2\mathbb{Z})[G], \mathbb{Z}/2\mathbb{Z}, \alpha)$. □

Lemma 9.11. *Let G be a finite abelian group of odd order, let e be the exponent of G, and let $\alpha : (\mathbb{Z}/2\mathbb{Z})[G] \times (\mathbb{Z}/2\mathbb{Z})[G] \to \mathbb{Z}/2\mathbb{Z}$ be the map defined in* Lemma 9.6. *Suppose that the residue class of -1 in $(\mathbb{Z}/e\mathbb{Z})^*$ is contained in the subgroup generated by the residue class of 2. Then $(\mathbb{Z}/2\mathbb{Z})[G]$ has no nontrivial self-annihilating sub-$(\mathbb{Z}/2\mathbb{Z})[G]$-modules with respect to α.*

Proof. Let k be an integer satisfying the congruence $2^k \equiv -1 \bmod e$. Since by Maschke's Theorem the group ring $(\mathbb{Z}/2\mathbb{Z})[G]$ is semisimple, the Artin–Wedderburn theorem implies that it is isomorphic to a product of finite fields of characteristic 2. The ring isomorphism $^- : (\mathbb{Z}/2\mathbb{Z})[G] \to (\mathbb{Z}/2\mathbb{Z})[G]$ that maps each element of G to its inverse acts as an automorphism on each finite field in the product, because for each $g \in G$ we have $g^{2^k} = g^{-1}$. Since α is a perfect pairing, on each component isomorphic to a finite field the map p_1 defined in Lemma 9.6 is not the zero map. The statement of Lemma 9.11 follows. □

Lemma 9.12. *Let p be an odd prime, let G a cyclic group of order p, let σ be a generator of G, and let $^- : (\mathbb{Z}/2\mathbb{Z})[G] \to (\mathbb{Z}/2\mathbb{Z})[G]$ be the ring isomorphism that maps σ to σ^{-1}. Suppose that the residue class of 2 in the group $(\mathbb{Z}/p\mathbb{Z})^*$ has even order and let d be its order. Then one has*

$$|\{u \in (\mathbb{Z}/2\mathbb{Z})[G]^* : u\overline{u} = 1\}| = (2^{d/2} + 1)^{\frac{p-1}{d}}.$$

Proof. The group ring $(\mathbb{Z}/2\mathbb{Z})[G]$ is isomorphic to the ring $(\mathbb{Z}/2\mathbb{Z})[X]/(X^p - 1)$ by mapping σ to the residue class of X. Let $\mathbb{F}_{2^d}$ be a finite field of 2^d elements. The factorization of $X^p - 1$ in $(\mathbb{Z}/2\mathbb{Z})[X]$ and the Chinese remainder theorem give a ring isomorphism

$$(\mathbb{Z}/2\mathbb{Z})[G] \xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z} \times (\mathbb{F}_{2^d})^{\frac{p-1}{d}}.$$

Since we have $2^{d/2} \equiv -1 \bmod p$ and $\overline{X} = X^{-1}$, we get $\overline{X} \equiv X^{2^{d/2}} \bmod X^p - 1$. Hence, the ring isomorphism $^- : (\mathbb{Z}/2\mathbb{Z})[G] \to (\mathbb{Z}/2\mathbb{Z})[G]$ maps every element in the ring to its $2^{d/2}$-th power and acts as an automorphism on each component isomorphic to the field $\mathbb{F}_{2^d}$. Since the equation $y^{2^{d/2}+1} = 1$ has $2^{d/2} + 1$ solutions in $\mathbb{F}_{2^d}$, the statement of Lemma 9.12 follows. □

Corollary 9.13. *Let the notation and hypotheses be as in* Lemma 9.12. *Then the following are equivalent.*

(i) *One has* $\{u \in (\mathbb{Z}/2\mathbb{Z})[G]^* : u\overline{u} = 1\} = G$.
(ii) *One has* $|\{u \in (\mathbb{Z}/2\mathbb{Z})[G]^* : u\overline{u} = 1\}| = p$.
(iii) *The prime p equals either* 3 *or* 5.

Proof. The inclusion $G \subseteq \{u \in (\mathbb{Z}/2\mathbb{Z})[G]^* : u\overline{u} = 1\}$ implies the equivalence between (i) and (ii). Since the pairs (d, p) of integers satisfying the equalities

$$\begin{cases} 2^{d/2} + 1 = p \\ \dfrac{p-1}{d} = 1 \end{cases}$$

are $(2, 3)$ and $(4, 5)$, by Lemma 9.12 we get the equivalence between (ii) and (iii). □

Corollary 9.14. *Let p be either 3 or 5, let G be a cyclic group of order p, let $\varphi : (\mathbb{Z}/2\mathbb{Z})[G] \to (\mathbb{Z}/2\mathbb{Z})[G]$ be a $(\mathbb{Z}/2\mathbb{Z})[G]$-module isomorphism, and let $\alpha : (\mathbb{Z}/2\mathbb{Z})[G] \times (\mathbb{Z}/2\mathbb{Z})[G] \to \mathbb{Z}/2\mathbb{Z}$ be the map defined in* Lemma 9.6. *Then the following are equivalent.*

(i) *The map φ is an isomorphism of skew abelian groups*

$$((\mathbb{Z}/2\mathbb{Z})[G], \mathbb{Z}/2\mathbb{Z}, \alpha) \xrightarrow{\sim} ((\mathbb{Z}/2\mathbb{Z})[G], \mathbb{Z}/2\mathbb{Z}, \alpha).$$

(ii) *The map φ permutes the basis $\{g : g \in G\}$ of the vector space $(\mathbb{Z}/2\mathbb{Z})[G]$ over $\mathbb{Z}/2\mathbb{Z}$.*

Proof. This follows from Lemma 9.8 and Corollary 9.13. □

Lemma 9.15. *Let n be a positive integer, let $\mathbb{F}_{2^n}$ be a finite field of 2^n elements, let $\mathrm{Tr} : \mathbb{F}_{2^n} \to \mathbb{Z}/2\mathbb{Z}$ be the trace map, and let δ be the map*

$$\begin{aligned} \delta : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} &\to \mathbb{Z}/2\mathbb{Z}, \\ (a, b) &\mapsto \mathrm{Tr}(ab). \end{aligned}$$

Then the triple $(\mathbb{F}_{2^n}, \mathbb{Z}/2\mathbb{Z}, \delta)$ is a skew abelian group.

Proof. The map δ is a perfect pairing, because the field extension $\mathbb{F}_{2^n}/(\mathbb{Z}/2\mathbb{Z})$ is separable. Since by definition it is symmetric and the field $\mathbb{Z}/2\mathbb{Z}$ has characteristic 2, it is antisymmetric. Hence, the triple $(\mathbb{F}_{2^n}, \mathbb{Z}/2\mathbb{Z}, \delta)$ is a skew abelian group. □

Definition 9.16 (Self-dual basis)**.** Let n be a positive integer, let L/K be a Galois field extension of degree n, and let $\mathrm{Tr} : L \to K$ be the trace map. A basis $\{e_i : i \in \mathbb{Z}/n\mathbb{Z}\}$ of the K-vector space L is a *self-dual basis* if for all $i, j \in \mathbb{Z}/n\mathbb{Z}$ one has

$$\mathrm{Tr}(e_i e_j) = \begin{cases} 0 & \text{if } i \neq j, \\ 1 & \text{if } i = j. \end{cases}$$

Theorem 9.17. *Let the notation be as in* Lemma 9.15*, let G be the Galois group of the field extension $\mathbb{F}_{2^n}/(\mathbb{Z}/2\mathbb{Z})$, and let $((\mathbb{Z}/2\mathbb{Z})[G], \mathbb{Z}/2\mathbb{Z}, \alpha)$ be the skew abelian group defined as in* Lemma 9.6*. Suppose that n is odd. Then there exists a $(\mathbb{Z}/2\mathbb{Z})[G]$-module isomorphism $\mathbb{F}_{2^n} \to (\mathbb{Z}/2\mathbb{Z})[G]$ that is an isomorphism of skew abelian groups from $(\mathbb{F}_{2^n}, \mathbb{Z}/2\mathbb{Z}, \delta)$ to $((\mathbb{Z}/2\mathbb{Z})[G], \mathbb{Z}/2\mathbb{Z}, \alpha)$.*

Proof. The field $\mathbb{F}_{2^n}$ is a free $(\mathbb{Z}/2\mathbb{Z})[G]$-module of rank 1. Since for each $\sigma \in G$ and for all $a, b \in \mathbb{F}_{2^n}$ we have

$$\delta(\sigma(a), \sigma(b)) = \delta(a, b),$$

the statement of Theorem 9.17 follows from Theorem 9.10. □

Corollary 9.18. *Every finite extension of $\mathbb{Z}/2\mathbb{Z}$ of odd degree has a self-dual normal basis.*

Proof. This follows from Theorem 9.17 and Remark 9.7. □

One may wonder which finite field extensions have a self-dual normal basis. A complete answer was given by Lempel and Weinberger [40]. Theorem 9.19 extends their result to finite abelian extensions of arbitrary fields.

Theorem 9.19 (Bayer-Fluckiger and Lenstra [4])**.** *Let n be a positive integer and let L/K be an abelian field extension of degree n.*

(a) *If K does not have characteristic 2, then L has a self-dual normal basis over K if and only if n is odd.*

(b) *If K has characteristic 2, then L has a self-dual normal basis over K if and only if the exponent of the Galois group of L/K is not divisible by 4.*

Proof. See Theorem 6.1 in [4] by Bayer-Fluckiger and Lenstra. □

9.3 Number fields unramified at two

Theorem 9.20. *Let $K/\mathbb{Q}$ be a Galois extension of number fields unramified at 2, let G be its Galois group, let $\mathcal{O}_K$ be the ring of integers of K, and let S_∞ be the set of Archimedean places of K. For each prime ideal $\mathfrak{P}$ of $\mathcal{O}_K$ dividing 2 denote by $\mathrm{Tr}_{\mathfrak{P}}$ the trace map from $\mathcal{O}_K/\mathfrak{P}$ to $\mathbb{Z}/2\mathbb{Z}$. Let β be the map*

$$\begin{aligned}\beta : \mathcal{O}_K/2\mathcal{O}_K \times \mathcal{O}_K/2\mathcal{O}_K &\to \{\pm 1\},\\ (a+2\mathcal{O}_K, b+2\mathcal{O}_K) &\mapsto \prod_{\mathfrak{P}\mid 2} (-1)^{\mathrm{Tr}_{\mathfrak{P}}(ab+\mathfrak{P})},\end{aligned}$$

with $\mathfrak{P}$ ranging over all prime ideals of $\mathcal{O}_K$ dividing 2 and let γ be the map

$$\begin{aligned}\gamma : \bigoplus_{v \text{ real}} \mathbb{R}^*/\mathbb{R}_{>0} \times \bigoplus_{v \text{ real}} \mathbb{R}^*/\mathbb{R}_{>0} &\to \{\pm 1\},\\ ((a_v \cdot \mathbb{R}_{>0})_v, (b_v \cdot \mathbb{R}_{>0})_v) &\mapsto \prod_{v \text{ real}} (-1)^{\frac{a_v - |a_v|_v}{2a_v}\frac{b_v - |b_v|_v}{2b_v}},\end{aligned}$$

with v ranging over all real Archimedean places of K. Then there is a natural $(\mathbb{Z}/2\mathbb{Z})[G]$-module isomorphism from a product of two free $(\mathbb{Z}/2\mathbb{Z})[G]$-modules to a free $(\mathbb{Z}/2\mathbb{Z})[G]$-module

$$\mathcal{O}_K/2\mathcal{O}_K \times \left(\bigoplus_{v \text{ real}} \mathbb{R}^*/\mathbb{R}_{>0}\right) \xrightarrow{\sim} \overline{U}/\overline{U}^{\perp} \tag{9.21}$$

that is an isomorphism of skew abelian groups from

$$(\mathcal{O}_K/2\mathcal{O}_K, \{\pm 1\}, \beta) \perp \left(\bigoplus_{v \text{ real}} \mathbb{R}^*/\mathbb{R}_{>0}, \{\pm 1\}, \gamma \right)$$

to the 2-nd unit residue group of K.

Proof. By Theorem 5.6 the 2-nd unit residue group of K is isomorphic to an orthogonal sum of skew abelian groups that are defined locally at the places of K dividing 2 and at the real Archimedean places of K.

Firstly, we consider the skew abelian groups that are defined locally at the places of K dividing 2. Since the group isomorphism given by Theorem 5.12 respects the natural actions of G on $(\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2}$ and on $\prod_{v|2} U_v/U_v^{\perp}$, we get a natural $(\mathbb{Z}/2\mathbb{Z})[G]$-module isomorphism

$$(\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2} \xrightarrow{\sim} \prod_{v|2} U_v/U_v^{\perp}.$$

Composing this map with the $(\mathbb{Z}/2\mathbb{Z})[G]$-module isomorphism of free $(\mathbb{Z}/2\mathbb{Z})[G]$-modules of rank 1 in Lemma 6.6

$$\begin{aligned} \mathcal{O}_K/2\mathcal{O}_K &\xrightarrow{\sim} (\mathcal{O}_K/4\mathcal{O}_K)^*/(\mathcal{O}_K/4\mathcal{O}_K)^{*2}, \\ a + 2\mathcal{O}_K &\mapsto (1 + 2a + 4\mathcal{O}_K) \cdot (\mathcal{O}_K/4\mathcal{O}_K)^{*2}, \end{aligned}$$

gives a $(\mathbb{Z}/2\mathbb{Z})[G]$-module isomorphism of free $(\mathbb{Z}/2\mathbb{Z})[G]$-modules of rank 1

$$\mathcal{O}_K/2\mathcal{O}_K \xrightarrow{\sim} \prod_{v|2} U_v/U_v^{\perp}.$$

This $(\mathbb{Z}/2\mathbb{Z})[G]$-module isomorphism, the explicit description of the quadratic norm-residue symbol in Lemma 3.106, Theorem 3.82, and Theorem 3.81 for the skew abelian groups at the real Archimedean places of K give the natural $(\mathbb{Z}/2\mathbb{Z})[G]$-module isomorphism of free $(\mathbb{Z}/2\mathbb{Z})[G]$-modules in the statement of Theorem 9.20. □

Remark 9.22. Let $K/\mathbb{Q}$ be a Galois extension of number fields unramified at 2 and let G be its Galois group. Then the 2-nd unit residue group of K is a free $(\mathbb{Z}/2\mathbb{Z})[G]$-module of rank either 1 or 2 according as the extension $K/\mathbb{Q}$ is complex or real.

Remark 9.23. Let the notation be as in Theorem 9.20. Then for each $\sigma \in G$ and for all $a, b \in \mathcal{O}_K/2\mathcal{O}_K$ one has

$$\beta(\sigma(a), \sigma(b)) = \beta(a, b)$$

and for each $\sigma \in G$ and for all $a, b \in \bigoplus_{v \text{ real}} \mathbb{R}^*/\mathbb{R}_{>0}$ one has

$$\gamma(\sigma(a), \sigma(b)) = \gamma(a, b).$$

Lemma 9.24. *Let $K/\mathbb{Q}$ be an abelian extension of number fields of odd degree. Then $K/\mathbb{Q}$ is unramified both at 2 and at infinity.*

Proof. Let $\mathbb{Q}_2$ be the field of 2-adic rationals. Since all subgroups of $\mathbb{Q}_2^*$ of odd index contain the group of units of the ring of integers of $\mathbb{Q}_2$, local class field theory implies that abelian extensions of $\mathbb{Q}_2$ of odd degree are unramified. Hence, the extension $K/\mathbb{Q}$ is unramified at 2.

Similarly, since $\mathbb{R}_{>0}$ is the only subgroup of finite index of $\mathbb{R}^*$ and has index 2, all Archimedean places of K are real. Hence, the extension $K/\mathbb{Q}$ is unramified at infinity. □

Theorem 9.25. *Let $K/\mathbb{Q}$ be an abelian extension of number fields of odd degree, let G be its Galois group, let e be the exponent of G, let $\mathcal{O}_K$ be the ring of integers of K, and let S_∞ be the set of Archimedean places of K. Suppose that the residue class of -1 in $(\mathbb{Z}/e\mathbb{Z})^*$ is contained in the subgroup generated by the residue class of 2. Let the triples*

$$(\bigoplus_{\mathfrak{P}|2} \mathcal{O}_K/\mathfrak{P}\mathcal{O}_K, \{\pm 1\}, \beta) \quad \text{and} \quad (\bigoplus_{v \in S_\infty} \mathbb{R}^*/\mathbb{R}_{>0}, \{\pm 1\}, \gamma)$$

be the skew abelian groups defined as in Theorem 9.20. *Then the preimage of the 2-nd virtual group of K under the natural $(\mathbb{Z}/2\mathbb{Z})[G]$-module isomorphism* 9.21 *is the graph of a $(\mathbb{Z}/2\mathbb{Z})[G]$-module isomorphism of free $(\mathbb{Z}/2\mathbb{Z})[G]$-modules of rank* 1

$$\mathcal{O}_K/2\mathcal{O}_K \xrightarrow{\sim} \bigoplus_{v \in S_\infty} \mathbb{R}^*/\mathbb{R}_{>0}$$

that is an isomorphism of skew abelian groups

$$(\bigoplus_{\mathfrak{P}|2} \mathcal{O}_K/\mathfrak{P}\mathcal{O}_K, \{\pm 1\}, \beta) \xrightarrow{\sim} (\bigoplus_{v \in S_\infty} \mathbb{R}^*/\mathbb{R}_{>0}, \{\pm 1\}, \gamma).$$

Proof. By Lemma 9.24 the extension $K/\mathbb{Q}$ is unramified at 2 and S_∞ contains only real places. By Lemma 6.6 the $(\mathbb{Z}/2\mathbb{Z})[G]$-module $\mathcal{O}_K/2\mathcal{O}_K$ is free of rank 1. Its image under the $(\mathbb{Z}/2\mathbb{Z})[G]$-module isomorphism 9.21 is the product of the local components of the 2-nd unit residue group of K at the places dividing 2.

Let S be the set of places of K and let π_2 be the canonical projection

$$\pi_2 : \prod_{v \in S} U_v/U_v^\perp \twoheadrightarrow \prod_{v|2} U_v/U_v^\perp$$

of the 2-nd unit residue group of K on the product of its local components at the places of K dividing 2. Similarly, let π_∞ be the canonical projection of the 2-nd unit residue group of K on the product of its local components at the Archimedean places. Let V be the 2-nd virtual group of K.

Since V is a self-annihilating subgroup of the 2-nd unit residue group of K, the preimage of $\ker \pi_2 \cap V$ under the isomorphism 9.21 gives a self-annihilating submodule of the skew abelian group $(\bigoplus_{\mathfrak{P}|2} \mathcal{O}_K/\mathfrak{P}\mathcal{O}_K, \{\pm 1\}, \beta)$. By Theorem 9.10 this skew abelian group is isomorphic to the skew abelian group $((\mathbb{Z}/2\mathbb{Z})[G], \mathbb{Z}/2\mathbb{Z}, \alpha)$ defined as in Lemma 9.6. Lemma 9.11 implies that the preimage of $\ker \pi_2 \cap V$ under the isomorphism 9.21 is trivial. By Theorem 5.17 the cardinality of V equals $2^{|G|}$ and therefore π_2 gives a $(\mathbb{Z}/2\mathbb{Z})[G]$-module isomorphism

$$V \xrightarrow{\sim} \prod_{v|2} U_v/U_v^{\perp}.$$

Analogously, it follows that the canonical projection of the 2-nd unit residue group of K on the product of its local components at the Archimedean places maps V isomorphically to this product. Hence V is a submodule of a product of two modules that maps bijectively both to the first factor and to the second factor. The statement of Theorem 9.25 follows. □

9.4 Cubic and quintic number fields

Definition 9.26 (Permutation module)**.** Let F be a field and let G be a finite group. A *permutation module* over $F[G]$ is an $F[G]$-module that has an F-basis permuted by G.

Theorem 9.27. *Let p be either 3 or 5, let $K/\mathbb{Q}$ be a cyclic number field extension of degree p, let G be its Galois group, let $\mathcal{O}_K$ be the ring of integers of K, and let S_∞ be the set of Archimedean places of K. Suppose that the rational prime 2 splits completely in the ring of integers of K and let S_2 be the set of prime ideals of $\mathcal{O}_K$ dividing 2. Then the preimage of the 2-nd virtual group of K under the natural $(\mathbb{Z}/2\mathbb{Z})[G]$-module isomorphism 9.21 is the graph of an isomorphism*

$$\bigoplus_{\mathfrak{P}\in S_2} \mathcal{O}_K/\mathfrak{P}\mathcal{O}_K \xrightarrow{\sim} \bigoplus_{v\in S_\infty} \mathbb{R}^*/\mathbb{R}_{>0}$$

of permutation modules over $(\mathbb{Z}/2\mathbb{Z})[G]$ that maps the $\mathbb{Z}/2\mathbb{Z}$-basis given by the nontrivial elements in the groups $\{\mathcal{O}_K/\mathfrak{P}\mathcal{O}_K : \mathfrak{P} \in S_2\}$ to the $\mathbb{Z}/2\mathbb{Z}$-basis given by the nontrivial elements in the groups $\{(\mathbb{R}^*/\mathbb{R}_{>0})_v : v \in S_\infty\}$.

Proof. Let the triples

$$(\bigoplus_{\mathfrak{P}|2} \mathcal{O}_K/\mathfrak{P}\mathcal{O}_K, \{\pm 1\}, \beta) \quad \text{and} \quad (\bigoplus_{v \text{ real}} \mathbb{R}^*/\mathbb{R}_{>0}, \{\pm 1\}, \gamma)$$

be the skew abelian groups defined as in Theorem 9.20. By Theorem 9.25 the preimage of the 2-nd virtual group of K under the natural $(\mathbb{Z}/2\mathbb{Z})[G]$-module isomorphism 9.21 is the graph of a $(\mathbb{Z}/2\mathbb{Z})[G]$-module isomorphism of free $(\mathbb{Z}/2\mathbb{Z})[G]$-modules of rank 1

$$\bigoplus_{\mathfrak{P} \in S_2} \mathcal{O}_K/\mathfrak{P}\mathcal{O}_K \xrightarrow{\sim} \bigoplus_{v \text{ real}} \mathbb{R}^*/\mathbb{R}_{>0} \tag{9.28}$$

that is an isomorphism of skew abelian groups

$$(\bigoplus_{\mathfrak{P}|2} \mathcal{O}_K/\mathfrak{P}\mathcal{O}_K, \{\pm 1\}, \beta) \xrightarrow{\sim} (\bigoplus_{v \text{ real}} \mathbb{R}^*/\mathbb{R}_{>0}, \{\pm 1\}, \gamma).$$

By Theorem 9.10 each of these two skew abelian groups is isomorphic to the skew abelian group $((\mathbb{Z}/2\mathbb{Z})[G], \mathbb{Z}/2\mathbb{Z}, \alpha)$ defined as in Lemma 9.6. Corollary 9.14 implies that the $(\mathbb{Z}/2\mathbb{Z})[G]$-module isomorphism 9.28 maps the $\mathbb{Z}/2\mathbb{Z}$-basis given by the nontrivial elements in the groups $\{\mathcal{O}_K/\mathfrak{P}\mathcal{O}_K : \mathfrak{P} \in S_2\}$ to the $\mathbb{Z}/2\mathbb{Z}$-basis given by the nontrivial elements in the groups $\{(\mathbb{R}^*/\mathbb{R}_{>0})_v : v \in S_\infty\}$. □

Lemma 9.29. *Let $\mathbb{F}_{2^3}$ be a finite field of 8 elements. Then the set of roots in $\mathbb{F}_{2^3}$ of the polynomial $X^3 + X^2 + 1$ is the unique self-dual normal basis of $\mathbb{F}_{2^3}$ over $\mathbb{Z}/2\mathbb{Z}$.*

Proof. Let b_1, b_2, and b_3 be the roots in $\mathbb{F}_{2^3}$ of the polynomial $X^3 + X^2 + 1$ and let $i, j \in \{1, 2, 3\}$. If we have $i \neq j$, we get $\mathrm{Tr}(b_i b_j) = 0$, because $\mathrm{Tr}(b_i b_j)$ equals the first degree coefficient of the polynomial $X^3 + X^2 + 1$. Otherwise, we have $\mathrm{Tr}(b_i b_j) = 1$. Indeed, since the field $\mathbb{F}_{2^3}$ has characteristic 2, the second degree coefficient of the polynomial $X^3 + X^2 + 1$ equals $\mathrm{Tr}(b_i)$ and we have $\mathrm{Tr}(b_i^2) = \mathrm{Tr}(b_i)^2$. Hence, the set $\{b_1, b_2, b_3\}$ is a self-dual normal basis of $\mathbb{F}_{2^3}$ over $\mathbb{Z}/2\mathbb{Z}$.

Corollary 9.14 and Theorem 9.17 imply that there is a unique self-dual normal basis of $\mathbb{F}_{2^3}$ over $\mathbb{Z}/2\mathbb{Z}$. □

Theorem 9.30. *Let $K/\mathbb{Q}$ be a cyclic extension of number fields of degree 3, let G be its Galois group, let $\mathcal{O}_K$ be the ring of integers of K, and let S_∞ be the set of Archimedean places of K. Suppose that the rational prime 2 is inert in $\mathcal{O}_K$ and let $S_2 = \{x \in \mathcal{O}_K/2\mathcal{O}_K : x^3 + x^2 + 1 = 0\}$. Then the preimage of the*

2-nd virtual group of K under the natural $(\mathbb{Z}/2\mathbb{Z})[G]$-module isomorphism 9.21 *is the graph of an isomorphism*

$$\bigoplus_{x\in S_2}(\mathbb{Z}/2\mathbb{Z})\cdot x \xrightarrow{\sim} \bigoplus_{v\in S_\infty}\mathbb{R}^*/\mathbb{R}_{>0}$$

of permutation modules over $(\mathbb{Z}/2\mathbb{Z})[G]$ that maps the $\mathbb{Z}/2\mathbb{Z}$-basis S_2 to the $\mathbb{Z}/2\mathbb{Z}$-basis given by the nontrivial elements in the groups $\{(\mathbb{R}^*/\mathbb{R}_{>0})_v : v\in S_\infty\}$.

Proof. Let the triples

$$(\bigoplus_{x\in S_2}(\mathbb{Z}/2\mathbb{Z})\cdot x, \{\pm 1\}, \beta) \quad \text{and} \quad (\bigoplus_{v \text{ real}}\mathbb{R}^*/\mathbb{R}_{>0}, \{\pm 1\}, \gamma)$$

be the skew abelian groups defined as in Theorem 9.20. By Theorem 9.25 the preimage of the 2-nd virtual group of K under the natural $(\mathbb{Z}/2\mathbb{Z})[G]$-module isomorphism 9.21 is the graph of a $(\mathbb{Z}/2\mathbb{Z})[G]$-module isomorphism of free $(\mathbb{Z}/2\mathbb{Z})[G]$-modules of rank 1

$$\bigoplus_{x\in S_2}(\mathbb{Z}/2\mathbb{Z})\cdot x \xrightarrow{\sim} \bigoplus_{v \text{ real}}\mathbb{R}^*/\mathbb{R}_{>0} \tag{9.31}$$

that is an isomorphism of skew abelian groups

$$(\bigoplus_{x\in S_2}(\mathbb{Z}/2\mathbb{Z})\cdot x, \{\pm 1\}, \beta) \xrightarrow{\sim} (\bigoplus_{v \text{ real}}\mathbb{R}^*/\mathbb{R}_{>0}, \{\pm 1\}, \gamma).$$

By Theorem 9.10 each of these two skew abelian groups is isomorphic by a $(\mathbb{Z}/2\mathbb{Z})[G]$-module isomorphism to the skew abelian group $((\mathbb{Z}/2\mathbb{Z})[G], \mathbb{Z}/2\mathbb{Z}, \alpha)$ defined as in Lemma 9.6. Corollary 9.14 implies that the $(\mathbb{Z}/2\mathbb{Z})[G]$-module isomorphism 9.31 maps the $\mathbb{Z}/2\mathbb{Z}$-basis S_2 to the $\mathbb{Z}/2\mathbb{Z}$-basis given by the nontrivial elements in the groups $\{(\mathbb{R}^*/\mathbb{R}_{>0})_v : v\in S_\infty\}$. □

Lemma 9.32. *Let $\mathbb{F}_{2^5}$ be a finite field of 32 elements. Then the set of roots in $\mathbb{F}_{2^5}$ of the polynomial $X^5+X^4+X^2+X+1$ is the unique self-dual normal basis of $\mathbb{F}_{2^5}$ over $\mathbb{Z}/2\mathbb{Z}$.*

Proof. Let $f(X)=X^5+X^4+X^2+X+1$, let b be a root in $\mathbb{F}_{2^5}$ of $f(X)$, and let $\mathrm{Tr}:\mathbb{F}_{2^5}\to\mathbb{Z}/2\mathbb{Z}$ be the trace map of the Galois extension $\mathbb{F}_{2^5}/(\mathbb{Z}/2\mathbb{Z})$. We get $\mathrm{Tr}(b^2)=1$, because we have $\mathrm{Tr}(b^2)=\mathrm{Tr}(b)^2$ and $\mathrm{Tr}(b)$ equals the fourth degree coefficient of $f(X)$. The trace of the product of two different Galois conjugates of b equals either $\mathrm{Tr}(b^3)$ or $\mathrm{Tr}(b^5)$ and the third degree coefficient of $f(X)$, which is zero, equals $\mathrm{Tr}(b^3)+\mathrm{Tr}(b^5)$. Hence, to prove that the set $\{b, b^2, b^4, b^8, b^{16}\}$ is a self-dual normal basis of $\mathbb{F}_{2^5}$ over $\mathbb{Z}/2\mathbb{Z}$, it suffices to show

the equality $\mathrm{Tr}(b^5) = 0$. Since b^2 and b^4 are Galois conjugates, they have the same trace. From the equality $b^5 = b^4 + b^2 + b + 1$ we get $\mathrm{Tr}(b^5) = \mathrm{Tr}(b) + \mathrm{Tr}(1)$ and therefore $\mathrm{Tr}(b^5) = 0$.

Corollary 9.14 and Theorem 9.17 imply that there is a unique self-dual normal basis of $\mathbb{F}_{2^5}$ over $\mathbb{Z}/2\mathbb{Z}$. □

Theorem 9.33. *Let $K/\mathbb{Q}$ be a cyclic extension of number fields of degree 5, let G be its Galois group, let $\mathcal{O}_K$ be the ring of integers of K, and let S_∞ be the set of Archimedean places of K. Suppose that the rational prime 2 is inert in $\mathcal{O}_K$ and let*

$$S_2 = \{x \in \mathcal{O}_K/2\mathcal{O}_K : x^5 + x^4 + x^2 + x + 1 = 0\}.$$

Then the preimage of the 2-nd virtual group of K under the natural $(\mathbb{Z}/2\mathbb{Z})[G]$-module isomorphism 9.21 is the graph of an isomorphism

$$\bigoplus_{x \in S_2} (\mathbb{Z}/2\mathbb{Z}) \cdot x \xrightarrow{\sim} \bigoplus_{v \in S_\infty} \mathbb{R}^*/\mathbb{R}_{>0}$$

of permutation modules over $(\mathbb{Z}/2\mathbb{Z})[G]$ that maps the $\mathbb{Z}/2\mathbb{Z}$-basis S_2 to the $\mathbb{Z}/2\mathbb{Z}$-basis given by the nontrivial elements in the groups $\{(\mathbb{R}^*/\mathbb{R}_{>0})_v : v \in S_\infty\}$.

Proof. Let the triples

$$(\bigoplus_{x \in S_2} (\mathbb{Z}/2\mathbb{Z}) \cdot x, \{\pm 1\}, \beta) \quad \text{and} \quad (\bigoplus_{v \text{ real}} \mathbb{R}^*/\mathbb{R}_{>0}, \{\pm 1\}, \gamma)$$

be the skew abelian groups defined as in Theorem 9.20. By Theorem 9.25 the preimage of the 2-nd virtual group of K under the natural $(\mathbb{Z}/2\mathbb{Z})[G]$-module isomorphism 9.21 is the graph of a $(\mathbb{Z}/2\mathbb{Z})[G]$-module isomorphism of free $(\mathbb{Z}/2\mathbb{Z})[G]$-modules of rank 1

$$\bigoplus_{x \in S_2} (\mathbb{Z}/2\mathbb{Z}) \cdot x \xrightarrow{\sim} \bigoplus_{v \text{ real}} \mathbb{R}^*/\mathbb{R}_{>0} \tag{9.34}$$

that is an isomorphism of skew abelian groups

$$(\bigoplus_{x \in S_2} (\mathbb{Z}/2\mathbb{Z}) \cdot x, \{\pm 1\}, \beta) \xrightarrow{\sim} (\bigoplus_{v \text{ real}} \mathbb{R}^*/\mathbb{R}_{>0}, \{\pm 1\}, \gamma).$$

By Theorem 9.10 each of these two skew abelian groups is isomorphic by a $(\mathbb{Z}/2\mathbb{Z})[G]$-module isomorphism to the skew abelian group $((\mathbb{Z}/2\mathbb{Z})[G], \mathbb{Z}/2\mathbb{Z}, \alpha)$ defined as in Lemma 9.6. Corollary 9.14 implies that the $(\mathbb{Z}/2\mathbb{Z})[G]$-module isomorphism 9.34 maps the $\mathbb{Z}/2\mathbb{Z}$-basis S_2 to the $\mathbb{Z}/2\mathbb{Z}$-basis given by the nontrivial elements in the groups $\{(\mathbb{R}^*/\mathbb{R}_{>0})_v : v \in S_\infty\}$. □

CHAPTER 10

A large norm group

10.1 Main results

Let p be a prime number and let F be a finite extension of the field $\mathbb{Q}_p$ of p-adic rationals. Let $\mathfrak{P}$ be the maximal ideal of the ring of integers of F and let $U^{(1)}$ be the group $U^{(1)} = 1 + \mathfrak{P}$, which is often called 'first higher unit group' or 'group of principal units' of the ring of integers of F. Theorem 3.37 and Theorem 3.38 imply that $U^{(1)}$ is an abelian pro-p-group, a group isomorphic to the inverse limit of an inverse system of discrete finite abelian p-groups. Since the quotient rings of $\mathbb{Z}$ of p-power order are naturally isomorphic to quotients of the ring $\mathbb{Z}_p$ of p-adic integers, the natural action of $\mathbb{Z}$ on abelian groups induces a continuous action of $\mathbb{Z}_p$ on pro-p-groups. Thus, this action makes abelian pro-p-groups into $\mathbb{Z}_p$-modules. In Theorem 10.1 for each prime element π of F we define the sub-$\mathbb{Z}_p$-module H_π of $U^{(1)}$, which is the subject of study in this chapter. The main results are Theorem 10.1 and Theorem 10.2.

Theorem 10.1. *Let p be a prime number and let F be a finite extension of the field $\mathbb{Q}_p$ of p-adic rationals. Let q be the cardinality of the residue field of F and let μ_{q-1} be the group of $q-1$-th roots of unity in F. Let $U^{(1)}$ be the first higher unit group of the ring of integers of F and for each prime element π of F let H_π be its subgroup*

$$H_\pi = \prod_{\substack{i \in \mathbb{Z}_{>0} \setminus p\mathbb{Z} \\ \zeta \in \mu_{q-1}}} (1 - \zeta \pi^i)^{\mathbb{Z}_p},$$

where $\mathbb{Z}_p$ is the ring of p-adic integers. Then for each prime element π of F the quotient group $U^{(1)}/H_\pi$ is cyclic of order p^n, where n is the maximal integer such that F contains a primitive p^n-th root of unity.

Proof. See Section 10.3. □

The case $n = 0$ of Theorem 10.1 is not very intriguing and follows from the equality $U^{(1)} = H_\pi$, which is an easy consequence of Lemma 10.7. Much more interesting is the result for $n > 0$. In this case the p^n-th power norm-residue symbol of F plays the dual role of both motivating the theorem and helping to prove it. In particular, the motivation comes from algorithms for computing the p^n-th power norm-residue symbol.

Let m be a positive integer. In [13] Daberkow proposed an algorithm for computing the m-th power norm-residue symbol in a local field F containing a primitive m-th root of unity. Note that by Remark 3.77 it is sufficient to deal with the case when m is a prime power. If the characteristic of the residue field of F does not divide m, then there is short formula for computing the symbol. Using Theorem 3.76 we assume $m = p^n$, where p is the characteristic of the residue field of F and n is the maximal integer such that F contains a primitive p^n-th root of unity. The computation is difficult when the local field F is a finite extension of the field $\mathbb{Q}_p$ of p-adic rationals and n is positive. In this case one shows easily the inclusion $H_\pi \subset \pi^\perp$ [Lemma 10.4], where π is a prime element of F and $\pi^\perp$ is the annihilator in F^* of π with respect to the p^n-th power norm-residue symbol, and the equality $U^{(1)} = \delta^{\mathbb{Z}_p} \cdot H_\pi$ [Lemma 10.11], where δ is a distinguished unit of F [Definition 10.8]. The main idea of Daberkow's algorithm and similar algorithms by Bouw [7] is to compute a distinguished unit δ of F and a prime element π of F in advance and for given $\alpha, \beta \in F^*$ write the symbol (α, β) as a power of the symbol (π, δ). In particular, the core part of Daberkow's algorithm expresses every norm-residue symbol of the form (π, u) with $u \in U^{(1)}$ as a power of (π, δ) by first using Lemma 10.11 in order to write an equality $u = \delta^k \cdot h$ with $k \in \mathbb{Z}_p$ and $h \in H_\pi$, and next using Lemma 10.4 to get $(\pi, u) = (\pi, \delta)^k$. Note that for the purpose of the algorithm it is enough to compute the value of k modulo p^n.

It is remarkable that the method just sketched works already before knowing the value of n. Of course it is needed that n is positive, because otherwise there is no distinguished unit of F, but (b) of Lemma 10.7 shows that it is easy to test this condition. Thus, it is natural to ask whether the number k has any significance independently of n and of the norm-residue symbol. Theorem 10.1 shows that the answer is negative: the value of k in the equality $u = \delta^k \cdot h$ is really only well-defined modulo p^n and since by Lemma 10.10 the p^n-th power norm-residue symbol (π, δ) has order p^n the integer k carries exactly the same information as the value of (π, u).

Theorem 10.2 clarifies the role of the norm-residue symbol.

Theorem 10.2. *Let the notation be as in* Theorem 10.1. *Let n be the maximal integer such that F contains a primitive p^n-th root of unity, let μ_{p^n} be the group of p^n-th roots of unity in F, and let $(\cdot,\cdot) : F^* \times F^* \to \mu_{p^n}$ be the p^n-th power norm-residue symbol of F. Then for each prime element π of F the map*

$$\begin{aligned} U^{(1)} &\to \mu_{p^n} \\ u &\mapsto (\pi, u) \end{aligned}$$

induces a group isomorphism

$$U^{(1)}/H_\pi \xrightarrow{\sim} \mu_{p^n}.$$

Proof. See Section 10.3. □

Using Theorem 10.2 the inclusion $H_\pi \subset \pi^\perp$ in Lemma 10.4 can be made more precise as stated in Corollary 10.3.

Corollary 10.3. *Let the notation be as in* Theorem 10.2. *Then for each prime element π of F one has the equality*

$$H_\pi = \pi^\perp \cap U^{(1)},$$

where $\pi^\perp$ is the annihilator in F^* of π with respect to the p^n-th power norm-residue symbol of F.

Proof. This follows from Theorem 10.2. □

10.2 Auxiliary results

Lemma 10.4. *Let the notation be as in* Theorem 10.2. *Then for each prime element π of F one has the inclusion*

$$H_\pi \subset \pi^\perp,$$

where $\pi^\perp$ is the annihilator in F^* of π with respect to the p^n-th power norm-residue symbol of F.

Proof. Let π be a prime element of F. Let $i \in \mathbb{Z}_{>0} \setminus p\mathbb{Z}$ and $\zeta \in \mu_{q-1}$. We have

$$1 = \left(1, 1-\zeta\pi^i\right) = \left(\zeta^{q-1}, 1-\zeta\pi^i\right) = \left(\zeta, 1-\zeta\pi^i\right)^{q-1}.$$

We get $\left(\zeta, 1-\zeta\pi^i\right) = 1$, because $q-1$ and p are coprime integers. By Theorem 3.74 for all $c \in F^* \setminus \{1\}$ we have $(c, 1-c) = 1$. Hence, we obtain

$$1 = \left(\zeta\pi^i, 1-\zeta\pi^i\right) = \left(\zeta, 1-\zeta\pi^i\right)\left(\pi^i, 1-\zeta\pi^i\right) = \left(\pi, 1-\zeta\pi^i\right)^i.$$

Since i and p are coprime integers, we get $\left(\pi, 1-\zeta\pi^i\right) = 1$. Now the result follows by continuity of the p^n-th power norm-residue symbol. □

For a different proof of Lemma 10.4 see Remark 10.12.

Theorem 10.5 (Schinzel's theorem [62])**.** *Let K be a field, let l be a positive integer not divisible by the characteristic of K, and let w be the number of l-th roots of unity in K. Then, for $a \in K$, the Galois group of $X^l - a$ over K is abelian if and only if there exists $b \in K$ with $a^w = b^l$.*

Proof. For an elegant proof see [67] by Stevenhagen. □

Lemma 10.6. *Let p be a prime number and let F be a finite extension of the field $\mathbb{Q}_p$ of p-adic rationals. Let π be a prime element of F and let n be the maximal integer such that F contains a primitive p^n-th root of unity. Then the largest abelian extension of F contained in $F(\sqrt[p^{n+1}]{\pi})$ is $F(\sqrt[p^n]{\pi})/F$.*

Proof. By Kummer theory the field extension $F(\sqrt[p^n]{\pi})/F$ is abelian. We only need to show that the extension $F(\sqrt[p^{n+1}]{\pi})/F$ is not abelian, because its extension degree $[F(\sqrt[p^{n+1}]{\pi}) : F(\sqrt[p^n]{\pi})]$ equals the prime number p. Since we have $\pi^{p^n} \notin F^{*p^{n+1}}$, by Schinzel's theorem [Theorem 10.5] the extension $F(\sqrt[p^{n+1}]{\pi})/F$ is not abelian. □

Lemma 10.7. *Let p be a prime number, let F be a finite extension of the field $\mathbb{Q}_p$ of p-adic rationals, and let e be the normalized valuation on F of p. For each $i \in \mathbb{Z}_{>0}$ let $U^{(i)}$ be the i-th higher unit group of the ring of integers of F and let $\varrho(i) = \min\{pi, i+e\}$. Then for each $i \in \mathbb{Z}_{>0}$ the p-th power map $F^* \to F^*$, $a \mapsto a^p$, induces a group homomorphism*

$$U^{(i)}/U^{(i+1)} \to U^{(\varrho(i))}/U^{(\varrho(i)+1)}$$

with the following properties.

(a) *For $i \neq e/(p-1)$ it is a group isomorphism.*

(b) *For $i = e/(p-1)$ it either has kernel and cokernel of order p or is a group isomorphism, according as F does or does not contain a primitive p-th root of unity.*

Proof. See Lemma A.4 of Appendix in [48] by Milnor. □

Definition 10.8 (Distinguished unit)**.** Let p be a prime number and let F be a finite extension of the field $\mathbb{Q}_p$ of p-adic rationals containing a primitive p-th root of unity. Let e be the normalized valuation on F of p and for each $i \in \mathbb{Z}_{>0}$ let $U^{(i)}$ be the i-th higher unit group of the ring of integers of F. A *distinguished unit* of F is an element $\delta \in U^{(pe/(p-1))}$ such that its residue class

in $U^{(pe/(p-1))}/U^{((pe/(p-1))+1)}$ generates the cokernel of the p-th power group homomorphism

$$U^{(e/(p-1))}/U^{((e/(p-1))+1)} \to U^{(pe/(p-1))}/U^{((pe/(p-1))+1)},$$
$$u \cdot U^{((e/(p-1))+1)} \mapsto u^p \cdot U^{((pe/(p-1))+1)}.$$

Remark 10.9. Since each of the elements $1+c\lambda^p \in F^*$ in (b) of Theorem 3.95 and $\alpha^m \in F^*$ in Lemma 3.99 is not in F^{*p}, Lemma 3.97 implies that each of them is a distinguished unit of F.

Lemma 10.10. *Let p be a prime number, let F be a finite extension of the field $\mathbb{Q}_p$ of p-adic rationals containing a primitive p-th root of unity, let δ be a distinguished unit of F, and let n be the maximal integer such that F contains a primitive p^n-th root of unity. Then the extension $F(\sqrt[p]{\delta})/F$ is an unramified extension of degree p and the p^n-th power norm-residue symbol (π, δ) has order p^n.*

Proof. Since we have the equality $F^{*p} \cap U^{(1)} = U^{(1)^p}$, which follows from Theorem 3.37, Lemma 10.7 implies the equality

$$F^{*p} \cap U^{(ep/(p-1))} = (U^{(e/(p-1))})^p.$$

By definition of distinguished unit we get $\delta \notin F^{*p}$. Hence, the extension $F(\sqrt[p]{\delta})/F$ has degree p. Theorem 3.95 shows that it is unramified. By (b) in Theorem 3.80 the p-th power norm-residue symbol $(\pi, \delta)_{F,p}$ has order p. The statement about the p^n-th power norm-residue symbol follows from Theorem 3.76. □

Lemma 10.11. *Let the notation be as in* Theorem 10.2. *Then one has for $n = 0$ the equality*

$$U^{(1)} = H_\pi$$

and for $n > 0$ the equality

$$U^{(1)} = \delta^{\mathbb{Z}_p} \cdot H_\pi,$$

where δ is a distinguished unit of F.

Proof. Let e be the normalized valuation on F of p, define the set I to be

$$I = \{i \in \mathbb{Z}_{>0} \setminus p\mathbb{Z} : i < pe/(p-1)\},$$

and define the sub-$\mathbb{Z}_p$-module I_π of H_π to be

$$I_\pi = \prod_{\substack{i \in I \\ \zeta \in \mu_{q-1}}} (1 - \zeta\pi^i)^{\mathbb{Z}_p}.$$

We claim that the $\mathbb{Z}_p$-module I_π is a closed subgroup of $U^{(1)}$. By definition it is finitely generated and therefore is the continuous image of a product of finitely many copies of $\mathbb{Z}_p$, which is compact. Since the continuous image of a compact space is compact and a compact subspace of a Hausdorff space is closed, the claim follows.
Define the quotient group $\bar{U}$ to be

$$\bar{U} = \begin{cases} U^{(1)}/I_\pi & \text{if } n = 0, \\ U^{(1)}/(\delta^{\mathbb{Z}_p} \cdot I_\pi) & \text{if } n > 0. \end{cases}$$

Since I_π is contained in H_π, it will suffice to show that $\bar{U}$ is the trivial group. For each $i \in \mathbb{Z}_{>0}$ let $\bar{U}^{(i)}$ be the image of $U^{(i)}$ in $\bar{U}$ under the quotient map $U^{(1)} \to \bar{U}$. By definition of I_π for each $i \in I$ we have the equality $U^{(i)} \cdot I_\pi = U^{(i+1)} \cdot I_\pi$ and therefore for each $i \in I$ the quotient group $\bar{U}^{(i)}/\bar{U}^{(i+1)}$ is trivial. Since for $n > 0$ the image of δ in $\bar{U}$ is the identity element, Lemma 10.7 implies that for each $i \in \mathbb{Z}_{>0}$ the p-th power map induces a surjective group homomorphism

$$\bar{U}^{(i)}/\bar{U}^{(i+1)} \to \bar{U}^{(\varrho(i))}/\bar{U}^{(\varrho(i)+1)},$$

where $\varrho(i)$ is defined as in Lemma 10.7, and by induction on i it follows that for each $i \in \mathbb{Z}_{>0}$ the quotient group $\bar{U}^{(i)}/\bar{U}^{(i+1)}$ is trivial. Hence, for each $i \in \mathbb{Z}_{>0}$ we have the equality $\bar{U}^{(1)} = \bar{U}^{(i)}$. It is well-known [Section 1 of Chapter III in [50] by Neukirch] that the topological group $U^{(1)}$ is isomorphic to the projective limit

$$\varprojlim_{i \in \mathbb{Z}_{>0}} U^{(1)}/U^{(i)}.$$

Since $\bar{U}$ is a quotient group of $U^{(1)}$ by a closed subgroup, by Corollary 3 in Section 1.4 of Chapter V in [9] by Cassels and Fröhlich it is isomorphic to a projective limit of an inverse system of finite groups and we get a group isomorphism

$$\bar{U} \xrightarrow{\sim} \varprojlim_{i \in \mathbb{Z}_{>0}} \bar{U}^{(1)}/\bar{U}^{(i)},$$

that is, the group $\bar{U}$ is isomorphic to a projective limit of an inverse system of trivial groups. Hence, it is the trivial group. □

10.3 Proofs of the main results

Proof of Theorem 10.2. Let π be a prime element of F. By Lemma 10.4 the map

$$\begin{aligned} \varphi : U^{(1)}/H_\pi &\to \mu_{p^n}, \\ a \cdot H_\pi &\mapsto (\pi, a), \end{aligned}$$

is a well-defined group homomorphism. The surjectivity of φ is clear for $n = 0$ and follows from Lemma 10.10 for $n \geq 1$. Now we need to prove the injectivity of φ. Since μ_{p^n} is a finite group of order p^n, it will suffice to show that $U^{(1)}/H_\pi$ has order p^n.

For $n = 0$ the injectivity of φ follows from the equality $U^{(1)} = H_\pi$ in Lemma 10.11. Thus, for the rest of the proof we assume $n \geq 1$. Let δ be a distinguished unit of F. By Lemma 10.11 we have the equality $U^{(1)} = \delta^{\mathbb{Z}_p} \cdot H_\pi$. Hence, the map

$$\begin{aligned} \mathbb{Z}_p &\twoheadrightarrow U^{(1)}/H_\pi, \\ m &\mapsto \delta^m \cdot H_\pi, \end{aligned}$$

is a surjective group homomorphism. Its kernel is contained in $p^n\mathbb{Z}_p$, because composing this map with φ gives a surjective group homomorphism $\mathbb{Z}_p \twoheadrightarrow \mu_{p^n}$. We need to prove that its kernel equals $p^n\mathbb{Z}_p$.

Define the fields E and L to be $E = F(\sqrt[p^{n+1}]{\pi})$ and $L = F(\sqrt[p^n]{\pi})$. The extensions E/F and L/F are totally ramified extensions of degrees p^{n+1} and p^n, respectively. Let $\pi_E = \sqrt[p^{n+1}]{\pi}$ and $\pi_L = \sqrt[p^n]{\pi}$. They are prime elements of E and L, respectively. Let H_E be the group

$$H_E = \prod_{\substack{i \in \mathbb{Z}_{>0} \setminus p\mathbb{Z} \\ \zeta \in \mu_{q-1}}} (1 - \zeta\pi_E^i)^{\mathbb{Z}_p}$$

and similarly let H_L be the group

$$H_L = \prod_{\substack{i \in \mathbb{Z}_{>0} \setminus p\mathbb{Z} \\ \zeta \in \mu_{q-1}}} (1 - \zeta\pi_L^i)^{\mathbb{Z}_p}.$$

Since the extension $F(\sqrt[p]{\delta})/F$ is unramified, it is linearly disjoint from E/F and from L/F. Hence, we have both $\delta \notin E^{*p}$ and $\delta \notin L^{*p}$. The straightforward computations of the normalized valuations on E and on L of $\delta - 1$ shows that δ is a distinguished unit both of E and of L. Hence, the same argument used for the local field F gives the equalities

$$U_E^{(1)} = \delta^{\mathbb{Z}_p} \cdot H_E \quad \text{and} \quad U_L^{(1)} = \delta^{\mathbb{Z}_p} \cdot H_L,$$

where $U_E^{(1)}$ and $U_L^{(1)}$ are the first higher unit groups of the rings of integers of E and of L, respectively.

Let $\mathrm{N}_{L/F} : L \to F$ be the norm map from L to F, let $\zeta \in \mu_{q-1}$, let $i \in \mathbb{Z}_{>0} \setminus p\mathbb{Z}$, and let $f(X) = X^{p^n} - \zeta^{p^n}\pi^i$. Then we have

$$\mathrm{N}_{L/F}(1 - \zeta\pi_L^i) = f(1) = 1 - \zeta^{p^n}\pi^i \in H_\pi.$$

Since the p^n-th power map $\mu_{q-1} \to \mu_{q-1}$, $\zeta \mapsto \zeta^{p^n}$, is a group isomorphism, we get $\mathrm{N}_{L/F} H_L = H_\pi$. Similarly, we get $\mathrm{N}_{E/F} H_E = H_\pi$, where $\mathrm{N}_{E/F} : E \to F$ is the norm map from E to F. The equalities

$$\mathrm{N}_{E/F} U_E^{(1)} = \delta^{p^{n+1}\mathbb{Z}_p} \cdot H_\pi \quad \text{and} \quad \mathrm{N}_{L/F} U_L^{(1)} = \delta^{p^n\mathbb{Z}_p} \cdot H_\pi$$

follow. Since by Lemma 10.6 the extension L/F is the largest abelian extension of F contained in E, Corollary 3.66 gives the equality

$$\delta^{p^{n+1}\mathbb{Z}_p} \cdot H_\pi = \delta^{p^n\mathbb{Z}_p} \cdot H_\pi.$$

Hence, we can write $\delta^{p^n} = \delta^{p^{n+1}m} \cdot h$ with $m \in \mathbb{Z}_p$ and $h \in H_\pi$. We get $\delta^{p^n(1-pm)} \in H_\pi$. From $1 - pm \in \mathbb{Z}_p^*$ we deduce $\delta^{p^n} \in H_\pi$. □

Remark 10.12. As a consequence of the equality $\mathrm{N}_{L/F} H_L = H_\pi$ shown in the proof of Theorem 10.2 we obtain another proof of Lemma 10.4 as follows. This equality implies that the group H_π consists of norms from $L = F(\sqrt[p^n]{\pi})$ to F. Using Lemma 3.72 and the antisymmetry of the norm-residue symbol we get the inclusion $H_\pi \subset \pi^\perp$ in Lemma 10.4.

Proof of Theorem 10.1. This follows from Theorem 10.2. □

CHAPTER 11

Quadratic characters

11.1 Main result

The Dedekind zeta function of a number field K is generally denoted by $\zeta_K(s)$. Let $\mathrm{L}_K : K^*/K^{*2} \to \mathrm{Mer}(\mathbb{C})$ be the function from the group K^*/K^{*2} to the set of meromorphic functions $\mathrm{Mer}(\mathbb{C})$ from $\mathbb{C}$ to $\mathbb{P}^1(\mathbb{C})$ defined by

$$\mathrm{L}_K(aK^{*2})(s) = \begin{cases} \zeta_{K(\sqrt{a})}(s)/\zeta_K(s) & \text{if } a \notin K^{*2}, \\ \zeta_K(s) & \text{if } a \in K^{*2}. \end{cases}$$

Our main result is the following theorem.

Theorem 11.1. *Let K and K' be number fields. Then the natural map from the set of field isomorphisms $K \to K'$ to the set of group isomorphisms $\beta : K^*/K^{*2} \to K'^*/K'^{*2}$ with the property that $\mathrm{L}_{K'} \circ \beta = \mathrm{L}_K$ is bijective.*

Proof. See Section 11.5. □

Theorem 11.1 implies the following known result, which is also a corollary of Theorem 11.3 by Pintonello.

Corollary 11.2. *Let K and K' be number fields. If there exists a group isomorphism $\beta : K^*/K^{*2} \to K'^*/K'^{*2}$ with the property that $\mathrm{L}_{K'} \circ \beta = \mathrm{L}_K$, then K and K' are isomorphic.*

Proof. This follows from Theorem 11.1. □

11.2 Introduction

Given a number field K, we denote its absolute Galois group by $\mathcal{G}_K$. Endowed with the Krull topology, the group $\mathcal{G}_K$ is a topological group. We will write $\mathrm{X}(K)$ for the group $\mathrm{Hom}_{\mathrm{cont}}(\mathcal{G}_K, \{\pm 1\})$ of continuous homomorphisms from $\mathcal{G}_K$ to the group $\{\pm 1\}$, which are also called quadratic characters of K.

It is more common to define an L-series for each element of the group $\mathrm{X}(K)$ of quadratic characters of K rather than of the group K^*/K^{*2}. This is not really different from what we do here, because, by Kummer theory, there is a group isomorphism

$$\begin{aligned} K^*/K^{*2} &\xrightarrow{\sim} \mathrm{X}(K), \\ aK^{*2} &\mapsto (\sigma \mapsto \sigma(\sqrt{a})/\sqrt{a}). \end{aligned}$$

This isomorphism provides a natural way of defining L-series on the group of quadratic characters as soon as they are defined on K^*/K^{*2}. In our case this agrees with the usual definition.

For every number field one can consider certain topological objects, such as adele rings and absolute Galois groups, and certain analytic objects, such as Dedekind zeta functions or, more generally, L-series. It is natural to ask how much information is contained in these objects. For instance, does the Dedekind zeta function of a number field determine the number field up to isomorphism? In 1926 Gaßmann showed that there exist non-isomorphic number fields with the same Dedekind zeta function [19]. Not even an isomorphism (as topological rings) of the adele rings of two number fields implies that the number fields are isomorphic [30], nor an isomorphism (as topological groups) of the Galois groups of their maximal abelian extensions [52].

In 1976 Uchida proved that the existence of an isomorphism of the absolute Galois groups of two number fields is a sufficient condition for the two number fields to be isomorphic [71]. Another positive result has been recently found by Cornelissen and Marcolli [12], using the map $\mathcal{L}_K : \mathrm{Hom}_{\mathrm{cont}}(\mathcal{G}_K, \mathbb{C}^*) \to \mathrm{Mer}(\mathbb{C})$ that sends a character to its L-series; so the restriction $\mathcal{L}_K|_{\mathrm{X}(K)}$ of $\mathcal{L}_K$ is the same as L_K. They have proved that if there is a group isomorphism $\beta : \mathrm{Hom}_{\mathrm{cont}}(\mathcal{G}_K, \mathbb{C}^*) \to \mathrm{Hom}_{\mathrm{cont}}(\mathcal{G}_{K'}, \mathbb{C}^*)$ between the groups of abelian characters of two absolute Galois groups of two number fields K and K' with the property that $\mathcal{L}_{K'} \circ \beta = \mathcal{L}_K$, then the two number fields are isomorphic. In the same article de Smit proved that given a number field K for every integer $k \geq 3$ there is a abelian character $\chi \in \mathrm{Hom}_{\mathrm{cont}}(\mathcal{G}_K, \mathbb{C}^*)$ of order k such that every number field K' for which there is a character $\chi' \in \mathrm{Hom}_{\mathrm{cont}}(\mathcal{G}_{K'}, \mathbb{C}^*)$ with $\mathcal{L}_{K'}(\chi') = \mathcal{L}_K(\chi)$ is isomorphic to K. For $k = 2$ there is the following theorem by Pintonello.

Theorem 11.3 (Pintonello [54])**.** *Let K be a number field. Then there are two characters $\chi_1, \chi_2 \in \mathrm{X}(K)$ such that every number field K' for which*

there are two characters $\chi_1', \chi_2' \in \mathrm{X}(K')$ *with* $\mathcal{L}_{K'}(\chi_1') = \mathcal{L}_K(\chi_1)$ *and* $\mathcal{L}_{K'}(\chi_2') = \mathcal{L}_K(\chi_2)$ *is isomorphic to* K*.*

Given a field isomorphism $\sigma : K \to K'$, there is a natural associated group isomorphism $\beta : \mathrm{X}(K) \to \mathrm{X}(K')$. Are all bijective maps β with $\mathcal{L}_{K'} \circ \beta = \mathcal{L}_K$ that are also group isomorphisms obtained in this way? The affirmative answer is Theorem 11.1. Each of Theorem 11.3 by Pintonello and Theorem 11.1 implies and generalizes the result by Cornelissen and Marcolli.

11.3 L-series

In this section we recall some definitions and results about L-series. We refer the reader to Chapters VIII and XI in the book [31] by Lang for more details and proofs.

Let K be a number field. We will give a formula for the function L_K from the group K^*/K^{*2} to the set of meromorphic functions $\mathrm{Mer}(\mathbb{C})$ from $\mathbb{C}$ to $\mathbb{P}^1(\mathbb{C})$.

Let $\mathfrak{P}$ be a finite prime of K above a rational prime p and let $f(\mathfrak{P}/p)$ be the inertia degree of $\mathfrak{P}$ over p. We denote the completion of K at $\mathfrak{P}$ by $K_\mathfrak{P}$ and the ring of integers of $K_\mathfrak{P}$ by $\mathcal{O}_\mathfrak{P}$. We define a function $\epsilon_\mathfrak{P}$ from $K_\mathfrak{P}^*/K_\mathfrak{P}^{*2}$ to the set of integers $\{-1, 1, 0\}$ by setting for every $aK_\mathfrak{P}^{*2}$ in $K_\mathfrak{P}^*/K_\mathfrak{P}^{*2}$

$$\epsilon_\mathfrak{P}(aK_\mathfrak{P}^{*2}) = \begin{cases} -1 & \text{if } K_\mathfrak{P}(\sqrt{a})/K_\mathfrak{P} \text{ is an unramified extension of degree 2,} \\ 1 & \text{if } K_\mathfrak{P}(\sqrt{a})/K_\mathfrak{P} \text{ is the trivial extension,} \\ 0 & \text{if } K_\mathfrak{P}(\sqrt{a})/K_\mathfrak{P} \text{ is ramified.} \end{cases}$$

Note that if p is odd we have $\epsilon_\mathfrak{P}(aK_\mathfrak{P}^{*2}) = 0$ if and only if $2 \nmid \mathrm{ord}_\mathfrak{P}(a)$ or, equivalently, if and only if $aK_\mathfrak{P}^{*2} \notin \mathcal{O}_\mathfrak{P}^*/\mathcal{O}_\mathfrak{P}^{*2}$, where we consider $\mathcal{O}_\mathfrak{P}^*/\mathcal{O}_\mathfrak{P}^{*2}$ as a subgroup of $K_\mathfrak{P}^*/K_\mathfrak{P}^{*2}$.

Let $\lambda_\mathfrak{P} : K_\mathfrak{P}^*/K_\mathfrak{P}^{*2} \to \mathbb{C}[T]$ be the map from $K_\mathfrak{P}^*/K_\mathfrak{P}^{*2}$ to the polynomial ring over $\mathbb{C}$ in one variable T given by

$$\lambda_\mathfrak{P}(aK_\mathfrak{P}^{*2}) = 1 - \epsilon_\mathfrak{P}(aK_\mathfrak{P}^{*2})T^{f(\mathfrak{P}/p)}.$$

For every $aK_\mathfrak{P}^{*2} \in K_\mathfrak{P}^*/K_\mathfrak{P}^{*2}$ we define the meromorphic function

$$\mathrm{L}_\mathfrak{P}(aK_\mathfrak{P}^{*2})(s) = \frac{1}{\lambda_\mathfrak{P}(aK_\mathfrak{P}^{*2})(p^{-s})}, \quad s \in \mathbb{C}.$$

It will be the Euler factor at $\mathfrak{P}$ of the L-function of every element of K^*/K^{*2} mapping to $aK_\mathfrak{P}^{*2}$ under the homomorphism $K^*/K^{*2} \to K_\mathfrak{P}^*/K_\mathfrak{P}^{*2}$ induced by the natural inclusion $K \hookrightarrow K_\mathfrak{P}$.

For every $aK^{*2} \in K^*/K^{*2}$ we get its L-function as an Euler product

$$\mathrm{L}_K(aK^{*2})(s) = \prod_{\mathfrak{P}} \mathrm{L}_{\mathfrak{P}}(aK_{\mathfrak{P}}^{*2})(s), \quad s \in \mathbb{C},$$

where the product ranges over all finite primes of K. This product converges absolutely and uniformly for $\mathrm{Re}(s) \geq 1+\delta$ with $\delta > 0$, therefore it is an analytic function in s. It can also be proved that it admits an analytic continuation to a meromorphic function on $\mathbb{C}$. A proof can be found in Tate's thesis, which is Chapter XV in [9].

It is sometimes useful to group together prime ideals above the same rational prime p. Therefore, we define the map $\lambda_p : K^*/K^{*2} \to \mathbb{C}[T]$ by

$$\lambda_p(aK^{*2}) = \prod_{\mathfrak{P}|p} \lambda_{\mathfrak{P}}(aK_{\mathfrak{P}}^{*2}).$$

Then, for every $aK^{*2} \in K^*/K^{*2}$ we have

$$\mathrm{L}_K(aK^{*2})(s) = \prod_{p \text{ prime}} \frac{1}{\lambda_p(aK^{*2})(p^{-s})}.$$

The p-th factor on the right-hand side is called the Euler p-factor. Note that the order of vanishing at 1 of $\lambda_p(aK^{*2})$ is equal to the number of primes $\mathfrak{P}$ above p for which a is a square in $K_{\mathfrak{P}}$ and that the degree of $\lambda_p(aK^{*2})$ is equal to the sum of the inertia degrees $f(\mathfrak{P}/p)$ of the primes $\mathfrak{P}$ for which $K_{\mathfrak{P}}(\sqrt{a})/K_{\mathfrak{P}}$ is unramified.

Lemma 11.4. *Let K be a number field and let β be an automorphism of the group K^*/K^{*2}. Then $\mathrm{L}_K \circ \beta = \mathrm{L}_K$ if and only if for all rational primes p and for all $a \in K^*$ one has $\lambda_p(\beta(aK^{*2})) = \lambda_p(aK^{*2})$.*

Proof. Fix an element a in K^*. Since two L-functions are equal if and only if they have the same Euler p-factors, we have $\mathrm{L}_K(\beta(aK^{*2})) = \mathrm{L}_K(aK^{*2})$ if and only if $\lambda_p(\beta(aK^{*2})) = \lambda_p(aK^{*2})$ for all rational primes p. By considering all a in K^* we conclude the proof. □

11.4 Lemmas

In the proof of Theorem 11.1 we will use many lemmas. Some of them may be interesting in themselves and are presented in this section. The first one is an easy case of a theorem in coding theory. Here we do not state the general theorem and we refer to [43] and [78] for more information.

Lemma 11.5. *Let V be a finite-dimensional $\mathbb{F}_2$-vector space of positive dimension n, let $\{e_1, \ldots, e_n\}$ be a basis of V, and let w be the Hamming weight, i.e. the function from V to $\mathbb{Z}_{\geq 0}$ that maps each vector of V to the number of its nonzero components in the basis $\{e_1, \ldots, e_n\}$. Then the natural map from the group of permutations of the basis $\{e_1, \ldots, e_n\}$ to the group of automorphisms of V respecting the Hamming weight is a bijection.*

Proof. Since the elements of the basis $\{e_1, \ldots, e_n\}$ are exactly all vectors of Hamming weight equal to 1, every automorphism of V respecting the Hamming weight has to permute this basis. On the other hand, it is immediately clear from the definition of the Hamming weight that every permutation of the basis $\{e_1, \ldots, e_n\}$ induces an automorphism of V respecting the Hamming weight. □

Lemma 11.6. *Let K be a number field and let A be a finite index subgroup of $K^*/{K^*}^2$. Then for all but finitely many rational primes p the natural map*

$$A \to \prod_{\mathfrak{P}|p} K_{\mathfrak{P}}^*/{K_{\mathfrak{P}}^*}^2,$$

where $\mathfrak{P}$ ranges over all primes of K above p, is surjective.

Proof. Let S be a finite set of rational primes such that for every prime $p \in S$ the group homomorphism

$$A \to \prod_{\mathfrak{P}|p} K_{\mathfrak{P}}^*/{K_{\mathfrak{P}}^*}^2$$

is not surjective. Since by the weak approximation theorem the group homomorphism

$$\phi_S : K^*/{K^*}^2 \twoheadrightarrow \prod_{p \in S} \prod_{\mathfrak{P}|p} K_{\mathfrak{P}}^*/{K_{\mathfrak{P}}^*}^2$$

is surjective, it induces a surjective group homomorphism

$$(K^*/{K^*}^2)/A \twoheadrightarrow \left(\prod_{p \in S} \prod_{\mathfrak{P}|p} K_{\mathfrak{P}}^*/{K_{\mathfrak{P}}^*}^2 \right) / \phi_S(A).$$

By construction the cardinality of the group on the right is at least $2^{\#S}$. The surjectivity of the group homomorphism gives an upper bound on the cardinality of S, namely $\#S \leq \log_2[K^*/{K^*}^2 : A]$. The statement of the lemma follows easily. □

Lemma 11.7. *Let K be a number field, let p be a rational prime, and let β be an automorphism of the group $K^*/{K^*}^2$ with the property that $\mathrm{L}_K \circ \beta = \mathrm{L}_K$. Then there exists a unique automorphism β_p of $\prod_{\mathfrak{P}|p} K_\mathfrak{P}^*/{K_\mathfrak{P}^*}^2$ such that the diagram*

$$\begin{array}{ccc} K^*/{K^*}^2 & \longrightarrow & \prod_{\mathfrak{P}|p} K_\mathfrak{P}^*/{K_\mathfrak{P}^*}^2 \\ {\scriptstyle\beta}\downarrow & & {\scriptstyle\beta_p}\downarrow \\ K^*/{K^*}^2 & \longrightarrow & \prod_{\mathfrak{P}|p} K_\mathfrak{P}^*/{K_\mathfrak{P}^*}^2 \end{array}$$

commutes.

Proof. By the weak approximation theorem for every rational prime p the natural map

$$K^*/{K^*}^2 \twoheadrightarrow \prod_{\mathfrak{P}|p} K_\mathfrak{P}^*/{K_\mathfrak{P}^*}^2$$

is surjective. Elements of the kernel of this map are characterized by the fact that the function λ_p maps them to polynomials divisible by $\prod_{\mathfrak{P}|p}(1-T)$. Since by Lemma 11.4 these polynomials are preserved by β, a unique automorphism β_p is induced on the group $\prod_{\mathfrak{P}|p} K_\mathfrak{P}^*/{K_\mathfrak{P}^*}^2$ and it makes the diagram commute. □

Definition 11.8 (Local quadratic symbol and quadratic symbol)**.** Let $\mathcal{O}$ be the ring of integers of a number field K and let $\mathfrak{P}$ be a nonzero prime ideal of $\mathcal{O}$ not dividing 2. Let $K_\mathfrak{P}$ be the completion of K at $\mathfrak{P}$ and let $\mathcal{O}_\mathfrak{P}$ be the ring of integers of $K_\mathfrak{P}$. The *local quadratic symbol* $\left(\frac{\cdot}{\mathfrak{P}}\right)$ is the unique group isomorphism

$$\left(\frac{\cdot}{\mathfrak{P}}\right) : \mathcal{O}_\mathfrak{P}^*/{\mathcal{O}_\mathfrak{P}^*}^2 \xrightarrow{\sim} \{\pm 1\}.$$

For every $a \in K^*$ in the inverse image of $\mathcal{O}_\mathfrak{P}^*/{\mathcal{O}_\mathfrak{P}^*}^2$ under the map $K^* \to K_\mathfrak{P}^*/{K_\mathfrak{P}^*}^2$, the *quadratic symbol* $\left(\frac{a}{\mathfrak{P}}\right)$ is defined by composing the map $K^* \to K_\mathfrak{P}^*/{K_\mathfrak{P}^*}^2$ with the local quadratic symbol.

Remark 11.9. In particular, the local quadratic symbol is defined for all elements of K with even valuation at $\mathfrak{P}$.

Remark 11.10. Definition 11.8 of the quadratic symbol extends the following commoner one: for every $a \in K^*$ with $\mathrm{ord}_\mathfrak{P}(a) = 0$, the quadratic symbol $\left(\frac{a}{\mathfrak{P}}\right)$ is defined by

$$\left(\frac{a}{\mathfrak{P}}\right) = \begin{cases} -1 \text{ if } a \text{ is not a square in } \mathcal{O}/\mathfrak{P}, \\ +1 \text{ if } a \text{ is a square in } \mathcal{O}/\mathfrak{P}. \end{cases}$$

Lemma 11.11. *Let K be a number field, let p be an odd rational prime, and let β be an automorphism of the group $K^*/{K^*}^2$ with the property that $\mathrm{L}_K \circ \beta = \mathrm{L}_K$. Then the induced automorphism β_p of $\prod_{\mathfrak{P}|p} K_\mathfrak{P}^*/{K_\mathfrak{P}^*}^2$ permutes the set of subgroups $\{\mathcal{O}_\mathfrak{P}^*/{\mathcal{O}_\mathfrak{P}^*}^2 : \mathfrak{P} \mid p\}$.*

Proof. For all odd rational primes the elements of the subgroup $\prod_{\mathfrak{P}|p} \mathcal{O}_\mathfrak{P}^*/{\mathcal{O}_\mathfrak{P}^*}^2$ of $\prod_{\mathfrak{P}|p} K_\mathfrak{P}^*/{K_\mathfrak{P}^*}^2$ are characterized by the fact that the function λ_p maps them to polynomials of maximal possible degree, that is, of degree $\sum_{\mathfrak{P}|p} f(\mathfrak{P}/p)$. Hence, the group $\prod_{\mathfrak{P}|p} \mathcal{O}_\mathfrak{P}^*/{\mathcal{O}_\mathfrak{P}^*}^2$ is invariant under β_p. Since for each prime $\mathfrak{P}$ above p the group $\mathcal{O}_\mathfrak{P}^*/{\mathcal{O}_\mathfrak{P}^*}^2$ has only two elements, we can think of the subgroup $\prod_{\mathfrak{P}|p} \mathcal{O}_\mathfrak{P}^*/{\mathcal{O}_\mathfrak{P}^*}^2$ of $\prod_{\mathfrak{P}|p} K_\mathfrak{P}^*/{K_\mathfrak{P}^*}^2$ as a vector space over $\mathbb{F}_2$ with a basis given by the nontrivial elements in the groups $\{\mathcal{O}_\mathfrak{P}^*/{\mathcal{O}_\mathfrak{P}^*}^2 : \mathfrak{P} \mid p\}$. The Hamming weight is also given by the difference between the number of primes $\mathfrak{P}$ above p and the order of vanishing at 1 of the polynomials obtained by the function λ_p. Thus, the automorphism β respects the Hamming weight and by Lemma 11.5 it permutes the basis, i.e., it acts on the group $\prod_{\mathfrak{P}|p} \mathcal{O}_\mathfrak{P}^*/{\mathcal{O}_\mathfrak{P}^*}^2$ as a permutation of the set of primes above p. □

Remark 11.12. By Lemma 11.11 the automorphism β acts on the set of primes above an odd rational prime p. We denote by $\beta(\mathfrak{P})$ the image of a prime $\mathfrak{P}$ above p under this action. Hence, for all elements $a \in K^*$ with even valuation at all primes above p we have

$$\left(\frac{a}{\mathfrak{P}}\right) = \left(\frac{\beta(a)}{\beta(\mathfrak{P})}\right).$$

Lemma 11.13. *Let β be an automorphism of the group $K^*/{K^*}^2$ of a number field K with the property that $\mathrm{L}_K \circ \beta = \mathrm{L}_K$ and let A be a finite index subgroup of $K^*/{K^*}^2$. If β is the identity on A, then it is the identity on $K^*/{K^*}^2$.*

Proof. Lemma 11.6 states that for all but finitely many rational primes p the natural map

$$\phi_p : A \to \prod_{\mathfrak{P}|p} K_\mathfrak{P}^*/{K_\mathfrak{P}^*}^2$$

is surjective. In this case, by Lemma 11.7 we know that the automorphism β_p induced by β on the latter group is trivial and therefore for every a in $K^*/{K^*}^2$ the element $a/\beta(a)$ is in the kernel of ϕ_p. Since this is true for all but finitely many rational primes p, by a corollary of the global cyclic norm index result in Section 5 of Chapter IX in [31] the quotient $a/\beta(a)$ is a square in $K^*/{K^*}^2$. Thus β is the identity on $K^*/{K^*}^2$. □

Lemma 11.14. *Let R be a ring, let G be a finite group, and let M be a nonzero free $R[G]$-module. Let H be a subgroup of G, let M^H be the subgroup of H-invariants of M, that is, the subgroup $\{m \in M : \forall h \in H : hm = m\}$, and let σ be an element of G. Then one has $\sigma(M^H) = M^H$ if and only if $H = \sigma H \sigma^{-1}$.*

Proof. Firstly, suppose we have a subgroup J of G such that $M^H \subseteq M^J$. We want to prove the inclusion $J \subseteq H$. Let τ be an element of J and observe the chain of inclusions

$$(\tau - 1)(\sum_{h \in H} h)M \subseteq (\tau - 1)M^H \subseteq (\tau - 1)M^J = \{0\}.$$

Since any nonzero free module over any ring is faithful, the element $(\tau - 1)(\sum_{h \in H} h)$ of $R[G]$ is 0. This implies the equality $\tau H = H$, that is, the element τ is in H. Thus, the inclusion $J \subseteq H$ is proved.

Now note the identity $\sigma(M^H) = M^{\sigma H \sigma^{-1}}$. From what we have just shown it follows that we have $\sigma(M^H) = M^H$ if and only if $H = \sigma H \sigma^{-1}$. □

11.5 Proof of the main theorem

This section is entirely devoted to the proof of Theorem 11.1.

Proof of Theorem 11.1. By Theorem 11.3 the set of field isomorphisms $K \to K'$ and the set of group isomorphisms $\beta : K^*/K^{*2} \to K'^*/K'^{*2}$ with the property that $\mathrm{L}_{K'} \circ \beta = \mathrm{L}_K$ are both empty when K is not isomorphic to K'. Hence, we may assume $K = K'$.

Let F be the Galois closure of K over $\mathbb{Q}$ in an algebraic closure of K and let G be the Galois group $\mathrm{Gal}(F/\mathbb{Q})$. Let p be a rational prime that splits completely in F, let $\mathfrak{P}$ be a prime of K above p, and let $\mathfrak{Q}$ be a prime of F above $\mathfrak{P}$. We remark that the diagram of fields with natural inclusions

$$\begin{array}{ccc} K & \longrightarrow & F \\ \downarrow & & \downarrow \\ K_{\mathfrak{P}} & \xrightarrow{\sim} & F_{\mathfrak{Q}} \end{array}$$

commutes and the bottom horizontal arrow is an isomorphism. Moreover, the induced homomorphism $K^*/K^{*2} \to F^*/F^{*2}$ has finite kernel $(K^* \cap F^{*2})/K^{*2}$, because by Kummer theory this kernel corresponds to a subextension of the finite extension F/K. We will denote the image in F^*/F^{*2} of an element a in K^*/K^{*2} by $\overline{a}$.

Let W be a subgroup of K^* containing $K^* \cap F^{*2}$ such that the quotient group $W/(K^* \cap F^{*2})$ is finite. Let V be a finite subgroup of F^*/F^{*2} containing, for every x in the image of $(W/K^{*2}) \cup \beta(W/K^{*2})$ under the map $K^*/K^{*2} \to F^*/F^{*2}$, all elements in the orbit of x under the action of G. Denote the group $\mathrm{Hom}(V, \{\pm 1\})$ by $\widehat{V}$ and the field $F(\sqrt{V})$ by L. By Kummer theory there is an isomorphism

$$\begin{aligned} \mathrm{Gal}(L/F) &\cong \widehat{V}, \\ \tau &\mapsto (v \mapsto \sqrt{v}^{\tau-1}). \end{aligned}$$

Now we introduce the set P of primes that we use in the next two lemmas. The set P is the set of all primes of F above odd primes of $\mathbb{Q}$ that split completely in F and are unramified in L.

Lemma 11.15. *There is a surjective map*

$$\begin{aligned} P &\twoheadrightarrow \widehat{V}, \\ \mathfrak{Q} &\mapsto \left(\frac{\cdot}{\mathfrak{Q}}\right), \end{aligned}$$

sending a prime $\mathfrak{Q}$ in P to the corresponding quadratic symbol.

Proof. Firstly, we show that the map is well-defined. With each prime $\mathfrak{Q}$ in P we associate the corresponding quadratic symbol with domain the set of elements in F^* with even valuation at $\mathfrak{Q}$. Since $\mathfrak{Q}$ is unramified in L, these elements represent all elements of the group V. Hence, the quadratic symbol may be considered as an element in $\widehat{V}$.

Since the set P has density 1 in the set of primes of F, by Chebotarëv's Density Theorem each element of the Galois group $\mathrm{Gal}(L/F)$ is the Frobenius symbol of infinitely many primes in P. This proves the surjectivity of the map in the statement of the lemma. □

Lemma 11.16. *Let $\mathfrak{Q}$ be a prime in P. Then there exists $\tau \in G$ such that for all $w \in W$*

$$\left(\frac{\beta(w)}{\mathfrak{Q}}\right) = \left(\frac{\tau(w)}{\mathfrak{Q}}\right).$$

Proof. Let $\mathfrak{P}$ be the prime of K below the prime $\mathfrak{Q}$ in P and let p be the rational prime below $\mathfrak{P}$. Every element of $W/(K^* \cap F^{*2})$ can be represented by an element of K^* with even valuation at all primes of K above p, because p is unramified in L. Since $\mathfrak{Q}$ is a prime of F above a prime of K that splits completely in F, the quadratic symbols of $\mathfrak{Q}$ and $\mathfrak{P}$ give rise to the same function from W to $\{\pm 1\}$. The prime $\beta^{-1}(\mathfrak{P})$ also lies above p, because by Lemma 11.11 the automorphism β acts on the set of primes above p. Hence,

both $\mathfrak{P}$ and $\beta^{-1}(\mathfrak{P})$ split completely in F. Since all primes of F above p are conjugate, there exists $\tau \in G$ such that $\tau^{-1}(\mathfrak{Q})$ is above $\beta^{-1}(\mathfrak{P})$. For such $\tau \in G$ we have, for all $w \in W$,

$$\left(\frac{\beta(w)}{\mathfrak{Q}}\right) = \left(\frac{\beta(w)}{\mathfrak{P}}\right) = \left(\frac{w}{\beta^{-1}(\mathfrak{P})}\right) = \left(\frac{w}{\tau^{-1}(\mathfrak{Q})}\right) = \left(\frac{\tau(w)}{\mathfrak{Q}}\right),$$

where the second equality comes from Remark 11.12. □

Lemma 11.17. *There exists $\sigma \in G$ such that*

$$\#\langle \sigma(\overline{w})/\overline{\beta(w)} : w \in W/K^{*2}\rangle \leq \#G.$$

Proof. Define, for each $\tau \in G$, the group

$$H_\tau = \{\chi \in \widehat{V} : \forall w \in W/K^{*2} : \chi(\tau(\overline{w})) = \chi(\overline{\beta(w)})\}.$$

By Lemma 11.15 every $\chi \in \widehat{V}$ is given by the quadratic symbol of a prime $\mathfrak{Q}$ in P and by Lemma 11.16 every such symbol is contained in at least one of the groups H_τ. Hence, we have

$$\bigcup_{\tau \in G} H_\tau = \widehat{V}.$$

Since $\widehat{V}$ is the union of $\#G$ sets, there exists $\sigma \in G$ such that $\#H_\sigma \geq \widehat{V}/\#G$ or, equivalently,

$$[\widehat{V} : H_\sigma] \leq \#G.$$

Considering the nondegenerate bilinear map $\widehat{V} \times V \to \{\pm 1\}$ that sends (χ, v) to $\chi(v)$, we also note that

$$[\widehat{V} : H_\sigma] = \#\langle \sigma(\overline{w})/\overline{\beta(w)} : w \in W/K^{*2}\rangle,$$

because H_σ is the annihilator in $\widehat{V}$ of $\langle \sigma(\overline{w})/\overline{\beta(w)} : w \in W/K^{*2}\rangle$. This concludes the proof. □

Let $\{W_i\}_{i \in \mathbb{Z}_{\geq 1}}$ be an increasing sequence of subgroups of K^* as W above such that $\bigcup_i W_i = K^*$. We have proved in Lemma 11.17 that for every W_i there exists $\sigma \in G$ such that

$$\#\langle \sigma(\overline{w})/\overline{\beta(w)} : w \in W_i/K^{*2}\rangle \leq \#G.$$

Since G is finite, we may restrict to a subsequence and suppose that all σ's are equal. This subsequence is still an increasing sequence of subgroups of K^* whose union is K^*. Hence, we have $\sigma \in G$ such that

$$\#\langle \sigma(\overline{a})/\overline{\beta(a)} : a \in K^*/K^{*2}\rangle \leq \#G.$$

The group homomorphism

$$\begin{aligned} K^*/{K^*}^2 &\to F^*/{F^*}^2 \\ a &\mapsto \sigma(\overline{a})/\overline{\beta(a)} \end{aligned}$$

has finite image and therefore the kernel $U = \{a \in K^*/{K^*}^2 : \sigma(\overline{a}) = \overline{\beta(a)}\}$ is a finite index subgroup of $K^*/{K^*}^2$. By Lemma 11.6 there is a rational prime p that splits completely in F such that the map $U \to \prod_{\mathfrak{P}|p} K_{\mathfrak{P}}^*/{K_{\mathfrak{P}}^*}^2$, where the product ranges over primes of K, is surjective. Hence each element in $\prod_{\mathfrak{P}|p} \mathcal{O}_{\mathfrak{P}}^*/{\mathcal{O}_{\mathfrak{P}}^*}^2$ is the image of an element of U. The group $\prod_{\mathfrak{P}|p} \mathcal{O}_{\mathfrak{P}}^*/{\mathcal{O}_{\mathfrak{P}}^*}^2$ is a subgroup of $\prod_{\mathfrak{Q}|p} \mathcal{O}_{\mathfrak{Q}}^*/{\mathcal{O}_{\mathfrak{Q}}^*}^2$, where the last product ranges over primes of F. The latter group is a free $\mathbb{F}_2[G]$-module of rank 1 and the former group is the subgroup of $\mathrm{Gal}(F/K)$-invariants. Since for all $u \in U$ we have $\sigma(\overline{u}) = \overline{\beta(u)}$, the action of σ on $\prod_{\mathfrak{Q}|p} \mathcal{O}_{\mathfrak{Q}}^*/{\mathcal{O}_{\mathfrak{Q}}^*}^2$ maps $\prod_{\mathfrak{P}|p} \mathcal{O}_{\mathfrak{P}}^*/{\mathcal{O}_{\mathfrak{P}}^*}^2$ to itself. By Lemma 11.14 we get $\mathrm{Gal}(F/K) = \sigma\,\mathrm{Gal}(F/K)\sigma^{-1} = \mathrm{Gal}(F/\sigma(K))$. Hence, we have $\sigma(K) = K$, that is, the automorphism σ of F restricted to K is an automorphism of K. Thus, for every $u \in U$ we have $\overline{\sigma(u)} = \sigma(\overline{u}) = \overline{\beta(u)}$. This implies that every quotient $\sigma(u)/\beta(u)$ is contained in kernel of the group homomorphism $K^*/{K^*}^2 \to F^*/{F^*}^2$, that is, in the finite group $(K^* \cap {F^*}^2)/{K^*}^2$.

We have shown that the group homomorphism

$$\begin{aligned} K^*/{K^*}^2 &\to K^*/{K^*}^2 \\ a &\mapsto \sigma(a)/\beta(a) \end{aligned}$$

has finite image on U. Since U is a finite index subgroup of $K^*/{K^*}^2$, the group homomorphism itself has finite image. Thus, the kernel

$$\{a \in K^*/{K^*}^2 : \sigma^{-1}(\beta(a)) = a\}$$

is a finite index subgroup of $K^*/{K^*}^2$. By Lemma 11.13 applied to $\sigma^{-1}\beta$ we deduce that $\beta(a) = \sigma(a)$ for all $a \in K^*/{K^*}^2$, that is, the group homomorphism β is induced by σ. □

Bibliography

[1] John V. Armitage and Albrecht Fröhlich. Classnumbers and unit signatures. *Mathematika*, 14:94–98, 1967.

[2] Emil Artin and John Tate. *Class field theory.* W. A. Benjamin, Inc., New York-Amsterdam, 1968.

[3] Reinhold Baer. Der Kern, eine charakteristische Untergruppe. *Compositio Math.*, 1:254–283, 1935.

[4] Eva Bayer-Fluckiger and Hendrik W. Lenstra, Jr. Forms in odd degree extensions and self-dual normal bases. *Amer. J. Math.*, 112(3):359–373, 1990.

[5] Dan Boneh and Matt Franklin. Identity-based encryption from the Weil pairing. In *Advances in cryptology—CRYPTO 2001 (Santa Barbara, CA)*, volume 2139 of *Lecture Notes in Comput. Sci.*, pages 213–229. Springer, Berlin, 2001.

[6] Nicolas Bourbaki. *Eléments de mathématique. XV. Première partie: Les structures fondamentales de l'analyse. Livre V: Espaces vectoriels topologiques. Chapitre I: Espaces vectoriels topologiques sur un corps valué. Chapitre II: Ensembles convexes et espaces localement convexes.* Actualités Sci. Ind., no. 1189. Hermann & Cie, Paris, 1953.

[7] Jan Bouw. Thesis (Ph.D.)–Leiden University, forthcoming.

[8] Peter Bruin. The Tate pairing for Abelian varieties over finite fields. *J. Théor. Nombres Bordeaux*, 23(2):323–328, 2011.

[9] John William Scott Cassels and Albrecht Fröhlich. *Algebraic Number Theory.* Academic Press, London, 1967.

[10] Henri Cohen. *Advanced topics in computational number theory*, volume 193 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[11] Henri Cohen and Hendrik W. Lenstra, Jr. Heuristics on class groups of number fields. In *Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983)*, volume 1068 of *Lecture Notes in Math.*, pages 33–62. Springer, Berlin, 1984.

[12] Gunther Cornelissen, Bart de Smit, Xin Li, Matilde Marcolli, and Harry Smit. Characterization of global fields by Dirichlet L-series. *Res. Number Theory*, 5(1):Art. 7, 15, 2019.

[13] Mario Daberkow. On computations in Kummer extensions. *J. Symbolic Comput.*, 31(1-2):113–131, 2001.

[14] Philippe Dutarte. Compatibilité avec le Spiegelungssatz de probabilités conjecturales sur le p-rang du groupe des classes. In *Number theory (Besançon), 1983–1984*, Publ. Math. Fac. Sci. Besançon, pages Exp. No. 4, 11. Univ. Franche-Comté, Besançon, 1984.

[15] Ivan B. Fesenko and Sergei V. Vostokov. *Local fields and their extensions*, volume 121 of *Translations of Mathematical Monographs*. American Mathematical Society, Providence, RI, second edition, 2002.

[16] Étienne Fouvry and Jürgen Klüners. On the Spiegelungssatz for the 4-rank. *Algebra Number Theory*, 4(5):493–508, 2010.

[17] Gerhard Frey and Hans-Georg Rück. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Math. Comp.*, 62(206):865–874, 1994.

[18] Albrecht Fröhlich and Martin J. Taylor. *Algebraic number theory*, volume 27 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1993.

[19] Fritz Gaßmann. Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe. *Math. Z.*, 25(1):661–675, 1926.

[20] Carl Friedrich Gauss, William C. Waterhouse, and Arthur A. Clarke. *Disquisitiones Arithmeticae*. Springer New York, 2018.

[21] Johann Carl Friedrich Gauss. *Disquisitiones Arithmeticae*. Leipzig, 1801.

[22] Pierre Antoine Grillet. *Abstract algebra*, volume 242 of *Graduate Texts in Mathematics*. Springer, New York, second edition, 2007.

[23] Paul Richard Halmos. *Measure Theory*. D. Van Nostrand Company, Inc., New York, N. Y., 1950.

[24] David R. Hayes. On the 2-ranks of Hilbert class fields. Working paper.

[25] Florian Hess. A note on the Tate pairing of curves over finite fields. *Arch. Math. (Basel)*, 82(1):28–32, 2004.

[26] Everett W. Howe. The Weil pairing and the Hilbert symbol. *Math. Ann.*, 305(2):387–392, 1996.

[27] Kenneth Ireland and Michael Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.

[28] Shokichi Iyanaga. *The theory of numbers*. North-Holland Publishing Company, Amsterdam, 1975.

[29] Helmut Koch. *Zahlentheorie*, volume 72 of *Vieweg Studium: Aufbaukurs Mathematik*. Friedr. Vieweg & Sohn, Braunschweig, 1997. Algebraische Zahlen und Funktionen.

[30] Keiichi Komatsu. On adèle rings of arithmetically equivalent fields. *Acta Arith.*, 43(2):93–95, 1984.

[31] Serge Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[32] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[33] Yoonjin Lee. Cohen-Lenstra heuristics and the Spiegelungssatz: number fields. *J. Number Theory*, 92(1):37–66, 2002.

[34] Yoonjin Lee. Cohen-Lenstra heuristics and the Spiegelungssatz: function fields. *J. Number Theory*, 106(2):187–199, 2004.

[35] Adrien-Marie Legendre. *Recherches d'analyse indéterminée*. Histoire de l'Académie Royale des Sciences. 1785.

[36] Adrien-Marie Legendre. *Essai sur la théorie des nombres*. Paris, 1798.

[37] Franz Lemmermeyer. *Reciprocity laws*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2000. From Euler to Eisenstein.

[38] Franz Lemmermeyer. Selmer groups and quadratic reciprocity. *Abh. Math. Sem. Univ. Hamburg*, 76:279–293, 2006.

[39] Franz Lemmermeyer. Euler, Goldbach, and "Fermat's Theorem". *Elem. Math.*, 65(4):144–153, 2010.

[40] Abraham Lempel and Marcelo J. Weinberger. Self-complementary normal bases in finite fields. *SIAM J. Discrete Math.*, 1(2):193–198, 1988.

[41] Heinrich-Wolfgang Leopoldt. Zur Struktur der l-Klassengruppe galoisscher Zahlkörper. *J. Reine Angew. Math.*, 199:165–174, 1958.

[42] Stephen Lichtenbaum. Duality theorems for curves over p-adic fields. *Invent. Math.*, 7:120–136, 1969.

[43] Jessie MacWilliams. Error-correcting codes for multiple-level transmission. *Bell System Tech. J.*, 40:281–308, 1961.

[44] Daniel A. Marcus. *Number fields*. Springer-Verlag, New York, 1977. Universitext.

[45] Thomas M. McCall, Charles J. Parry, and Ramona R. Ranalli. The 2-rank of the class group of imaginary bicyclic biquadratic fields. *Canad. J. Math.*, 49(2):283–300, 1997.

[46] James S. Milne. *Arithmetic Duality Theorems*. BookSurge, LLC, second edition, 2006.

[47] James S. Milne. Lectures on etale cohomology (v2.21), 2013. Available at www.jmilne.org/math/.

[48] John Milnor. *Introduction to algebraic K-theory*. Princeton University Press, Princeton, N.J., 1971.

[49] Sidney Allen Morris. *Pontryagin duality and the structure of locally compact abelian groups*. Cambridge University Press, Cambridge, 1977. London Mathematical Society Lecture Note Series, No. 29.

[50] Jürgen Neukirch. *Class field theory*, volume 280 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, Berlin, 1986.

[51] Jürgen Neukirch. *Algebraic Number Theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, Berlin, 1999.

[52] Midori Onabe. On the isomorphisms of the Galois groups of the maximal Abelian extensions of imaginary quadratic fields. *Natur. Sci. Rep. Ochanomizu Univ.*, 27(2):155–161, 1976.

[53] Bernard Oriat. Relation entre les 2-groupes des classes d'idéaux au sens ordinaire et restreint de certains corps de nombres. *Bull. Soc. Math. France*, 104(3):301–307, 1976.

[54] Matteo Pintonello. Characterizing number fields with quadratic L-functions. Master's thesis, Università degli studi di Padova and Universiteit Leiden, 2018.

[55] Lev Semenovich Pontryagin. Über stetige algebraische Körper. *Ann. of Math. (2)*, 33(1):163–174, 1932.

[56] Lev Semenovich Pontryagin. *Topological groups*. Translated from the second Russian edition by Arlen Brown. Gordon and Breach Science Publishers, Inc., New York, 1966.

[57] Bjorn Poonen and Michael Stoll. The Cassels-Tate pairing on polarized abelian varieties. *Ann. of Math. (2)*, 150(3):1109–1149, 1999.

[58] Heinz Prüfer. Untersuchungen über die Zerlegbarkeit der abzählbaren primären Abelschen Gruppen. *Math. Z.*, 17(1):35–61, 1923.

[59] Derek John Scott Robinson. *A course in the theory of groups*, volume 80 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1982.

[60] Joseph J. Rotman. *An introduction to the theory of groups*, volume 148 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, fourth edition, 1995.

[61] Edward F. Schaefer. A new proof for the non-degeneracy of the Frey-Rück pairing and a connection to isogenies over the base field. In *Computational aspects of algebraic curves*, volume 13 of *Lecture Notes Ser. Comput.*, pages 1–12. World Sci. Publ., Hackensack, NJ, 2005.

[62] Andrzej Schinzel. Abelian binomials, power residues and exponential congruences. *Acta Arith.*, 32(3):245–274, 1977.

[63] Arnold Scholz. Über die Beziehung der Klassenzahlen quadratischer Körper zueinander. *J. Reine Angew. Math.*, 166:201–203, 1932.

[64] René Schoof. Computing Arakelov class groups. In *Algorithmic number theory: lattices, number fields, curves and cryptography*, volume 44 of *Math. Sci. Res. Inst. Publ.*, pages 447–495. Cambridge Univ. Press, Cambridge, 2008.

[65] Jean-Pierre Serre. *Corps locaux*. Publications de l'Institut de Mathématique de l'Université de Nancago, VIII. Actualités Sci. Indust., No. 1296. Hermann, Paris, 1962.

[66] Romyar T. Sharifi. On norm residue symbols and conductors. *J. Number Theory*, 86(2):196–209, 2001.

[67] Peter Stevenhagen. *Class groups and governing fields.* ProQuest LLC, Ann Arbor, MI, 1988. Thesis (Ph.D.)–University of California, Berkeley.

[68] Henning Stichtenoth. *Algebraic Function Fields and Codes.* Springer Publishing Company, Incorporated, 2nd edition, 2008.

[69] Attila Szakács. Unitary subgroup of the unit group of group algebra of finite abelian group. *Nauk. Vīsn. Uzhgorod. Univ. Ser. Mat.*, (1):35–39, 1994.

[70] John Tate. *WC-groups over $\mathfrak{p}$-adic fields*, volume 13 of *Séminaire Bourbaki; 10e année: 1957/1958. Textes des conférences; Exposés 152 à 168; 2e éd. corrigée, Exposé 156.* Secrétariat mathématique, Paris, 1958.

[71] Kôji Uchida. Isomorphisms of Galois groups. *J. Math. Soc. Japan*, 28(4):617–620, 1976.

[72] David van Dantzig. *Studiën over topologische algebra.* Dissertation. H. J. Paris, Amsterdam, 1931.

[73] Charles Terence Clegg Wall. Quadratic forms on finite groups, and related topics. *Topology*, 2:281–298, 1963.

[74] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, second edition, 1997.

[75] André Weil. *L'intégration dans les groupes topologiques et ses applications.* Actual. Sci. Ind., no. 869. Hermann & Cie, Paris, 1940.

[76] André Weil. *Basic number theory.* Springer-Verlag, New York-Berlin, third edition, 1974. Die Grundlehren der Mathematischen Wissenschaften, Band 144.

[77] André Weil. *Number theory.* Modern Birkhäuser Classics. Birkhäuser Boston, Inc., Boston, MA, 2007. An approach through history from Hammurapi to Legendre, Reprint of the 1984 edition.

[78] Jay A. Wood. Duality for modules over finite rings and applications to coding theory. *Amer. J. Math.*, 121(3):555–575, 1999.

Summary

The present thesis consists of eleven chapters.

In 1897, Hilbert introduced into algebraic number theory the *norm-residue symbol*, which is a bimultiplicative map whose values are roots of unity. Using the norm-residue symbol, in Sections 1.1 to 1.6 of Chapter 1 we reformulate the *quadratic reciprocity law*, together with its two supplementary laws, in terms of bilinear forms on vector spaces over the field of two elements. We also introduce the *unit residue group* of the field of rational numbers. Section 1.7 is an overview of the content of the thesis and each of Sections 1.8 to 1.17 outlines the main results of one of the chapters of the thesis.

A *skew abelian group* is a finite abelian group equipped with an antisymmetric perfect pairing. Every skew abelian group has a special element called its *skew element*, which has order dividing 2. Chapter 2, which is purely auxiliary, collects some results about skew abelian groups, rephrasing them in terms of the skew element.

In Chapter 3 we review local class field theory and the norm-residue symbol. We also examine some skew abelian groups of which the pairing is the norm-residue symbol.

The group of ideles of any global field is equipped with a pairing induced by the local norm-residue symbols. This pairing and its connections to the Tate pairing are studied in Chapter 4.

Chapter 5 is devoted to introducing the unit residue group and the *virtual group*, which is a subgroup of the unit residue group, and presenting general results on them.

We explicitly describe all unit residue groups and virtual groups of quadratic number fields in Chapter 6. The descriptions include the Galois module structure.

The classical theorem of Armitage–Fröhlich gives a lower bound on the 2-rank of the ideal class group of a number field. Chapter 7 places the 2-nd virtual group of a number field in this context of inequalities involving 2-ranks

of ideal class groups.

In 1932 Scholz proved a theorem about the 3-ranks of ideal class groups of quadratic number fields. Using unit residue groups we rephrase and prove Scholz's theorem in Chapter 8. Moreover, we present and employ a probabilistic model on 3-ranks of ideal class groups of quadratic number fields. The probabilities that we compute from this model coincide with those predicted by the Cohen—Lenstra heuristics.

In Chapter 9 we describe the 2-nd unit residue group and the 2-nd virtual group of a number field that is Galois over $\mathbb{Q}$ and unramified at 2. In the case of a cyclic number field $K/\mathbb{Q}$ of degree either 3 or 5 these descriptions give rise to an unexpected bijection involving the set of real Archimedean places of K.

A certain subgroup of the group of units of a finite extension of the field of p-adic rationals, where p is a prime, occurs in algorithms for computing the norm-residue symbol by Daberkow and Bouw. This subgroup is the subject of study in Chapter 10.

In Chapter 11 we deal with group isomorphisms between the groups of quadratic characters of two number fields that preserve L-series. In particular, we prove that the natural map from the set of field isomorphisms between two number fields to the set of group isomorphisms between their groups of quadratic characters that preserve L-series is bijective.

Samenvatting

Dit proefschrift, getiteld 'De groep van eenheidsrestklassen', bestaat uit elf hoofdstukken.

In 1897 introduceerde Hilbert in de algebraïsche getaltheorie het *normrestsymbool*. Dit is een bimultiplicatieve afbeelding met waarden die eenheidswortels zijn. In Paragraaf 1.1 tot en met 1.6 van Hoofdstuk 1 herformuleren we, gebruikmakend van het normrestsymbool, de *kwadratische reciprociteitswet*, samen met beide aanvullingswetten, in termen van bilineaire vormen op vectorruimten over het lichaam van twee elementen. We introduceren ook de *eenheidsrestklassengroep* van het lichaam der rationale getallen. Paragraaf 1.7 bevat een overzicht van de inhoud van het proefschrift als geheel, en Paragrafen 1.8 tot en met 1.17 geven elk een overzicht van de hoofdresultaten van een van de afzonderlijke hoofdstukken van het proefschrift.

Een *scheve abelse groep* is een eindige abelse groep uitgerust met een antisymmetrische perfecte paring. Iedere scheve abelse groep heeft een speciaal element, genaamd het *scheve element*, waarvan de orde een deler is van 2. Hoofdstuk 2 bestaat uit een verzameling hulpresultaten over scheve abelse groepen, geherformuleerd in termen van het scheve element.

In Hoofdstuk 3 laten we lokale klassenlichamentheorie en het normrestsymbool de revue passeren. We bekijken ook een aantal scheve abelse groepen waarvan de paring gegeven wordt door het normrestsymbool.

De groep van idèles van een globaal lichaam is uitgerust met een paring geïnduceerd door de lokale normrestsymbolen. Deze paring en de manier waarop deze samenhangt met de Tate-paring worden onderzocht in Hoofdstuk 4.

In Hoofdstuk 5 voeren we de eenheidsrestklassengroep en de *virtuele groep* in, die een ondergroep van de eenheidsrestklassengroep is, en we behandelen algemene resultaten over deze groepen.

We geven in Hoofdstuk 6 een expliciete beschrijving van alle eenheidsrestklassengroepen en virtuele groepen van kwadratische getallenlichamen, inclusief hun Galois-moduulstructuur.

De klassieke stelling van Armitage–Fröhlich geeft een ondergrens voor de 2-rang van de ideaalklassengroep van een getallenlichaam. Hoofdstuk 7 plaatst de tweede virtuele groep van een getallenlichaam in de context van dergelijke ongelijkheden aangaande 2-rangen van ideaalklassengroepen.

In 1932 bewees Scholz een stelling over de 3-rangen van ideaalklassengroepen van kwadratische getallenlichamen. Gebruikmakende van eenheidsrestklassengroepen geven we een herformulering en een bewijs van de stelling van Scholz in Hoofdstuk 8. Verder geven we een probabilistisch model voor 3-rangen van ideaalklassengroepen van kwadratische getallenlichamen. De kansen die we met dit model berekenen, zijn precies de kansen die voorspeld worden door de Cohen–Lenstra-heuristiek.

In Hoofdstuk 9 beschrijven we de tweede eenheidsrestklassengroep en de tweede virtuele groep van een getallenlichaam dat Galois is over $\mathbb{Q}$ en onvertakt is bij 2. In het geval van een cyklische uitbreiding K van $\mathbb{Q}$ van graad 3 of 5 geven deze beschrijvingen aanleiding tot een onverwachte bijectie waarin de verzameling van reële Archimedische plaatsen van K voorkomt.

Een zekere ondergroep van de eenhedengroep van een eindige uitbreiding van het lichaam der p-adische getallen, met p een priemgetal, die een rol speelt in algoritmen voor het berekenen van normrestsymbolen van Daberkow en Bouw, bestuderen we in Hoofdstuk 10.

In Hoofdstuk 11 kijken we naar isomorfismen tussen de groepen van kwadratische karakters van twee getallenlichamen die L-reeksen behouden. In het bijzonder bewijzen we dat de natuurlijke afbeelding van de verzameling van lichaamsisomorfismen tussen twee getallenlichamen naar de verzameling van groepsisomorfismen tussen hun groepen van kwadratische karakters die L-reeksen behouden, een bijectie is.

Curriculum vitae

Gabriele Dalla Torre was born in Trento (Italy) on 19 January 1983. There he grew up and got his diploma at Liceo classico Giovanni Prati in 2002. After winning a scholarship at Scuola Normale Superiore in Pisa, he moved to Tuscany to study Mathematics.

In 2005 he achieved his Bachelor's degree in Mathematics with a thesis in algebraic number theory entitled "Il teorema di densità di Chebotarev e alcune sue applicazioni" ("Chebotarev's density theorem and some applications") under the supervision of Professor Roberto Dvornicich at the Università di Pisa. He took his Master's degree in Mathematics with the thesis "Alcuni problemi di class field theory" ("Some problems in class field theory") under the supervision of Professor Roberto Dvornicich in 2007. He graduated from the Scuola Normale Superiore in 2008, became a PhD student at Scuola Normale Superiore and then, in 2011, at the Mathematisch Instituut of the Universiteit Leiden. He wrote his PhD thesis, with the title "The unit residue group" under the supervision of Professor Hendrik Lenstra.

During his studies Gabriele worked as an editor of the problem section of the Nieuw Archief voor Wiskunde and has been an active collaborator of the mathematical olympiad. Since 2014 he has been a member of the Italian national committee "Olimpiadi della matematica".

Back in Italy he got the teaching qualification in Mathematics and Physics for secondary school and has organized and supervised many Math camps for high school students. He was a teaching assistant and has been a collaborator of Professor Gabriele Anzellotti at the Università degli studi di Trento since 2013.

Currently, he is also working on the preparation and validation of Cisia university entrance tests and at the Università degli studi di Trento to implement a tutoring system for students in Italian universities.