THEORIE DES NOMBRES
BESANCON

Année 1988/1989
Fascicule 1

# RAY CLASS GROUPS AND GOVERNING FIELDS

Peter Stevenhagen

Universiteit van Amsterdam
Proefschrift
June 1989

## Contents

# CHAPTER I

# Introduction

## 1. Background

Number theory finds its origins in the study of integral and rational numbers, and the problem of finding integral or rational numbers that satisfy some given equation. An old result on integral numbers—usually called integers—that was already known to Euclid (300 B.C.) is the so called fundamental theorem of arithmetic. It states that every positive integer can be written as a product of prime numbers, and that this prime number decomposition is essentially unique. Finding integral or rational solutions to a given equation is a problem that was studied by Diophantos of Alexandria (250 A.D.), and his name has been attached to such equations. Solving diophantine equations is a notoriously difficult problem that has stimulated the development of new methods until our days. There is no general method to find the solutions to these equations, but many interesting results have been obtained for certain classes of equations. A diophantine equation that has acquired some fame even outside mathematical circles is the *Fermat equation* $X^n + Y^n = Z^n$. As to date, it is unknown whether Fermat's statement (1637) that there are no solutions in non-zero integers when $n$ larger than 2 is true.

History has shown that, even though a problem is formulated entirely in terms of rational numbers, it is often fruitful to admit numbers that are not necessarily rational. Real and complex numbers are probably the examples that most readily come to mind, but there are many more. For instance, many of the results on the Fermat equation were derived by studying the equation over the *cyclotomic field* $\mathbb{Q}(\zeta_n)$, where it can be written as

$$X^n = (Z - Y)(Z - \zeta_n Y)(Z - \zeta_n^2 Y) \ldots (Z - \zeta_n^{n-1} Y).$$

Here $\zeta_n$ denotes a primitive $n$-th root of unity, i.e. a number such that $\zeta_n^n = 1$ and $\zeta_n^k \neq 1$ for $k = 1, 2, \ldots, n-1$. Such a number is not rational if $n > 2$, and in that case the field $\mathbb{Q}(\zeta_n)$, which consists of elements $x$ that can be written as

$$x = a_0 + a_1\zeta_n + a_2\zeta_n^2 + \ldots + a_{n-1}\zeta_n^{n-1}$$

for certain rational $a_i$, is strictly larger than the field of rational numbers $\mathbb{Q}$. The field $\mathbb{Q}(\zeta_n)$ can be viewed as a subfield of the field of complex numbers $\mathbb{C}$ by taking $\zeta_n = e^{\frac{2\pi i}{n}}$, but it has finite dimension as a vector space over $\mathbb{Q}$ and is therefore much smaller than $\mathbb{C}$. It has been proved for many $n$ that the Fermat equation does not have non-zero solutions $X$, $Y$ and $Z$ in $\mathbb{Q}(\zeta_n)$. Note that the Fermat equation has infinitely many non-zero solutions for any $n$ if we allow them to be in $\mathbb{C}$ or the field of real numbers $\mathbb{R}$.

Fields like the cyclotomic field $\mathbb{Q}(\zeta_n)$ that are finite dimensional as a vector space over the field of rational numbers $\mathbb{Q}$ are called *algebraic number fields*. They play a major role in algebraic number theory. An algebraic number field can always be obtained from $\mathbb{Q}$ by

adjoining a root $\alpha$ of an polynomial with coefficients in $\mathbf{Q}$. This means that all elements of this number field can be written in the form

$$x = a_0 + a_1\alpha + a_2\alpha^2 + ... + a_k\alpha^k$$

with $a_i$ in $\mathbf{Q}$.

Number fields are usually much better tools for studying arithmetical questions than a large field like $\mathbf{C}$. The most important reason is that they allow an arithmetical theory that is not too different from the arithmetic of $\mathbf{Q}$ as described by Euclid. This theory was developed in the 19-th century by mathematicians as Kummer, Kronecker and Dedekind.

Any number field $K$ has a *ring of integers* $\mathcal{O}$ that is defined as the integral closure of the ring of ordinary integers $\mathbf{Z}$. This means that $\mathcal{O}$ consists of those $x$ in $K$ that are zeroes of a monic polynomial with coefficients in $\mathbf{Z}$. For $K = \mathbf{Q}$ we find $\mathcal{O} = \mathbf{Z}$. In general, $\mathcal{O}$ is a ring that contains $\mathbf{Z}$, and every element of $K$ is the quotient of two elements from $\mathcal{O}$.

Rings of integers behave somewhat differently from $\mathbf{Z}$ in the sense that their group of invertible elements may be infinite—in $\mathbf{Z}$ one only has $\{\pm 1\}$ as the unit group—and that they need not have unique prime factor decomposition. However, the structure of the unit group of a ring of integers $\mathcal{O}$ is given explicitly by the Dirichlet unit theorem, and unique factorization can be obtained by looking at prime *ideals* rather than prime elements of this ring. One has unique prime factor decomposition of elements in $\mathcal{O}$ if and only if all ideals of $\mathcal{O}$ are principal, i.e. generated by a single element in the ideal. In general, if one considers the group of all *fractional* $\mathcal{O}$-ideals the subgroup of principal fractional ideals is always of finite index. The corresponding factor group is the *class group* $Cl$ of $\mathcal{O}$ (or of $K$). It is a finite abelian group that measures how many ideals in $\mathcal{O}$ are principal. Its order is the *class number* $h$ of $K$. Fields with unique prime factor decomposition are the fields for which $h = 1$.

Prime numbers from $\mathbf{Z}$ need no longer be prime elements in the ring of integers $\mathcal{O}$ of $K$. If we set $\mathrm{i} = \sqrt{-1}$, the field $\mathbf{Q}(\mathrm{i})$ has ring of integers $\mathcal{O} = \mathbf{Z}[\mathrm{i}] = \mathbf{Z} + \mathbf{Z} \cdot \mathrm{i}$. The prime numbers that are not the sum of two squares in $\mathbf{Z}$, like 3, 7, 11 or 163, are prime elements in $\mathcal{O}$. Fermat proved that these are exactly the prime numbers that are congruent to 3 modulo 4. All other prime numbers, like $2 = 1^2 + 1^2$ and $13 = 2^2 + 3^2$, split in $\mathcal{O}$, as is shown by the equations

$$2 = (1 + \mathrm{i})(1 - \mathrm{i}) = \mathrm{i}(1 - \mathrm{i})^2 \qquad \text{and} \qquad 13 = (2 + 3\mathrm{i})(2 - 3\mathrm{i}).$$

Primes that remain prime in $\mathcal{O}$ are called *inert*, and primes that split into different primes in $\mathcal{O}$ are said to be *split*. The prime 2, which has a square factor in $\mathcal{O}$, is a *ramified* prime.

For fields of the form $\mathbf{Q}(\sqrt{d})$, called *quadratic fields*, the splitting behaviour of a prime $p$ depends on whether $p$ can be represented by quadratic expressions, like $X^2 + Y^2$ in the

preceding example. This is part of the theory of quadratic forms, which was developed by Gauss (1801). It furnishes the oldest description of the class group of a quadratic field.

The splitting of primes in fields of degree larger than 2, such as the cyclotomic fields $\mathbb{Q}(\zeta_n)$ for $n = 5$ and $n > 6$, was initiated by Kummer (1847). It turns out that the splitting behaviour of a prime number $p$ in a cyclotomic extension is particularly simple to describe: it only depends on the residue class of $p$ modulo $n$. There are only finitely many primes $p$ that divide $n$, and—if $p = 2$ is treated with care—these are exactly the primes that are ramified in $\mathbb{Q}(\zeta_n)$. The other prime numbers $p$ split into a number of primes that is exactly the *index* of the subgroup generated by $p$ mod $n$ in the $(\mathbb{Z}/n\mathbb{Z})^*$. Here $(\mathbb{Z}/n\mathbb{Z})^*$ denotes the multiplicative group of integers modulo $n$ that are coprime to $n$. The *order* of $p$ mod $n$ gives us the 'size' the primes over $p$. In particular, it follows that the prime numbers that are congruent to 1 modulo $n$ split into the maximal number of different primes. Such primes are said to *split completely*. The reader may check that we find the result of Fermat for $\mathbb{Q}(\zeta_4) = \mathbb{Q}(\mathrm{i})$.

It turns out that the only number fields in which the splitting of prime numbers is determined by congruence conditions are the fields $\mathbb{Q}(\zeta_n)$ and their subfields. These fields have the special property that their automorphisms form an *abelian* group, i.e. a group in which $\sigma\tau = \tau\sigma$ for all elements $\sigma$ and $\tau$. Indeed, for each element $a$ mod $n$ in $(\mathbb{Z}/n\mathbb{Z})^*$ there is an automorphism $\sigma_a$ that sends $\zeta_n$ to $\zeta_n^a$, and any automorphism of $\mathbb{Q}(\zeta_n)$ must be of this form. One deduces that the automorphism group of $\mathbb{Q}(\zeta_n)$ is given by

$$\mathrm{Aut}(\mathbb{Q}(\zeta_n)) = (\mathbb{Z}/n\mathbb{Z})^*,$$

and this is an abelian group. A theorem due to Kronecker and Weber (1886) states that the cyclotomic fields and their subfields are the *only* number fields with this property.

Kummer's splitting theory for cyclotomic fields was generalized by Dedekind, Kronecker and Hilbert to arbitrary extensions of number fields $K \subset L$ rather than $\mathbb{Q} \subset \mathbb{Q}(\zeta_n)$. The theory of the automorphisms of fields in a general setting had already been developed by Galois (1821). Enlarging $L$ to a 'normal' field when necessary, one can define the *Galois group* $\mathrm{Gal}(L/K)$ as consisting of all automorphisms of $L$ that are the identity on $K$. If one excludes the finite number of primes that are ramified from consideration, the splitting behaviour of a prime $\mathfrak{p}$ from $K$ in the extension $L$ can now be described by associating to the prime $\mathfrak{p}$ certain elements in $\mathrm{Gal}(L/K)$, called *Frobenius symbols*. If $\mathrm{Gal}(L/K)$ is *abelian* there is exactly one such element, the *Artin symbol* of $\mathfrak{p}$. The Artin symbol of a prime number $p$ in the cyclotomic extension $\mathbb{Q} \subset \mathbb{Q}(\zeta_n)$ is the element $\sigma_p = p \bmod n$ that raises $\zeta_n$ to the $p$-th power. In the general case, the Artin symbol is also characterized as the element in $\mathrm{Gal}(L/K)$ that in a certain sense 'raises to the power $\mathfrak{p}$'. Its order in $\mathrm{Gal}(L/K)$ gives the size of the primes over $\mathfrak{p}$ in $L$, and the index of the subgroup it generates in $\mathrm{Gal}(L/K)$ is just the number of primes into which $\mathfrak{p}$ splits in $L$.

Led by the analogy with cyclotomic extensions, one may now ask whether the splitting behaviour of $\mathfrak{p}$ in abelian extensions $L$ of $K$ is determined by congruence conditions on the prime $\mathfrak{p}$, and whether this characterizes the abelian extensions of $K$. The positive answer to this question is given by *class field theory*, a theory developed between 1895 and 1955 by several mathematicians including Hilbert, Weber, Takagi, Artin, Hasse, Chevalley and Tate. It gives an intimate connection between the arithmetic of a number field $K$—described by groups like the class group $Cl$ of $K$—and the existence of certain abelian extensions of $K$.

If the splitting behaviour of a prime number $p$ in an extension $L$ of $\mathbb{Q}$ only depends on $p$ mod $f$, we know that $L/\mathbb{Q}$ is abelian, and even a subfield of the cyclotomic field $\mathbb{Q}(\zeta_f)$. Analogously, if the splitting behaviour of a prime $\mathfrak{p}$ in an extension $L$ of $K$ only depends on the 'residue class' of $\mathfrak{p}$ modulo $\mathfrak{f}$, then $L/K$ is an abelian extension that is a subfield of the *ray class field* $H_\mathfrak{f}$. There is again a Kronecker-Weber theorem that asserts that all abelian extensions of $K$ are obtained as subfields of a ray class field $H_\mathfrak{f}$. There is no general method to find the ray class fields $H_\mathfrak{f}$ of $K$ explicitly in terms of $K$ and $\mathfrak{f}$, except when $K$ equals $\mathbb{Q}$ or a field $\mathbb{Q}(\sqrt{d})$ with $d < 0$. However, the Galois groups $\mathrm{Gal}(H_\mathfrak{f}/K)$ are explicitly given by class field theory. They are the *ray class groups* $C_\mathfrak{f}$ that form the main object of study in this thesis.

The class group $Cl$ of the field $K$, which occurs as $C_\mathfrak{f}$ for $\mathfrak{f} = 1$, is the simplest ray class group of $K$. All other class groups are larger in the sense that there is a natural surjection

$$C_\mathfrak{f} \longrightarrow Cl$$

for all $\mathfrak{f}$. One way to specify the structure of $C_\mathfrak{f}$ is to describe which *extension* of $Cl$ it gives. Homological algebra gives a formalism to describe extensions of abelian groups that are again abelian. If one takes for $\mathfrak{f}$ only primes $\mathfrak{p}$ of $K$, fixes an integer $m$ and restricts attention to a group $C'_\mathfrak{p}$ that is slightly smaller than $C_\mathfrak{p}$, the extension types one obtains are elements of certain *extension groups* $\mathrm{Ext}(Cl, \langle\zeta_n\rangle)$ with $n$ dividing $m$. The obvious question is: which primes $\mathfrak{p}$ give rise to which extension classes? In this thesis, it is proved that the answer to such questions is given by a *governing field* for the extension structure. An extension $M/K$ is said to be a governing field for the extension structure if the class of the extension $C'_\mathfrak{p}$ in the extension group $\mathrm{Ext}(Cl, \langle\zeta_n\rangle)$ is determined by the splitting behaviour of $\mathfrak{p}$ in the extension $M/K$. The precise formulation of this statement is given by homomorphisms from automorphism groups of $M$ to extension groups that map Artin symbols over $\mathfrak{p}$ to extension classes coming from $C'_\mathfrak{p}$. The type of question sketched above is the subject of the second chapter of this thesis. It introduces a new type of extension group that is especially well-suited to describe extension structures that arise in the context of ray class groups.

An interesting feature of the existence of a governing field is that it enables us to

derive *density statements* for the set of primes $\mathfrak{p}$ in $K$ that give rise to ray class groups with a given extension behaviour. These statements are based on an analytic theorem, due to Čebotarev (1925), which tells us how many primes $\mathfrak{p}$ in $K$ give rise to prescribed Frobenius symbols in $\mathrm{Gal}(M/K)$.

The third chapter of this thesis considers ray class groups of $K$ with respect to a prime from a base field $k$ that is smaller than $K$. It leads to extensions of ray class groups with a fixed group, and methods from idelic class field theory are employed to show that these structures can also be described by governing fields.

In the fourth and last chapter, our main theorem on ray class group extensions is applied to a problem of Cohn and Lagarias. It was in this context that the concept of a governing field was originally introduced. The problem consists of finding governing fields for certain invariants, the $2^k$-*ranks*, that determine the structure of the 2-*primary part* of the class group of the field $\mathbb{Q}(\sqrt{dp})$. Such fields had been found for certain values of $k$ and $d$, and computer calculations led Cohn and Lagarias to enounce a set of conjectures concerning the existence of governing fields. For $k = 1$ (Gauss, 1801) and $k = 2$ (Rédei-Reichardt, 1934) the conjectures were already known to hold. We prove the 8-*rank conjecture* corresponding to the case $k = 3$. The conjectures remain open for $k \geq 4$.

## 2. Outline

This section serves two purposes. First of all, it introduces most of the notations and results from class field theory that are used throughout this thesis. Secondly, it sketches the results and the main ideas of the proofs in this thesis by treating several simple cases in some detail. In doing so, it also serves as a motivation for the more technical approach in the following chapters.

We start with some basic facts from class field theory that are essential to the formulation of our results. More details and proofs of all statements can be found in [7] and [21].

The oldest version of class field theory (Takagi-Artin, 1927) uses the concept of cycles of $K$. A *cycle* of $K$ is a formal product $\mathfrak{f} = \prod \mathfrak{p}^{n(\mathfrak{p})}$ over all primes $\mathfrak{p}$ of $K$, with non-negative integral exponents that are almost all zero. The exponent is required to be at most one at real primes, and zero at complex primes. Divisibility of cycles is defined in the obvious way. For a finite abelian extension $K \subset L$ and a cycle $\mathfrak{f} = \prod \mathfrak{p}^{n(\mathfrak{p})}$ that is divisible by all primes that ramify in $K \subset L$, one considers the *Artin map*

$$\psi = \psi_{\mathfrak{f},L/K} : \mathcal{I}(\mathfrak{f}) \longrightarrow \mathrm{Gal}(L/K)$$

on the group $\mathcal{I}(\mathfrak{f})$ of fractional $\mathcal{O}$-ideals that have no primes occurring in $\mathfrak{f}$ in their prime ideal decomposition. This map is defined as the homomorphism that sends a prime ideal

$\mathfrak{p} \in \mathcal{I}(\mathfrak{f})$ to its Artin symbol in $\mathrm{Gal}(L/K)$. The main theorem of class field theory states that given $K \subset L$, the exponents of $\mathfrak{f}$ at the ramifying primes can be chosen in such a way that

$$\ker\psi \supset \mathcal{S}(\mathfrak{f}), \tag{2.1}$$

where $\mathcal{S}(\mathfrak{f})$, the *ray modulo* $\mathfrak{f}$, is the subgroup of $\mathcal{I}(\mathfrak{f})$ consisting of the principal ideals $\alpha\mathcal{O}$ that are generated by an element $\alpha \equiv 1 \bmod^* \mathfrak{f}$. This *multiplicative* congruence means that $\mathrm{ord}_{\mathfrak{p}}(\alpha-1) \geq n(\mathfrak{p})$ at all finite primes $\mathfrak{p}$ in $\mathfrak{f}$, and that $\alpha$ is positive in the completions of $K$ at the real primes in $\mathfrak{f}$. A multiplicative congruence $\alpha \equiv \beta \bmod^* \mathfrak{f}$ stands for $\alpha\beta^{-1} \equiv 1 \bmod^* \mathfrak{f}$. The minimal cycle satisfying (2.1) is the *conductor* $\mathfrak{f}_{L/K}$ of the extension $K \subset L$. It is exactly divisible by the primes that ramify in $K \subset L$, and tamely ramifying primes have exponent 1 in the conductor. The maximal abelian extension of $K$ that has conductor $\mathfrak{f}$ is called the *ray class field* $H_{\mathfrak{f}}$ of $K$ modulo $\mathfrak{f}$. It is a finite extension of $K$, and the Artin map induces an isomorphism

$$\mathcal{C}_{\mathfrak{f}} = \mathcal{I}(\mathfrak{f})/\mathcal{S}(\mathfrak{f}) \xrightarrow{\sim} \mathrm{Gal}(H_{\mathfrak{f}}/K). \tag{2.2}$$

The group $\mathcal{C}_{\mathfrak{f}}$ is known as the *ray class group* modulo $\mathfrak{f}$. There is an inclusion reversing bijection between the set of abelian extensions of $K$ inside some algebraic closure and the set of *ideal groups* of $K$. An ideal group of $K$ is a set of groups $\{\mathcal{B}(\mathfrak{f})\}_{\mathfrak{f}\in\mathfrak{F}}$, with $\mathcal{S}(\mathfrak{f}) \subset \mathcal{B}(\mathfrak{f}) \subset \mathcal{I}(\mathfrak{f})$. Here $\mathcal{B}_{\mathfrak{g}}$ is the canonical inverse image of $\mathcal{B}_{\mathfrak{f}}$ if $\mathfrak{f} \mid \mathfrak{g}$ and $\mathfrak{f}, \mathfrak{g} \in \mathfrak{F}$, and $\mathfrak{F}$ consists of all multiples of a minimal cycle, the conductor of the ideal group. Inclusions between ideal groups are defined by looking at representatives $\mathcal{B}(\mathfrak{f})$ modulo a common $\mathfrak{f}$. The extension $K \subset L$ corresponds to the ideal group $\{\ker\psi_{\mathfrak{f},L/K}\}_{\mathfrak{f}_{L/K}|\mathfrak{f}}$. It follows that every finite abelian extension of $K$ can be obtained as a subfield of a ray class field. For $K = \mathbb{Q}$, where the ray class fields are the cyclotomic fields and their maximal real subfields, this is the Kronecker-Weber theorem.

In the special case that $\mathfrak{f}$ is the trivial cycle, the ray class group modulo $\mathfrak{f}$ is the ordinary class group $Cl$ of $\mathcal{O}$. It follows that $Cl$ is canonically isomorphic to the Galois group $\mathrm{Gal}(H/K)$, where the *Hilbert class field* $H$ of $K$ is the maximal abelian extension of $K$ that is unramified at all primes. Taking for $\mathfrak{f}$ the product of the real primes of $K$, usually abbreviated to $\infty$, one obtains an analogous statement for the *strict class group* and the *strict Hilbert class field*, which is defined as the maximal abelian extension of $K$ that is unramified at all finite primes.

We now come to the contents of the chapters II and III of this thesis.

Let $\mathfrak{f}$ and $\mathfrak{g}$ be cycles of $K$, and suppose that $\mathfrak{f}$ is divisible by $\mathfrak{g}$. Then there is an inclusion $H_{\mathfrak{g}} \subset H_{\mathfrak{f}}$ and a corresponding surjection of ray class groups $\mathcal{C}_{\mathfrak{f}} \to \mathcal{C}_{\mathfrak{g}}$. In

particular, if we take $\mathfrak{g} = 1$ and write $\mathfrak{f} = \prod_{\mathfrak{p}} \mathfrak{p}^{n(\mathfrak{p})}$, we see that all ray class fields contain the Hilbert class field $H$ of $K$, and that there is an extension of abelian groups

$$0 \longrightarrow A_{\mathfrak{f}} \longrightarrow C_{\mathfrak{f}} \longrightarrow Cl \longrightarrow 0.$$

Denote by $E$ the unit group of $\mathcal{O}$. Then the kernel $A_{\mathfrak{f}}$ can be given explicitly as

$$A_{\mathfrak{f}} = S(1)/S(\mathfrak{f}) \cong \Big( \prod_{\mathfrak{p}|\mathfrak{f} \text{ finite}} (\mathcal{O}/\mathfrak{p}^{n(\mathfrak{p})})^* \times \prod_{\mathfrak{p}|\mathfrak{f} \text{ real}} \langle -1 \rangle \Big) \Big/ \operatorname{im}[E] \tag{2.3}$$

$$[\alpha\mathcal{O}] \mapsto ((\alpha \bmod \mathfrak{p}^{n(\mathfrak{p})})_{\mathfrak{p}}, (\operatorname{sign}_{\mathfrak{p}} \alpha)_{\mathfrak{p}}).$$

Several natural questions about the number field $K$ can be translated into questions about this extension. For instance, one might ask (Cornell [10]): for how many primes $\mathfrak{p}$ does $K$ have a cyclic extension of degree $m$ that is totally and only ramified at $\mathfrak{p}$, if $m \in \mathbb{Z}_{>0}$ is fixed? An equivalent question is, for $\mathfrak{p}$ not dividing $m$: for how many $\mathfrak{p}$ is $\#A_{\mathfrak{p}}$ divisible by $m$ and does the exact sequence

$$\mathcal{E}_{\mathfrak{p}} : \ 0 \longrightarrow A_{\mathfrak{p}}/A_{\mathfrak{p}}^m \longrightarrow C_{\mathfrak{p}}/A_{\mathfrak{p}}^m \longrightarrow Cl \longrightarrow 0$$

split? From (2.3) we see that in this case, we have to deal with extensions of $Cl$ with a *cyclic* group of order dividing $m$. In case $K$ contains a primitive $m$-th root of unity $\zeta_m$, there is an $m$-th power residue symbol at all primes $\mathfrak{p} \nmid m$ that ensures that the group $A_{\mathfrak{p}}/A_{\mathfrak{p}}^m$ is *canonically* isomorphic to a subgroup of $\langle \zeta_m \rangle$. For those $\mathfrak{p}$ that split completely in $K(\sqrt[m]{E})/K$, it is the full group $\langle \zeta_m \rangle$. For these $\mathfrak{p}$ we can view $\mathcal{E}_{\mathfrak{p}}$ as an element of the abelian group $\operatorname{Ext}(Cl, \langle \zeta_m \rangle)$ that classifies all abelian extensions of $Cl$ with the group $\langle \zeta_m \rangle$ (cf. [15, 24]).

Chapter II investigates how the extension classes $\mathcal{E}_{\mathfrak{p}}$ depend on $\mathfrak{p}$. As a special case of the main theorem 5.6 and its corollary 5.12 in the next chapter, we present the following theorem.

**2.4 Theorem.** *Suppose $\zeta_m \in K$. Then there is a canonical isomorphism*

$$\operatorname{Gal}(K(\sqrt[m]{W})/K(E^{1/m})) \cong \operatorname{Ext}(Cl, \langle \zeta_m \rangle).$$

*mapping the Frobenius at a prime $\mathfrak{p} \nmid m$ of $K$ that splits completely in $K(\sqrt[m]{E})/K$ to the class of the extension $\mathcal{E}_{\mathfrak{p}}$. Here $E$ is the unit group of the ring of integers $\mathcal{O}$ of $K$, and $W \subset K^*$ consists of the elements $\alpha$ for which $\alpha\mathcal{O}$ is an $m$-th power of an ideal.*

Let us sketch a proof of theorem 2.4. It is based on a homological lemma that describes the group of extension classes of an arbitrary abelian group with a cyclic group of order

$m$. The lemma itself is proved in the next chapter (3.5). For an arbitrary abelian group $B$, it gives a canonical isomorphism

$$\mathrm{Ext}(B, \langle \zeta_m \rangle) \xrightarrow{\sim} \mathrm{Hom}(B_m, \langle \zeta_m \rangle),$$

where $B_m$ is the subgroup of $B$ consisting of all elements of order dividing $m$. Now take $B = Cl$. If the ideal class $[\mathfrak{a}]$ has order $m$, there exists $a \in W$ that generates $\mathfrak{a}^m$. The class $[\mathfrak{a}]$ determines $\mathfrak{a}$ up to multiplication by principal ideals, and $\mathfrak{a}^m$ determines $a$ up to multiplication by an element of $E$, so there is a canonical isomorphism $Cl_m \xrightarrow{\sim} W/EK^{*m}$. It follows that there is an isomorphism

$$\mathrm{Ext}(Cl, \langle \zeta_m \rangle) \xrightarrow{\sim} \mathrm{Hom}(W/EK^{*m}, \langle \zeta_m \rangle).$$

If $\zeta_m$ is in $K$, the right hand side is isomorphic to $\mathrm{Gal}(K(\sqrt[m]{W})/K(\sqrt[m]{E}))$ by Kummer theory. Looking at the explicit form of all isomorphisms above, one arrives at the statement given in the theorem.

It follows from 2.4 that the splitting behaviour of the sequence $\mathcal{E}_\mathfrak{p}$ for primes $\mathfrak{p}$ that split completely in $K(\sqrt[m]{E})$ is determined by the splitting behaviour of the prime $\mathfrak{p}$ in the extension $K(\sqrt[m]{W})/K$. In fact, if one also uses the theorem with the divisors $m'$ of $m$ in place of $m$, this statement is even true for all finite $\mathfrak{p} \nmid m$. The Čebotarev density theorem [21] now implies that all extensions of $Cl$ with a subgroup of $\langle \zeta_m \rangle$ can be realized as extensions $\mathcal{E}_\mathfrak{p}$, and that the set of primes realizing a given extension has a natural density that can be given explicitly. For instance, the extensions $\mathcal{E}_\mathfrak{p}$ of the primes $\mathfrak{p}$ that split completely in $K(\sqrt[m]{E})$ are equidistributed over $\mathrm{Ext}(Cl, \langle \zeta_m \rangle)$. Note that $\mathrm{Ext}(Cl, \langle \zeta_m \rangle)$ is a non-trivial group whenever $\gcd(m, \#Cl) > 1$.

If we no longer require that $K$ contains the $m$-th roots of unity, two problems arise. First of all, we need an extension of $\mathfrak{p}$ to $K(\zeta_m)$ in order to map $A_\mathfrak{p}/A_\mathfrak{p}^m$ canonically into $\langle \zeta_m \rangle$. On the other hand, Kummer theory now shows that $\mathrm{Hom}(W/EK^{*m}, \langle \zeta_m \rangle)$ contains a subgroup isomorphic to $\mathrm{Gal}(K(\zeta_m, \sqrt[m]{W})/K(\zeta_m, \sqrt[m]{E}))$. The extension $K(\zeta_m, \sqrt[m]{W})$ is not necessarily abelian over $K$, so Artin symbols of primes $\mathfrak{p}$ are no longer uniquely determined in this extension: we only have Frobenius symbols at primes lying over $\mathfrak{p}$. The ambiguity on both sides is circumvented by considering extensions $\mathcal{E}_\mathfrak{P}$ depending on primes $\mathfrak{P}$ lying over $\mathfrak{p}$ in $K(\zeta_m)$. The extension class of $\mathcal{E}_\mathfrak{p}$ now corresponds to a conjugacy class of Frobenius symbols. Still, the essential feature that the extension class of $\mathcal{E}_\mathfrak{p}$ is determined by the splitting behaviour in a normal extension $M$ of $K$ is preserved. In the terminology of the previous section, we say that the structure of $\mathcal{E}_\mathfrak{p}$ for variable $\mathfrak{p}$ is governed by $M$, or that $M$ is a *governing field* for the extension structure. In particular, we obtain a precise answer to Cornell's question: the primes $\mathfrak{p} \nmid m$ that split completely in $M/K$ are precisely those primes $\mathfrak{p}$ for which $K$ has a cyclic extension of degree $m$ that is totally and only ramified at $\mathfrak{p}$.

More generally, we can take $B_\mathfrak{p} = \ker[C_{\mathfrak{d}\mathfrak{p}} \to C_\mathfrak{d}]$ for an arbitrary conductor $\mathfrak{d}$ and try to generalize the preceding theorem to extensions of the type

$$0 \longrightarrow B_\mathfrak{p}/B_\mathfrak{p}^m \longrightarrow C_{\mathfrak{d}\mathfrak{p}}/B_\mathfrak{p}^m \longrightarrow C_\mathfrak{d} \longrightarrow 0. \tag{2.5}$$

The results tend to be much weaker than for $\mathfrak{d} = 1$. This is due to the fact that the 'arithmetical extensions' (2.5) have additional structure coming from the primes in $\mathfrak{d}$ that arbitrary extensions need not share. For instance, we know that the inertia groups in $C_\mathfrak{d}$ at the primes in $\mathfrak{d}$ are isomorphic images of the corresponding inertia groups in $C_{\mathfrak{d}\mathfrak{p}}/B_\mathfrak{p}^m$. This imposes a certain partial splitting condition on the extensions (2.5) that is most conveniently described by considering ray class groups as factor groups of the *idèle group* $J$ of $K$.

The idèle group of $K$ is the restricted product

$$J = \prod_\mathfrak{p}{}' K_\mathfrak{p}^*$$

of the multiplicative groups of the completions $K_\mathfrak{p}$ at the finite and infinite primes $\mathfrak{p}$ of $K$. The restriction is that all but finitely many coordinates of an element $x \in J$ lie in the unit group $U_\mathfrak{p}$ of the ring of integers of $K_\mathfrak{p}$. The group $K^*$ is diagonally embedded into $J$, and the factorgroup $C = J/K^*$ is the *idèle class group* of $K$.

For finite $\mathfrak{p}$, the unit element $1 \in K_\mathfrak{p}^*$ has a local base of open subgroups $U_\mathfrak{p}^{(k)} = 1 + \mathfrak{p}^k$ $(k > 0)$ in the topology on $K_\mathfrak{p}^*$. We set $U_\mathfrak{p}^{(0)} = U_\mathfrak{p}$. For archimedean $\mathfrak{p}$ we let $U_\mathfrak{p}^{(0)} = K_\mathfrak{p}^*$ and, in case $\mathfrak{p}$ is real, $U_\mathfrak{p}^{(1)} = K_{\mathfrak{p},>0}$. With this notation, a subgroup $H$ of $J$ is open in the restricted product topology if and only if there exists a cycle $\mathfrak{f} = \prod \mathfrak{p}^{n(\mathfrak{p})}$ such that $H$ contains the subgroup

$$W_\mathfrak{f} = \prod_\mathfrak{p} U_\mathfrak{p}^{(n(\mathfrak{p}))}. \tag{2.6}$$

The open subgroups of the idèle class group $C$ are those subgroups that contain the homomorphic image $D_\mathfrak{f}$ of $W_\mathfrak{f}$ for some $\mathfrak{f}$. A straightforward computation shows that there is an isomorphism

$$C/D_\mathfrak{f} \xrightarrow{\sim} \mathcal{I}(\mathfrak{f})/\mathcal{S}(\mathfrak{f})$$

that sends the residue class of a prime element $\pi_\mathfrak{p} \in K_\mathfrak{p}^* \subset J$ in $C/D_\mathfrak{f}$ to the class of the finite prime $\mathfrak{p}$ when $\mathfrak{p} \nmid \mathfrak{f}$. It follows that each class of ideal groups corresponding to an abelian extension $L/K$ gives rise to an open subgroup $D$ of $C$. If the ideal group has a representative modulo $\mathfrak{f}$, then $D_\mathfrak{f}$ is contained in $D$. The conductor of the ideal group is the smallest cycle $\mathfrak{f}$ for which $D_\mathfrak{f}$ is contained in the corresponding open subgroup of $C$.

In its idèlic form, class field theory can be formulated as the statement that there is an inclusing reversing bijection between the set of open subgroups of the idèle class group

$C$ of $K$ and the set of abelian extensions of $K$ (Chevalley, 1942). The open subgroup corresponding to $L/K$ is the norm subgroup $N_{L/K}C_L$ of $C_K$. The exponent $n(\mathfrak{p})$ to which a finite prime $\mathfrak{p}$ occurs in the conductor $\mathfrak{f}_{L/K}$ can be computed in a local extension $L_\mathfrak{q}/K_\mathfrak{p}$ at $\mathfrak{p}$. It is the smallest non-negative integer $k$ for which $U_\mathfrak{p}^{(k)} \subset N_{L_\mathfrak{q}/K_\mathfrak{p}}[U_\mathfrak{q}]$.

Returning to our sequence (2.5), we see that there is a concise way of giving the additional structure of such extensions: the canonical map $f : J \to C_\mathfrak{d}$ from the idèle group $J$ of $K$ onto $C_\mathfrak{d}$ factors via $C_{\mathfrak{d}\mathfrak{p}}/B_\mathfrak{p}^m$. This is not necessarily true for arbitrary extensions of $C_\mathfrak{d}$ with $B_\mathfrak{p}/B_\mathfrak{p}^n$, and the obstruction to this 'lifting property' exists only for the components of $J$ at primes that are real or divide $\mathfrak{d}$. The presence of arithmetical obstructions leads us to introduce a new type of extension groups that classify group extensions together with a lift of a given homomorphism. Section 3 of this thesis defines such groups, derives some of their fundamental properties and shows their relation to the ordinary Ext-groups (3.1–3.4). It contains only homological algebra, and furnishes the technical basis for the main section of the next chapter, section 5.

Theorem 5.6 is the main theorem of chapter II. It is a fairly general result on the extensions (2.5) in terms of our generalized extension groups. The main characteristic is that there always exists a normal extension that governs the structure of ray class group extensions. We show that for special choices of the parameters and under additional assumptions concerning roots of unity, special cases as the theorem stated above are obtained (5.11, 5.12). It turns out that it is not easy to determine in general whether the field extensions occurring in our theorem are non-trivial, and whether the homomorphism whose existence is given by the theorem is in fact an isomorphism. The investigation of these matters leads to purely field theoretic questions that can be solved using some not too well known results on radical extensions (5.13). A separate section preceding section 5 is devoted to an exposition of these results.

The final section of chapter II is concerned with density statements for the set of primes that give rise to some fixed extension type of ray class groups (6.1, 6.3). The main ingredients are the results from section 5 and the theorems from field theory given in section 4. In particular, it gives a precise answer to the question of Cornell we mentioned before. In more general situations, the result becomes less precise (6.7).

So far, our treatment of the splitting behaviour of exact sequences involving ray class groups has been purely algebraic. The fact that they can be thought of as representing certain Galois groups is the underlying motivation, but it is actually never used in the proofs. This is no longer the case if one takes for the prime $\mathfrak{p}$ in (2.5) not a prime of $K$, but a prime of a subfield $k$ of $K$. In that case, $\mathfrak{p}$ factors in $K$ as a product of primes. Some information is given by a formal extension 7.2 of the results in section 5 to include 'multi-prime extensions', but this is less than we want.

More precisely, one considers for all primes $\mathfrak{p} \nmid \mathfrak{d}$ of the subfield $k \subset K$ the maximal abelian extension $L(\mathfrak{p}) = L(\mathfrak{p}, \mathfrak{d}, m)$ of $K$ of conductor dividing $\mathfrak{d}\mathfrak{p}$ in which the ramification indices at primes over $\mathfrak{p}$ in $L(\mathfrak{p})$ divide $m$. Then $L(\mathfrak{p})$ contains the ray class field $H_{\mathfrak{d}}$ of $K$ of conductor $\mathfrak{d}$ and there is an exact sequence

$$0 \longrightarrow \mathrm{Gal}(L(\mathfrak{p})/H_{\mathfrak{d}}) \longrightarrow \mathrm{Gal}(L(\mathfrak{p})/K) \longrightarrow \mathrm{Gal}(H_{\mathfrak{d}}/K) \longrightarrow 0.$$

The group $\mathrm{Gal}(L(\mathfrak{p})/H_{\mathfrak{d}})$ is generated by the inertia groups of the primes in $\mathfrak{p}$, and in terms of ray class groups this is exactly the sequence (2.5). If the extensions for primes $\mathfrak{p}_1$ and $\mathfrak{p}_2$ of $k$ are isomorphic, there is an isomorphism $\mathrm{Gal}(L(\mathfrak{p}_1)/K) \xrightarrow{\sim} \mathrm{Gal}(L(\mathfrak{p}_2)/K)$ of Galois groups that respects the projection onto $\mathrm{Gal}(H_{\mathfrak{d}}/K)$ and maps inertia groups at primes over $\mathfrak{p}_1$ to inertia groups of primes over $\mathfrak{p}_2$. The special conditions about the lifting of decomposition groups in section 5 even imply a much stronger equivalence: they give a Galois isomorphism

$$L(\mathfrak{p}_1) \otimes_K K_{\mathfrak{q}} \xrightarrow{\sim} L(\mathfrak{p}_2) \otimes_K K_{\mathfrak{q}}$$

of algebras over the local field $K_{\mathfrak{q}}$ for a finite number of primes $\mathfrak{q}$ of $K$ that can be prescribed.

If $K/k$ is Galois and $\mathfrak{d}$ is Galois invariant, the fields $L(\mathfrak{p})$ and $H_{\mathfrak{d}}$ are Galois over $k$ and it is natural to require that we have isomorphisms for $\mathrm{Gal}(L(\mathfrak{p})/k)$ and for algebras over the local fields $k_{\mathfrak{q}}$. Note however that these are isomorphisms of not necessarily abelian groups, and that this introduces a behaviour of primes $\mathfrak{p}$ that is not in an obvious way described by an element of an Ext-group. Of course, this does not imply that the purely algebraic approach of chapter II cannot be made to work. One needs that all isomorphisms of Galois groups over $K$ are in fact isomorphisms over $k$, and this just means that they have the same extension with $\mathrm{Gal}(K/k)$. Such extensions are described by canonical classes, but so far it is not clear how the algebraic formalism can force a correspondence of canonical classes. We therefore use an approach that explicitly constructs the isomorphism $\mathrm{Gal}(L(\mathfrak{p}_1)/k) \xrightarrow{\sim} \mathrm{Gal}(L(\mathfrak{p}_2)/k)$. In fact, we slightly redefine the extensions $L(\mathfrak{p})$ so as to have Kummer theory at our disposal (7.4). This does not essentially change the situation as the former extensions are contained in extensions of the new type and conversely. Our explicit construction can be performed if there exists an element $x$ of $K$ that satisfies various local conditions. If $\mathfrak{P}_1$ and $\mathfrak{P}_2$ are primes over $\mathfrak{p}_1$ and $\mathfrak{p}_2$ in $K$, and $\pi_1$ and $\pi_2$ are prime elements at these primes in the idèle group $J$ of $K$, the condition requires that $x\pi_1\pi_2^{-1}$ be contained in a certain open subgroup of $J$. By class field theory, this simply means that $\mathfrak{P}_1$ and $\mathfrak{P}_2$ have the same Artin symbol in a corresponding abelian extension $M$ of $K$, so we once more arrive at a governing field theorem (8.1) for the structure of the extensions $L(\mathfrak{p})/k$. This governing field construction, which is the core of chapter III, can be found in section 8.

The last chapter of this thesis contains an application of our governing field results to prove a conjecture of Cohn and Lagarias concerning the 8-rank of the (strict) class group of a quadratic order $\mathcal{C}(\Delta)$. We discuss these conjectures in the remaining part of this section.

For any integer $\Delta \equiv 0,1 \bmod 4$ that is not a perfect square, the *quadratic order of discriminant* $\Delta$ is the ring

$$\mathcal{O}_\Delta = \mathbb{Z}[\frac{\Delta + \sqrt{\Delta}}{2}].$$

It is a subring of finite index $f$ in the ring of integers $\mathcal{O}$ of the quadratic field $\mathbb{Q}(\sqrt{\Delta})$, and there exists an integer $d$ such that

$$\Delta = f^2 d \qquad \text{and} \qquad \mathcal{O}_\Delta = \mathbb{Z} + f \cdot \mathbb{Z}[\frac{d + \sqrt{d}}{2}] = \mathbb{Z} + f \cdot \mathcal{O}.$$

The integer $d$ in this equation is the discriminant of the quadratic field $\mathbb{Q}(\sqrt{\Delta})$. It is the integer without odd square factors that satisfies $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{\Delta})$ and either $d \equiv 1 \bmod 4$ or $d \equiv 8,12 \bmod 16$. Discriminants $\Delta$ that have $f = 1$ are called *fundamental discriminants*. The order $\mathcal{O}_\Delta$ is said to be real quadratic if $\Delta > 0$, and imaginary quadratic if $\Delta < 0$.

The *strict ideal class group* $\mathcal{C}(\Delta)$ of the quadratic order $\mathcal{O}_\Delta$ is defined as the factor group $\mathcal{I}_\Delta / \mathcal{P}_\Delta$, where $\mathcal{I}_\Delta$ is the group of invertible $\mathcal{O}_\Delta$-ideals and $\mathcal{P}_\Delta$ is the group of those principal ideals $\alpha\mathcal{O}_\Delta$ that are generated by an element $\alpha \in \mathbb{Q}(\sqrt{d})$ that has positive norm in $\mathbb{Q}$. Factoring out by the subgroup of *all* principal ideals, one obtains the *ordinary ideal class group*. The strict ideal class group coincides with the ordinary ideal class group for imaginary quadratic orders and for real quadratic orders having a unit of negative norm. In real quadratic orders having units of positive norm only, the kernel of the canonical map from $\mathcal{C}(\Delta)$ onto the ordinary class group has order two and is generated by the class of the ideal $\sqrt{\Delta} \cdot \mathcal{O}_\Delta$. If $f = 1$, then $\Delta = d$ and $\mathcal{C}(\Delta)$ is also known as the *narrow* or *strict* class group of $\mathbb{Q}(\sqrt{d})$. Its order is the *strict class number* of $\mathbb{Q}(\sqrt{d})$.

The class group $\mathcal{C}(\Delta)$ was originally introduced by Gauss as a group of equivalence classes of primitive integral binary quadratic forms of discriminant $\Delta$. It was inspired by old problems concerning the representations of integers by quadratic forms. In Gauss's definition, the *class group of quadratic forms* of discriminant $\Delta$ is the set of $SL_2(\mathbb{Z})$-orbits of primitive quadratic forms $aX^2 + bXY + cY^2 \in \mathbb{Z}[X,Y]$ of discriminant $\Delta = b^2 - 4ac$. Primitivity means that $\gcd(a,b,c) = 1$, and $SL_2(\mathbb{Z})$ acts on the right on the set of forms $F = aX^2 + bXY + cY^2$ by

$$F \cdot \begin{pmatrix} u & v \\ w & x \end{pmatrix} = F(uX + vY, wX + xY).$$

If $\Delta < 0$, one restricts to quadratic forms in which the coefficient $a$ of $X^2$ is positive. The set of orbits of quadratic forms of discriminant $\Delta$ has a group structure since there is a

natural bijection to $C(\Delta)$ that is given by

$$[aX^2 + bXY + cY^2] \longleftrightarrow [\mathbf{Z} \cdot a + \mathbf{Z} \cdot \frac{b + \sqrt{\Delta}}{2}]$$

when $a > 0$, and

$$[aX^2 + bXY + cY^2] \longleftrightarrow [(\mathbf{Z} \cdot a + \mathbf{Z} \cdot \frac{b + \sqrt{\Delta}}{2}) \cdot \sqrt{\Delta}]$$

when $a < 0$ and $\Delta > 0$.

If $p$ is a rational prime number and $F = aX^2 + bXY + cY^2$ is a quadratic form that assumes the value $p$ on $\mathbf{Z} \times \mathbf{Z}$, then $F$ is said to *represent* $p$. Replacing $F$ by an equivalent form when necessary, one can assume that $F(1,0) = p$. Then $\Delta = b^2 - 4pc$, so $\Delta$ is a square modulo $p$ and the middle coefficient of $F$ is a square root of $\Delta$ modulo $p$. From the bijection given above, one sees that the ideal class corresponding to the class of $F$ contains an ideal of norm $p$. Conversely, an ideal of norm $p$ gives rise to a quadratic form that represents $p$ in the corresponding class of quadratic forms.

The description of $C(\Delta)$ by means of quadratic forms is mainly useful for computational purposes [23]. From a theoretical point of view, the ideal class description is usually to be preferred.

Being a finite abelian group, $C(\Delta)$ can be written as a product of a group of odd order and a 2-group, its *2-primary part*. The group of odd order is not easily described as a function of $\Delta$, and not very much has been proved about its structure. The 2-primary part, however, turns out to be a manageable object that has been studied extensively. Like any finite abelian 2-group, it can be characterized up to isomorphism by giving its $2^k$*-rank* for $k \geq 1$. The $2^k$-rank of a finite abelian group $G$ is defined as the number of factors 2 in the index $[G^{2^{k-1}} : G^{2^k}]$. Thus, the $2^k$-rank of a product of cyclic groups of orders $m_1, m_2, ..., m_r$ is exactly the number of $i$ for which $m_i$ is divisible by $2^k$. It is obvious that $r_{2^{k+1}} \leq r_{2^k}$, and that $r_{2^k} = 0$ for $k$ sufficiently large.

The computation of the 2-rank of the class group $C(\Delta)$ goes back to Gauss. Taking squares in $C(\Delta)$, one obtains an exact sequence

$$0 \longrightarrow C(\Delta)_2 \longrightarrow C(\Delta) \xrightarrow{\square} C(\Delta) \longrightarrow C(\Delta)/C(\Delta)^2 \longrightarrow 0,$$

which shows that the order of $C(\Delta)/C(\Delta)^2$ equals the order of the 2-torsion subgroup $C(\Delta)_2$. Elements in $C(\Delta)_2$ are called *ambiguous forms* or *ambiguous ideal classes*. Gauss determined their number and showed that the 2-rank of $C(\Delta)$ is equal to or one or two less than the number of distinct prime factors in the discriminant $\Delta$.

The same result can be obtained by *genus theory*, which describes the factor group $C(\Delta)/C(\Delta)^2$ as a Galois group $\mathrm{Gal}(H_2/K)$ for a field $H_2$ that is abelian over $\mathbf{Q}$. Combined with the previous approach, it leads to a description of the 4-rank $r_4$ since

$$r_4 = \dim_{\mathbf{F}_2}(\ker [C(\Delta)_2 \longrightarrow C(\Delta)/C(\Delta)^2]).$$

For the 8-rank, the corresponding equation is

$$r_8 = \dim_{\mathbf{F}_2}(\ker[C(\Delta)_2 \longrightarrow C(\Delta)/C(\Delta)^4]), \tag{2.7}$$

so one would like to describe the extension $H_4/K$ that has $C(\Delta)/C(\Delta)^4$ as its Galois group. The field $H_4$ is normal, but not necessarily abelian over $\mathbf{Q}$, and its generators are not as easily given as for $H_2$. However, sufficient information can sometimes be obtained by looking at an appropriate subfield.

As an example, take for $C(\Delta)$ the class group of the imaginary quadratic field $K = \mathbf{Q}(\sqrt{-p})$, with $p > 2$ a rational prime number. If $p \equiv 3 \bmod 4$, the discriminant of $\mathbf{Q}(\sqrt{-p})$ is prime and its class number is odd. Therefore, we shall further assume that $p \equiv 1 \bmod 4$ and study the 2-primary part of $C = C(-4p)$. In this case we have $H_2 = \mathbf{Q}(\mathrm{i}, \sqrt{p})$, so $r_2 = 1$ and the 2-primary part of $C$ is cyclic.

The field $H_4$ is an unramified extension of degree $\leq 2$ of $H_2$, and it is normal over $\mathbf{Q}(\mathrm{i})$. It cannot be cyclic of order 4 over $\mathbf{Q}(\mathrm{i})$ because there is a ramification group at $p$ in $\mathrm{Gal}(H_4/\mathbf{Q}(\mathrm{i})$ of order 2 that is not $\mathrm{Gal}(H_4/H_2)$. Consequently, $H_4$ is a Galois extension of $\mathbf{Q}(\mathrm{i})$ with a group that is an *elementary abelian* 2-group. Since $H_4$ is unramified over $H_2 = \mathbf{Q}(\mathrm{i}, \sqrt{p})$, it must be a subfield of the ray class field of $\mathbf{Q}(\mathrm{i})$ modulo $(p)$. As the class group $Cl$ is trivial for $\mathbf{Q}(\mathrm{i})$, the ray class group of $\mathbf{Q}(\mathrm{i})$ modulo $(p)$ is given by (2.3) as

$$\mathcal{T} = (k_\pi^* \times k_{\bar{\pi}}^*)/\mathrm{im}\langle \mathrm{i} \rangle$$

Here $k_\pi$ and $k_{\bar{\pi}}$ are the residue class fields at the primes $\pi$ and $\bar{\pi}$ over $p$ in $\mathbf{Q}(\mathrm{i})$. As $\mathrm{Gal}(H_4/\mathbf{Q}(\mathrm{i}))$ is of exponent 2, it is the surjective image of $\mathcal{T}/\mathcal{T}^2$. It is clear that $\#(\mathcal{T}/\mathcal{T}^2) \leq 4$. We thus have

$$\begin{aligned} r_4 = 1 \iff [H_4 : \mathbf{Q}(\mathrm{i}, \sqrt{p})] = 2 &\iff [H_4 : \mathbf{Q}(\mathrm{i})] = 4 \\ &\implies \#(\mathcal{T}/\mathcal{T}^2) = 4 \\ &\iff \mathrm{i} \text{ is a square in } k_\pi \text{ and } k_{\bar{\pi}} \\ &\iff -1 \text{ is a 4-th power modulo } p \\ &\iff p \text{ splits completely in } \mathbf{Q}(\sqrt[4]{-1}) = \mathbf{Q}(\zeta_8). \end{aligned}$$

The converse is also true, since $\#(\mathcal{T}/\mathcal{T}^2) = 4$ implies that there is a $V_4$-extension $F$ of $\mathbf{Q}(\mathrm{i})$ containing $\mathbf{Q}(\mathrm{i}, \sqrt{p})$ that is ramified at $\pi$ and $\bar{\pi}$ only. The ramification indices at these primes cannot exceed two since the ramification is tame, so $F$ is a normal unramified extension of degree 4 of $\mathbf{Q}(\sqrt{-p})$, hence equal to $H_4$.

Assume now that $r_4 = 1$, i.e. $p \equiv 1 \bmod 8$. In order to find the 8-rank of $C$, we use the fact that the prime ideal $\mathfrak{p}_2$ in $\mathbf{Q}(\sqrt{-p})$ that lies over 2 is non-principal—there is no element of norm 2—but its square is. As the 2-torsion subgroup of $C$ is cyclic it is generated

by the class $[\mathfrak{p}_2]$. In this case, (2.7) tells us that the order of the cyclic group $C$ is divisible by 8 if and only if there is an element of order 2 that is a 4-th power, and we find

$$\begin{aligned} r_8 = 1 &\iff [\mathfrak{p}_2] \in C^4 \\ &\iff \mathfrak{p}_2 \text{ has a trivial Artin symbol in } C/C^4 \\ &\iff \mathfrak{p}_2 \text{ splits completely in } H_4/\mathbb{Q}(\sqrt{-p}) \\ &\iff (1+\mathrm{i}) \text{ splits completely in } H_4/\mathbb{Q}(\mathrm{i}) \\ &\iff (1+\mathrm{i}) \text{ has a trivial Artin symbol in } T/T^2 \\ &\iff 1+\sqrt{-1} \text{ is a square modulo } p \\ &\iff p \text{ splits completely in } \mathbb{Q}(\zeta_8, \sqrt{1+\mathrm{i}}). \end{aligned}$$

Note that the choice of $\sqrt{-1}$ modulo $p$ in the penultimate condition is irrelevant as the product $(1+\sqrt{-1})(1-\sqrt{-1}) = 2$ is a square modulo $p$. We have found a characterization of the primes for which 8 divides the class number of $\mathbb{Q}(\sqrt{-p})$ that goes back to Barrucand and Cohn [1].

Summarizing, we see that the 2-, 4- and 8-ranks of the class group of $\mathbb{Q}(\sqrt{-p})$ only depend on the splitting behaviour of $p$ in the extension $\mathbb{Q}(\zeta_8, \sqrt{1+\mathrm{i}})/\mathbb{Q}$. This means that $\mathbb{Q}(\zeta_8, \sqrt{1+\mathrm{i}})$ is a governing field for the 2-, 4- and 8-ranks of the class group of $\mathbb{Q}(\sqrt{-p})$.

The existence of a governing field in the example above directly implies that the set of primes $p$ for which the ranks $r_2$, $r_4$ and $r_8$ of the class group of $\mathbb{Q}(\sqrt{-p})$ have prescribed values has a natural density inside the set of all prime numbers. More precisely, the Čebotarev density theorem shows that $r_2 = 1$ for $1/2$ of the primes, $r_4 = 1$ for $1/4$ of the primes and $r_8 = 1$ for $1/8$ of the primes.

This example rises two natural questions. First, one might ask whether there exist governing fields that determine the 16-rank or even higher 2-power ranks of $\mathbb{Q}(\sqrt{-p})$. Secondly, one might wonder whether the situation above is special for the fields $\mathbb{Q}(\sqrt{-p})$, or that one parameter families of fields as $\mathbb{Q}(\sqrt{2p})$ exhibit a similar behaviour. More generally, one can pose the question for the class groups $C(Dp)$ for some fixed $D$ and variable primes $p$ for which $Dp \equiv 0, 1 \bmod 4$.

In their general form, the Cohn-Lagarias conjectures [9] assert that the answer to both questions is positive.

**2.8 Conjecture (Cohn-Lagarias).** *Let $D \not\equiv 2 \bmod 4$ be an arbitrary integer, and $w$ a power of 2. Then there exists a normal extension $M/\mathbb{Q}$ such that the $w$-rank of the class group $C(Dp)$ for odd primes $p \nmid D$ satisfying $Dp \equiv 0, 1 \bmod 4$ only depends on the Artin class of $p$ in $M/\mathbb{Q}$.*

For $w = 2$, the truth of the conjecture is a direct consequence of Gauss's results: the 2-rank of $C(Dp)$ simply does not depend on $p$. For $w = 4$, the conjecture is true for all

fundamental discriminants $D$ by a result of Rédei and Reichardt [29, 30]. For $w \geq 16$, the conjecture is not even known to hold for a single value of $D$, and so far there is not much evidence supporting it.

The study of the 8-rank of quadratic class groups originated with work of Rédei [31, 32], who proved that for each integral triple $(a, b, c)$ with $a \geq b \geq c \geq 0$, there exist infinitely many real quadratic fields for which $r_2 = a$, $r_4 = b$ and $r_8 = c$. Many papers on the subject have appeared since then. An especially large number of criteria concerning the 8-rank of class groups with cyclic 2-primary part has been derived, usually in terms of the solutions of certain Diophantine equations (E. Brown [3, 4, 5], H. Hasse [13, 14], P. Kaplan [16, 17], H. Koch & W. Zink [20]). A considerable part of the literature still uniquely uses Gauss's early 19-th century terminology of quadratic forms. The governing field approach to the problem starts with the already mentioned paper of Barrucand and Cohn [1]. The most satisfactory results in this direction have been obtained by Morton [25, 26, 27, 28]. The conjecture 2.8 for the 8-rank has been proved by him for special classes of fundamental discriminants $D$. His methods do not furnish an obvious dependence on $D$ of the governing fields that are obtained.

The main result of chapter IV, theorem 10.4, is a slightly sharpened version of the following theorem.

**2.9 Theorem.** *Let $D \not\equiv 2 \bmod 4$ be an arbitrary non-zero integer, and define $K$ by*

$$K = \mathbb{Q}(\sqrt{q} : \ q \mid D \text{ is a fundamental prime power discriminant}).$$

*Then the isomorphism type of $C(Dp)/C(Dp)^8$ for primes $p$ satisfying $Dp \equiv 0, 1 \bmod 4$ only depends on the Frobenius class of $p$ in the maximal abelian extension of $K$ that is unramified outside $2D \cdot \infty$ and has a Galois group of exponent 2 over $K$.*

Note that we obtain the governing field from our example if we set $D = -4$.

The idea in the proof of 2.9 is that one knows the 8-rank of $C(Dp)$ if one knows the structure of $C(Dp)/C(Dp)^4$ and the canonical image of the 2-torsion subgroup $C(Dp)_2$ in $C(Dp)/C(Dp)^4$. Indeed, one can rewrite (2.7) as

$$r_8 = r_2 - \dim_{\mathbb{F}_2}(\mathrm{im}[C(Dp)_2 \longrightarrow C(Dp)/C(Dp)^4]).$$

Just as in the case $D = -4$ considered above, the field $H(p)$ that is invariant under $C(Dp)^4$ is abelian of exponent 2 over a field $K_D$ that does not depend on $p$. Moreover, its conductor over $K_D$ equals $\mathfrak{d}p$, where $\mathfrak{d}$ is some fixed cycle depending on $D$. This means that the extensions $H(p)/\mathbb{Q}$ are subextensions of extensions $L(p)/\mathbb{Q}$ that we have studied in chapter III. One deduces that the structure of $C(Dp)/C(Dp)^4$ is determined by the splitting behaviour of $p$ in some governing field. Moreover, the formalism in chapter III

allows us to take into account the local behaviour at a finite set of rational primes. In section 9, we describe class groups of quadratic orders by class field theory and reformulate classical results on their 2-torsion subgroup in order to show that the 2-torsion of $C(Dp)$ comes from the inertia groups of primes over $D$ and $\infty$ (lemma 9.8). We can then use the governing field theorem 8.1 for the extensions $L(p)$ with local conditions at the primes in $D \cdot \infty$ to prove that there exists a governing field for the structure of $C(Dp)/C(Dp)^4$ plus the canonical image of the 2-torsion. By what we said above, this gives the Cohn-Lagarias conjecture for the 8-rank.

If $D$ has only few distinct prime factors, one can often find more precise descriptions of the 8-rank than that from 2.9. For instance, the argument we gave for $D = -4$ is easily adapted to treat the case of fundamental discriminants that have cyclic 2-class groups [35]. The situation is more complicated when $r_2 > 1$. To give an idea of the methods that can be employed for small $D$, we conclude this chapter by an example that shows how to compute the 8-rank for $D = -21$, using explicit descriptions of $C(Dp)/C(Dp)^4$ and $C(Dp)_2$ as sketched above. It proves a conjecture based on computational evidence in [9]. See also [28].

**2.10 Theorem.** *Let $p \equiv 3 \bmod 4$ be a prime number. Then the 4-rank of $C(-21p)$ equals 1 unless $p = 7$ or $\left(\frac{p}{3}\right) = -\left(\frac{p}{7}\right) = 1$, when it is 0. The 8-rank of $C(-21p)$ is 1 if and only if $p$ splits completely in one of following fields:*

$$M_1 = \mathbb{Q}(\sqrt{-3}, \sqrt{7}, \sqrt{2 - \sqrt{-3}})$$
$$M_2 = \mathbb{Q}(\sqrt{3}, \sqrt{7}, \sqrt{2(7 + \sqrt{21})})$$
$$M_3 = \mathbb{Q}(\sqrt{-3}, \sqrt{-7}, \sqrt{-3 + 2\sqrt{-3}}).$$

**Proof.** Write $C$ for $C(-21p)$. For $p = 3$ and $p = 7$ the group $C$ is cyclic of order respectively 4 and 2, so the theorem holds for these values of $p$. We will further assume $p > 7$.

The discriminant $-21p$ of $K = \mathbb{Q}(\sqrt{-21p})$ has three distinct prime factors, so according to standard theory that will be recalled in section 9 one has $r_2 = 2$. It also gives $H_2 = \mathbb{Q}(\sqrt{-3}, \sqrt{-7}, \sqrt{-p}) = K(\sqrt{-3}, \sqrt{-7})$ and

$$C/C^2 \cong \mathrm{Gal}(K(\sqrt{-3}, \sqrt{-7})/K).$$

The 2-torsion group $C_2$ is also a Klein four group $V_4$. As there are no elements in $\mathcal{O}_K$ of norm 3, 7 or 21, the primes $\mathfrak{p}_3$ and $\mathfrak{p}_7$ in $K$ lying over 3 and 7 have order 2 in the class group and generate $C_2$. The 4-rank of $C$ equals

$$r_4 = \dim_{\mathbb{F}_2}(\ker[C_2 \longrightarrow C/C^2]).$$

As $\mathfrak{p}_3$ is inert in $K(\sqrt{-7})/K$, it is not in this kernel and one has $r_4 \leq 1$.

Suppose first that $\left(\frac{7}{p}\right) = 1$, so $p$ splits in $\mathbb{Q}(\sqrt{7})$. In this case, $\mathfrak{p}_7$ splits completely in $H_2 = K(\sqrt{-3}, \sqrt{-p})$, so $[\mathfrak{p}_7]$ generates $\ker[\mathcal{C}_2 \to \mathcal{C}/\mathcal{C}^2])$ and $r_4 = 1$. We see that

$$r_8 = \dim_{\mathbb{F}_2}(\ker[\mathcal{C}_2 \longrightarrow \mathcal{C}/\mathcal{C}^4])$$

equals 1 if and only if $\mathfrak{p}_7$ splits completely in $H_4/K$. This splitting behaviour can be treated by class field theory over a field $F = K_{-21} = \mathbb{Q}(\sqrt{-3}, \sqrt{-7})$ that does not depend on $p$.

The field $F$ is a totally complex biquadratic field of class number one. Its fundamental unit $\epsilon = (\sqrt{-3} + \sqrt{-7})/2$ has a square $(-5 - \sqrt{21})/2$ that is a fundamental unit in the real subfield $\mathbb{Q}(\sqrt{21})$. As $1 - \epsilon^2 = (7 + \sqrt{21})/2$ is an element of norm 7 in $\mathbb{Q}(\sqrt{21})$, we see that $(1 - \epsilon)$ generates a prime ideal over 7 in $F$. We arrive at

$$r_8 = 1 \iff (1 - \epsilon) \text{ splits completely in } H_4/F.$$

As $H_2 = F(\sqrt{-p})$ and $H_4/H_2$ is unramified, $H_4/F$ is a $V_4$-extension of conductor $p$. By (2.3), the ray class group modulo $p$ over $F$ is isomorphic to

$$\mathcal{T} = (\mathcal{O}_F/p\mathcal{O}_F)^*/\langle -1, \epsilon\rangle \cong (\mathbb{F}_{p^2}^* \times \mathbb{F}_{p^2}^*)/\langle -1, \epsilon\rangle.$$

We have $\mathcal{T}/\mathcal{T}^2 \cong \mathrm{Gal}(H_4/F)$, so the last equivalence can be rewritten as

$$r_8 = 1 \iff 1 - \epsilon \text{ is a square in } \mathcal{O}_F/p\mathcal{O}_F \cong \mathbb{F}_{p^2} \times \mathbb{F}_{p^2}.$$

If $p$ splits in $\mathbb{Q}(\sqrt{-3})$, then we can take the norm to this field and find

$$\begin{aligned} r_8 = 1 &\iff N_{F/\mathbb{Q}(\sqrt{-3})}(1 - \epsilon) = 2 - \sqrt{-3} \text{ is a square in } \mathbb{F}_p \\ &\iff p \text{ splits completely in } M_1/\mathbb{Q}. \end{aligned}$$

If this is not the case, $p$ splits in $\mathbb{Q}(\sqrt{21})$ and taking the norm $N_{F/\mathbb{Q}(\sqrt{21})}$ gives

$$\begin{aligned} r_8 = 1 &\iff N_{F/\mathbb{Q}(\sqrt{21})}(1 - \epsilon) = (7 + \sqrt{21})/2 \text{ is a square in } \mathbb{F}_p \\ &\iff p \text{ splits completely in } M_2/\mathbb{Q}. \end{aligned}$$

This proves the theorem for the primes that satisfy $\left(\frac{7}{p}\right) = 1$.

Suppose now that $\left(\frac{7}{p}\right) = -1$, so that $p$ splits in $\mathbb{Q}(\sqrt{-7})/\mathbb{Q}$. Then $\mathfrak{p}_7$ is inert in $K(\sqrt{-p})/K$, so $[\mathfrak{p}_3]$ and $[\mathfrak{p}_7]$ are both non-trivial in $\mathcal{C}/\mathcal{C}^2$. In order for the 4-rank to be non-zero the only other element $[\mathfrak{p}_3\mathfrak{p}_7]$ of order 2 must be trivial in $\mathcal{C}/\mathcal{C}^2$. As $\mathfrak{p}_3\mathfrak{p}_7$ is equivalent to the prime $\mathfrak{r} = (\sqrt{-21p})\mathfrak{p}_3^{-1}\mathfrak{p}_7^{-1}$ over $p$ in $\mathcal{C}$, we now have

$$\begin{aligned} r_4 = 1 &\iff \mathfrak{r} \text{ splits completely in } K(\sqrt{-3}, \sqrt{-7})/K \\ &\iff p \text{ splits completely in } \mathbb{Q}(\sqrt{-3}, \sqrt{-7}). \end{aligned}$$

As before, we derive that

$$r_8 = 1 \iff \mathfrak{r} \text{ splits completely in } H_4/K.$$

This time, we have to look at the splitting behaviour of a prime lying over $p$. As such primes are ramified in $H_4/F$ we cannot use the method above. Instead, we will use explicit generators for $H_4$. We can further assume that $r_4 = 1$, so $p$ splits in the ring of integers $\mathbb{Z}[\zeta_3]$ of $\mathbb{Q}(\sqrt{-3})$ as $p = \pi\overline{\pi}$.

The decomposition field of $\mathfrak{p}_3$ in $H_4/K$ is quadratic over of $K(\sqrt{7p}) = \mathbb{Q}(\sqrt{-3}, \sqrt{7p})$ and does not contain $\sqrt{-7}$. It follows that $H_4/K(\sqrt{7p})$ is an unramified $V_4$-extension. The norm map $Cl_{K(\sqrt{7p})} \to Cl_{\mathbb{Q}(\sqrt{-3})}$ is trivial, and this implies by class field theory that $\mathrm{Gal}(K(\sqrt{7p})/\mathbb{Q}(\sqrt{-3}))$ acts on $\mathrm{Gal}(H_4/K(\sqrt{7p}))$ by inversion. One deduces that $\mathrm{Gal}(H_4/\mathbb{Q}(\sqrt{-3}))$ is the direct product of $V_4$ and the inertia group of some prime dividing $7p$, i.e. elementary abelian of type $2 \times 2 \times 2$. Using (2.3) once more, we find that $H_4$ is the maximal elementary abelian 2-extension of $\mathbb{Q}(\sqrt{-3})$ of conductor dividing $7p$. It can be given explicitly as

$$H_4 = \mathbb{Q}(\sqrt{-3}, \sqrt{-7}, \sqrt{-p}, \sqrt{\pi(2+\sqrt{-3})}),$$

where the prime element $\pi | p$ in $\mathbb{Z}[\zeta_3]$ has to be chosen such that $\pi(2+\sqrt{-3}) \equiv 1 \bmod 4$. Writing $\pi = a + b\zeta$ and $2 + \sqrt{-3} = 3 + 2\zeta$, one sees that this comes down to $a \equiv 3 \bmod 4$ and $b \equiv 2 \bmod 4$. One obtains

$$\begin{aligned} r_8 = 1 &\iff \mathfrak{r} \text{ splits completely in } H_4/K \\ &\iff \overline{\pi} \text{ splits completely in } \mathbb{Q}(\sqrt{\pi(2+\sqrt{-3})})/\mathbb{Q}(\sqrt{-3}) \\ &\iff \left(\frac{\pi(2+\sqrt{-3})}{\overline{\pi}}\right) = 1. \end{aligned}$$

As $\zeta = \zeta^4$ is a square modulo $\overline{\pi}$, the quadratic character of $\pi$ modulo $\overline{\pi}$ equals that of

$$\bar{\zeta}\pi - \zeta\overline{\pi} = a(\bar{\zeta} - \zeta) = -a\sqrt{-3}.$$

The equation $p = \pi\overline{\pi} = a^2 - ab + b^2$ gives quadratic symbols

$$\left(\frac{p}{a}\right)_{\mathbb{Q}} = \left(\frac{-a}{p}\right)_{\mathbb{Q}} = \left(\frac{-a}{\overline{\pi}}\right)_{\mathbb{Q}(\sqrt{-3})} = 1,$$

so we have

$$\begin{aligned} r_8 = 1 &\iff \left(\frac{\sqrt{-3}(2+\sqrt{-3})}{\overline{\pi}}\right)_{\mathbb{Q}(\sqrt{-3})} = 1 \\ &\iff \left(\frac{\sqrt{-3}(2+\sqrt{-3})}{p}\right)_{\mathbb{Q}} = 1 \\ &\iff p \text{ splits completely in } M_3/\mathbb{Q}. \end{aligned}$$

This finishes the proof of 2.10.

# CHAPTER II

## On the structure of ray class groups

## 3. Generalized group extensions.

In the preceding chapter, we discussed the need for a type of extension groups that classify group extensions admitting the lift of some given homomorphism. In this section we introduce such generalized Ext-groups. Their definition is similar to the definition of the ordinary Ext-groups $\mathrm{Ext}(B,A)$ given in [15] or [24]. Here $\mathrm{Ext}(B,A)$ is defined as a set of isomorphism classes of extensions $0 \to A \to E \to B \to 0$ of $B$ with $A$ in the category of abelian groups, and an explicit addition formula for extensions is written down. We modify this procedure in the following way.

**3.1. Definition.** *Let $A$ be an abelian group and $f : C \to B$ a homomorphism of abelian groups. Then an extension $(E,\phi)$ of $A$ with $f$ is a commutative diagram of abelian groups*

$$\begin{array}{ccccccccc} & & & & & & C & & \\ & & & & & \swarrow_{\phi} & \downarrow{\scriptstyle f} & & \\ 0 & \longrightarrow & A & \longrightarrow & E & \longrightarrow & B & \longrightarrow & 0. \end{array}$$

*Two extensions $(E_1,\phi_1)$ and $(E_2,\phi_2)$ are said to be isomorphic if there exists an isomorphism $j : E_1 \to E_2$ that induces the identity on $A$ and $B$ and satisfies $j \circ \phi_1 = \phi_2$. The set of isomorphism classes of extensions of $A$ with $f$ is denoted by* $\mathrm{Ext}(f;A)$.

When $C = 0$, the set $\mathrm{Ext}(f;A)$ can be identified with the underlying set of the ordinary extension group $\mathrm{Ext}(B,A)$. It turns out that for any $f$, the set $\mathrm{Ext}(f;A)$ can be equipped with a natural abelian group structure such that the natural map $\mathrm{Ext}(f;A) \to \mathrm{Ext}(B,A)$ becomes a group homomorphism.

In order to define a group structure, we first observe that the functor $\mathrm{Ext}(f;-)$ is covariant in its second argument. That is, given $f : C \to B$ and a homomorphism of abelian groups $\alpha : A_1 \to A_2$, there is a natural map $\alpha_* : \mathrm{Ext}(f;A_1) \to \mathrm{Ext}(f;A_2)$ that sends the class of an extension $(E,\phi)$ in $\mathrm{Ext}(f;A_1)$ to the class of the *fibred sum* $(A_2 +_{A_1} E, 0 \oplus \phi)$ in $\mathrm{Ext}(f;A_2)$. Here the fibred sum is defined as

$$A_2 +_{A_1} E = (A_2 \oplus E) \,/\, \big\{(\alpha(a_1), -a_1)\big\}_{a_1 \in A_1}.$$

It is the push-out of $\alpha : A_1 \to A_2$ and the inclusion map $A_1 \to E$.

Analogously, given $A$ and $f_2 : C_2 \to B_2$, a transformation $(\beta,\gamma)$ of $f_1$ to $f_2$—by this we mean a commutative diagram

$$\begin{array}{ccc} C_1 & \xrightarrow{f_1} & B_1 \\ \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \beta} \\ C_2 & \xrightarrow{f_2} & B_2 \end{array}$$

—gives rise to a natural map $\mathrm{Ext}(f_2;A) \to \mathrm{Ext}(f_1;A)$. In this case the class of an extension $(E,\phi)$ in $\mathrm{Ext}(f_2;A)$ is sent to the class of the *fibred product* $\big(E \times_{B_2} B_1, (\phi \circ \gamma, f_1)\big)$ in $\mathrm{Ext}(f_1;A)$. The fibred product is defined by

$$E \times_{B_2} B_1 = \{(e,b_1) \in E \times B_1 : \pi(e) = \beta(b_1)\},$$

where $\pi$ is the homomorphism $E \to B_2$. It is the pull-back of $\pi$ and $\beta$.

In order to define the sum of the classes of two extensions $(E_1,\phi_1)$ and $(E_2,\phi_2)$ in $\mathrm{Ext}(f;A)$, we consider the extension $(E_1 \oplus E_2, \phi_1 \oplus \phi_2)$ of $A \oplus A$ with $f \oplus f : C \oplus C \to B \oplus B$. Transform this to an extension of $A$ with $f$ by subsequently taking (in arbitrary order) the push-out induced by the addition map $\nabla : A \oplus A \to A$ and the pull-back induced by the 'diagonal embedding' $\Delta : f \to f \oplus f$. The class of the resulting extension $\nabla_*\Delta^*(E_1 \oplus E_2, \phi_1 \oplus \phi_2)$ is the required sum in $\mathrm{Ext}(f;A)$.

**3.2 Proposition.** *Under the definition of addition of extension classes*

$$[(E_1,\phi_1)] \;+\; [(E_2,\phi_2)] \;=\; [\nabla_*\Delta^*(E_1 \oplus E_2, \phi_1 \oplus \phi_2)]$$

*given above, the set* $\mathrm{Ext}(f;A)$ *has a natural abelian group structure. The unit element in the group* $\mathrm{Ext}(f;A)$ *is the class of the split extension* $(A \oplus B, 0 \oplus f)$.

**Proof.** The verification that the addition is well defined on $\mathrm{Ext}(f;A)$ and that it induces an abelian group structure on $\mathrm{Ext}(f;A)$ is essentially the same as the corresponding verification for the ordinary Ext-groups. The latter is written out in detail in [24, III.2], so there is no need to repeat the argument here. □

The following theorem gives some fundamental properties of the groups $\mathrm{Ext}(f;A)$. It uses the fact that the ordinary Ext-functor $\mathrm{Ext}(-,A)$ is the right derived functor of $\mathrm{Hom}(-,A)$.

**3.3 Theorem.** *Let* $A$ *be an abelian group and* $f : C \to B$ *a homomorphism of abelian groups.*

(a) *There is a natural exact sequence*

$$\mathrm{Hom}(B,A) \longrightarrow \mathrm{Hom}(C,A) \longrightarrow \mathrm{Ext}(f;A) \longrightarrow \mathrm{Ext}(B,A) \longrightarrow \mathrm{Ext}(C,A).$$

*Here the first and the last homomorphisms are induced by* $f$, *the second maps* $g \in \mathrm{Hom}(C,A)$ *to the class of the extension* $(A \oplus B,\ (g,f))$ *and the third is the canonical map.*

(b) *If* $f$ *is surjective, there is a canonical isomorphism*

$$\mathrm{Ext}(f;A) \xrightarrow{\sim} \mathrm{Hom}(\ker f, A)$$

*that maps the class of* $(E,\phi)$ *to* $\phi|_{\ker f} : \ker f \to A \subset E$.

(c) *If $f$ is injective and* $\operatorname{cok} f$ *denotes the cokernel of $f$, there is a canonical isomorphism*

$$\operatorname{Ext}(f;A) \xrightarrow{\sim} \operatorname{Ext}(\operatorname{cok} f, A)$$

*that maps the class of $(E,\phi)$ to the class of the extension* $0 \to A \to E/\phi[C] \to \operatorname{cok} f \to 0$.

**Proof.** (a) For exactness at $\operatorname{Ext}(B,A)$, we observe that the upper sequence in the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & E \times_B C & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow & & \downarrow{\scriptstyle f} & & \\ 0 & \longrightarrow & A & \longrightarrow & E & \longrightarrow & B & \longrightarrow & 0. \end{array}$$

is split if and only if there is a retract homomorphism $C \to E \times_B C$. If $\phi : C \to E$ is the composition of this homomorphism with the projection to the first coordinate, this amounts to saying that the lower sequence comes from the element $(E,\phi) \in \operatorname{Ext}(f;A)$.

Exactness at $\operatorname{Ext}(f;A)$: an extension of $A$ with $f$ is split if and only if it is of the form

$$\begin{array}{ccccccccc} & & & & & & C & & \\ & & & & & \swarrow_{g\oplus f} & \downarrow{\scriptstyle f} & & \\ 0 & \longrightarrow & A & \longrightarrow & A \oplus B & \longrightarrow & B & \longrightarrow & 0 \end{array}$$

for some $g \in \operatorname{Hom}(C,A)$. This means exactly that it is the image of the homomorphism $g \in \operatorname{Hom}(C,A)$ in our sequence.

Exactness at $\operatorname{Hom}(C,A)$: a homomorphism $g \in \operatorname{Hom}(C,A)$ gives rise to the trivial element in $\operatorname{Ext}(f;A)$ if and only if there is an isomorphism $\chi : A \oplus B \xrightarrow{\sim} A \oplus B$ that respects the embedding $A \to A \oplus B$ and the projection $A \oplus B \to B$ and satisfies $g \oplus f = \chi \circ (0 \oplus f) \in \operatorname{Hom}(C, A \oplus B)$. Since $\chi(a,b) = (a + h(b), b)$ for some $h \in \operatorname{Hom}(B,A)$, this means exactly that $g = hf$ for some $h \in \operatorname{Hom}(B,A)$.

(b) Let $\chi : \operatorname{Ext}(f;A) \to \operatorname{Hom}(\ker f, A)$ be the given map. Apply $\operatorname{Hom}(-,A)$ to the short exact sequence $0 \to \ker f \to C \to B \to 0$, form the long exact Ext-sequence and compare with the sequence in (a).

$$\begin{array}{ccccccccccc} \operatorname{Hom}(B,A) & \longrightarrow & \operatorname{Hom}(C,A) & \longrightarrow & \operatorname{Ext}(f;A) & \longrightarrow & \operatorname{Ext}(B,A) & \longrightarrow & \operatorname{Ext}(C,A) \\ \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \chi} & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \mathrm{id}} \\ \operatorname{Hom}(B,A) & \longrightarrow & \operatorname{Hom}(C,A) & \longrightarrow & \operatorname{Hom}(\ker f, A) & \longrightarrow & \operatorname{Ext}(B,A) & \longrightarrow & \operatorname{Ext}(C,A) \end{array}$$

By the five lemma, we are done if we can show that $\chi$ makes the diagram commute. For the square to the left of $\chi$, this is immediate from the definition of the map $\operatorname{Hom}(C,A) \to$

$\mathrm{Ext}(f;A)$. For the square to the right, we consider for an extension $(E,\phi)$ of $A$ with $f$ the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ker f & \longrightarrow & C & \xrightarrow{f} & B & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \phi|\ker f} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 0 & \longrightarrow & A & \longrightarrow & E & \longrightarrow & B & \longrightarrow & 0, \end{array}$$

which shows that $E$ is the push-out of $\phi|\ker f$ and $\ker f \to C$. By the explicit description [24, III.3] of $\mathrm{Hom}(\ker f, A) \to \mathrm{Ext}(B,A)$, this implies that the class of $E$ in $\mathrm{Ext}(A,B)$ is the image of $\phi|\ker f$.

As a consequence of the proof, we note that $\chi$ has an inverse $\chi^{-1} : \mathrm{Hom}(\ker f, A) \xrightarrow{\sim} \mathrm{Ext}(f;A)$ that maps $g \in \mathrm{Hom}(\ker f, A)$ to the class of the extension $(A +_{\ker f} C, 0 + \mathrm{id}_C)$ in $\mathrm{Ext}(f;A)$.

(c) By the same argument for $0 \to C \to B \to \mathrm{cok}\, f \to 0$, we obtain

$$\begin{array}{ccccccccccc} \mathrm{Hom}(B,A) & \longrightarrow & \mathrm{Hom}(C,A) & \longrightarrow & \mathrm{Ext}(f;A) & \longrightarrow & \mathrm{Ext}(B,A) & \longrightarrow & \mathrm{Ext}(C,A) \\ \downarrow{\scriptstyle -1} & & \downarrow{\scriptstyle -1} & & \downarrow{\scriptstyle \chi} & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \mathrm{id}} \\ \mathrm{Hom}(B,A) & \longrightarrow & \mathrm{Hom}(C,A) & \longrightarrow & \mathrm{Ext}(\mathrm{cok}\, f, A) & \longrightarrow & \mathrm{Ext}(B,A) & \longrightarrow & \mathrm{Ext}(C,A) \end{array}$$

and we verify that the given map $\chi : \mathrm{Ext}(\mathrm{cok}\, f, A) \to \mathrm{Ext}(f;A)$ makes the diagram commute. For the square to the left of $\chi$, this comes down to the observation that for any $g \in \mathrm{Hom}(C,A)$, the extension $(A \oplus B)/(-g,f)[C]$ of $\mathrm{cok}\, f$ with $A$ is the push-out of $g$ and $f$. For the square to the right, the diagram

$$\begin{array}{ccccccccc} & & & & & & C & & \\ & & & & & \swarrow{\scriptstyle \phi} & \downarrow{\scriptstyle f} & & \\ 0 & \longrightarrow & A & \longrightarrow & E & \longrightarrow & B & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A & \longrightarrow & E/\phi[C] & \longrightarrow & \mathrm{cok}\, f & \longrightarrow & 0 \end{array}$$

shows that $E$ can be viewed as the pull-back of $E/\phi[C] \to \mathrm{cok}\, f$ and $B \to \mathrm{cok}\, f$. This is just the commuting of the square under consideration.

Here the inverse map $\chi^{-1} : \mathrm{Ext}(\mathrm{cok}\, f, A) \xrightarrow{\sim} \mathrm{Ext}(f;A)$ maps the class of an extension $\hat{E}$ in $\mathrm{Ext}(\mathrm{cok}\, f, A)$ to the class of $(\hat{E} \times_{\mathrm{cok}\, f} B, (0,f))$ in $\mathrm{Ext}(f;A)$.

This finishes the proof of 3.3. □

Parts (b) and (c) of the preceding theorem show that the groups $\mathrm{Ext}(f;A)$ are easily expressed in terms of Hom-groups and ordinary Ext-groups in case $f$ is either surjective or injective. In general, one can 'enlarge the domain of $f$' such that (b) becomes applicable. More precisely, the result is as follows.

**3.4 Theorem.** *Let $A$ be an abelian group and $f : C \to B$ a homomorphism of abelian groups. If $F$ is a free abelian group and $f' : C \times F \to B$ is a surjective homomorphism that extends $f$, there is an isomorphism*

$$\mathrm{Ext}(f; A) \xrightarrow{\sim} \mathrm{cok}\left[\mathrm{Hom}(F, A) \xrightarrow{g} \mathrm{Hom}(\ker f', A)\right]$$

*with $g$ induced by the projection $\ker f' \subset C \times F \to F$. Under this isomorphism, the class of an extension $(E, \phi)$ in $\mathrm{Ext}(f; A)$ is mapped to the residue class of $\phi'|_{\ker f'} : \ker f' \to A \subset E$ for an extension $(E, \phi')$ of $f'$ with $A$ that extends $(E, \phi)$.*

**Proof.** Application of the snake lemma to the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & C & \longrightarrow & C \times F & \longrightarrow & F & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f'} & & \downarrow & & \\ 0 & \longrightarrow & B & \longrightarrow & B & \longrightarrow & 0 & & \end{array}$$

furnishes an exact sequence

$$0 \longrightarrow \ker f \longrightarrow \ker f' \longrightarrow F \longrightarrow \mathrm{cok}\, f \longrightarrow 0.$$

Taking homomorphisms to $A$, we obtain

$$0 \longrightarrow \mathrm{Hom}(\mathrm{cok}\, f, A) \longrightarrow \mathrm{Hom}(F, A) \xrightarrow{g} \mathrm{Hom}(\ker f', A)$$

We have an isomorphism $\mathrm{Hom}(\ker f', A) \cong \mathrm{Ext}(f'; A)$ by theorem 3.4(b), and a natural map $\mathrm{Ext}(f'; A) \to \mathrm{Ext}(f; A)$ that is surjective because $F$ is free. We claim that their combination leads to an exact sequence

$$\mathrm{Hom}(\mathrm{cok}\, f, A) \longrightarrow \mathrm{Hom}(F, A) \longrightarrow \mathrm{Hom}(\ker f', A) \longrightarrow \mathrm{Ext}(f; A) \longrightarrow 0.$$

Thus, we have to check which extensions of $f'$ by $A$ lead to the trivial extension of $A$ by $f$. For such extensions, the extension group is the split extension $A \oplus B$ and there exists $g : F \longrightarrow A$ such that the lift $\chi : C \times F \to A \oplus B$ of $f'$ sends $(c, x) \in C \times F$ to $g(x) \oplus f'(c, x)$. From the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ker f' & \longrightarrow & C \times F & \xrightarrow{f'} & B & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle g|\ker f'} & & \downarrow{\scriptstyle \chi} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 0 & \longrightarrow & A & \longrightarrow & A \oplus B & \longrightarrow & B & \longrightarrow & 0, \end{array}$$

we see that this implies that the extension comes from the homomorphism $g : F \longrightarrow A$, and that, conversely, any homomorphism $g : F \longrightarrow A$ gives rise to the trivial extension in $\mathrm{Ext}(f; A)$. □

We conclude this section with a proof of the result on ordinary Ext-groups that was used in the preceding chapter to sketch a proof of theorem 2.4.

**3.5 Theorem.** *Let $B$ be an abelian group and $A$ a cyclic group of order $m$. Denote by $B_m$ the subgroup of $m$-torsion elements of $B$. Then there is an isomorphism*

$$\mathrm{Ext}(B, A) \xrightarrow{\sim} \mathrm{Hom}(B_m, A),$$

*that is functorial in $A$ and $B$ and sends the class of an extension $0 \to A \to E \xrightarrow{\pi} B \to 0$ to the homomorphism $B_m \to A$ that maps $\beta \in B_m$ to $m\pi^{-1}(\beta) \in A \subset E$.*

**Proof.** Choose a free presentation $0 \to R \to F \xrightarrow{f} B \to 0$ of $B$. Standard homology gives the first isomorphism in

$$\begin{aligned}\mathrm{Ext}(B, A) &\cong \mathrm{cok}\,[\mathrm{Hom}(F, A) \to \mathrm{Hom}(R, A)] \\ &\cong \mathrm{cok}\,[\mathrm{Hom}(F/mF, A) \to \mathrm{Hom}(R/mR, A)] \\ &\cong \mathrm{Hom}(\ker\,[R/mR \to F/mF], A).\end{aligned}$$

The second isomorphism is clear from the fact that $A$ is of exponent $m$, for the third isomorphism one should observe that the injectivity of $A$ as a $\mathbf{Z}/m\mathbf{Z}$-module implies that $\mathrm{Hom}(-, A)$ is an exact functor on $\mathbf{Z}/m\mathbf{Z}$-modules.

The snake lemma applied to the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & R & \longrightarrow & F & \longrightarrow & B & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle m} & & \downarrow{\scriptstyle m} & & \downarrow{\scriptstyle m} & & \\ 0 & \longrightarrow & R & \longrightarrow & F & \longrightarrow & B & \longrightarrow & 0 \end{array}$$

shows that we have an isomorphism $B_m \xrightarrow{\sim} \ker\,[R/mR \to F/mF]$ that sends $b \in B_m$ to the residue class of $mf^{-1}(b)$ in $R/mR$. The theorem follows immediately. □

**Other proof of 3.5.** This proof—for $B$ finitely generated—shows that 3.6 is an isomorphism by identifying both groups with the dual of $\mathrm{Hom}(B, A)$.

First take $B = A$. Then $\mathrm{Ext}(A, A)$ and $\mathrm{Hom}(A, A)$ are both cyclic of order $m$, and the kernel of the map $\mathrm{Ext}(A, A) \to \mathrm{Hom}(A, A)$ is just the class of the split extension. It follows that the theorem holds in this case. For the general case, write $t$ for the map in the theorem and consider the diagram

$$\begin{array}{ccc} \mathrm{Ext}(B, A) \otimes_{\mathbf{Z}} \mathrm{Hom}(A, B) & \longrightarrow & \mathrm{Ext}(A, A) \\ \downarrow{\scriptstyle t\otimes \mathrm{id}} & & \downarrow{\scriptstyle t} \\ \mathrm{Hom}(B_m, A) \otimes_{\mathbf{Z}} \mathrm{Hom}(A, B) & \longrightarrow & \mathrm{Hom}(A, A). \end{array}$$

For the upper horizontal arrow we use the fact that $\mathrm{Ext}(-,A)$ is contravariant to define a homomorphism $\mathrm{Ext}(B,A) \to \mathrm{Ext}(A,A)$ for each element $g$ of $\mathrm{Hom}(A,B)$. If $g$ induces the zero map, then $0 \to \ker g \to A \to B$ gives

$$\mathrm{Ext}(B,A) \longrightarrow \mathrm{Ext}(A,A) \xrightarrow{\sim} \mathrm{Ext}(\ker g, A) \longrightarrow 0,$$

so $\mathrm{Ext}(A,A) = \mathrm{Ext}(\ker g, A)$ and $g = 0$. Since $\mathrm{Ext}(B,A)$ and $\mathrm{Hom}(A,B)$ both have order $\#B_m$—for $\mathrm{Ext}(B,A)$ this follows from the case that $B$ is cyclic—we conclude that we have a perfect pairing that identifies $\mathrm{Ext}(B,A)$ with the dual of $\mathrm{Hom}(A,B)$.

It is even easier to verify that the lower horizontal arrow, that sends $f \otimes g$ to the composition $f \circ g \in \mathrm{Hom}(A,A)$, is also a perfect pairing that identifies $\mathrm{Hom}(B_m, A)$ with the dual of $\mathrm{Hom}(A,B)$.

All arrows are functorial, so we are done if we can show that the diagram commutes. Take the class $\mathcal{E}$ of an extension $0 \to A \to E \xrightarrow{\pi} B \to 0$ and a homomorphism $g \in \mathrm{Hom}(A,B)$. Then the image of $\mathcal{E} \otimes g$ in $\mathrm{Ext}(A,A)$ is the extension class of the top row in

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & E \times_B A & \xrightarrow{h} & A & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow & & \downarrow{\scriptstyle g} & & \\ 0 & \longrightarrow & A & \longrightarrow & E & \xrightarrow{\pi} & B & \longrightarrow & 0. \end{array}$$

In $\mathrm{Hom}(A,A)$ this corresponds to the map $a \mapsto mh^{-1}(a)$. Taking the image the other way around, we arrive at the homomorphism $a \mapsto m\pi^{-1}g(a)$. Looking at the diagram, we see that these homomorphisms coincide. □

## 4. Three theorems from field theory

We start with a result that is due to Schinzel [33].

**4.1 Theorem.** *Let $K$ be a field, $m$ a positive integer not divisible by $\mathrm{char}(K)$ and $w$ the number of $m$-th roots of unity in $K$. Let $L$ be the splitting field of $X^m - a$ over $K$ for some $a \in K$. Then one has*

$$L/K \text{ is abelian} \iff a^w \in K^m.$$

**Proof.** If $a^w = b^m$ for some $b \in K$, then $a = \zeta b^{m/w}$ for some $w$-th root of unity $\zeta$ and $L/K$ is a subextension of the abelian extension $K(\sqrt[w]{b}, \zeta_{wm})/K$. It follows that $L/K$ is abelian.

For the converse, take $\sigma \in \mathrm{Gal}(L/K)$ and suppose $\sigma$ acts on a primitive $m$-th root of unity $\zeta_m$ by $\sigma(\zeta_m) = \zeta_m^{k(\sigma)}$. For arbitrary $\tau \in \mathrm{Gal}(L/K)$ and $\alpha \in L$ satisfying $\alpha^m = a$ the assumption that $\mathrm{Gal}(L/K)$ is abelian implies that

$$\frac{\tau\sigma(\alpha)}{\sigma(\alpha)} = \sigma\Big(\frac{\tau(\alpha)}{\alpha}\Big) = \Big(\frac{\tau(\alpha)}{\alpha}\Big)^{k(\sigma)} = \frac{\tau(\alpha^{k(\sigma)})}{\alpha^{k(\sigma)}},$$

so the element $a^{k(\sigma)}/\sigma(\alpha)$ is invariant under all $\tau \in \mathrm{Gal}(L/K)$, whence in $K$. It follows that its $m$-th power $a^{k(\sigma)-1}$ is in $K^m$.

We conclude that $a^v$ is in $K^m$, where $v$ denotes the greatest common divisor of $m$ and all numbers $k(\sigma)-1$, $\sigma \in \mathrm{Gal}(L/K)$. As $\langle \zeta_v \rangle$ is exactly the set of $\mathrm{Gal}(L/K)$-invariant $m$-th roots of unity, we have $v = w$. □

**Remark.** The proof of the implication $\Rightarrow$ in 4.1 can also be phrased in terms of cohomology. If $L/K$ is Galois with group $G$ and $\zeta_m$ is in $L$, Hilbert 90 furnishes an isomorphism

$$(L^{*m} \cap K^*)/K^{*m} \xrightarrow{\sim} H^1(G, \langle \zeta_m \rangle)$$

that sends the class of $\alpha^m \in L^{*m} \cap K^*$ to the class of the cocycle $\tau \mapsto \tau(\alpha)/\alpha$. The proof given above shows that such cocycles are annihilated by $k(\sigma)-1$ when $G = \mathrm{Gal}(L/K)$ is abelian. Alternatively, one can prove directly that $H^1(G, \langle \zeta_m \rangle)$ is annihilated by $k(\sigma)-1$ by observing that the action of $\sigma$ on this group via an inner automorphism of $G$ and via the natural action on $\langle \zeta_m \rangle$ coincide [7, IV 4.3]: the first action is trivial because $G$ is abelian, the second raises to the power $k(\sigma)$, so $k(\sigma)-1$ kills all elements.

Our next result, due to Kneser, is useful in determining the degree of radical extensions of a field $K$. The problem comes down to finding the degree of $K(M)/K$ for subgroups $M$ of the multiplicative group of the separable closure of $K$ that are of finite index over $K^*$. Obviously, one has $[K(M) : K] \leq [M : K^*]$. If $M/K^*$ has exponent $m$ and $K$ contains a primitive $m$-th root of unity, $K(M)/K$ is a Kummer extension and equality holds. On the other hand, it is easily seen that cyclotomic extensions can give rise to strict inequality.

**4.2 Theorem.** *Let $K$ be a field with separable closure $K_{\mathrm{sep}}$, and suppose $M$ is a subgroup of $K_{\mathrm{sep}}^*$ containing $K^*$ such that $[M : K^*] < \infty$. Then one has*

$$[K(M) : K] = [M : K^*]$$

*if and only if the following conditions are satisfied:*

(1) *if $p$ is an odd prime dividing $[M : K^*]$ and $M$ contains a primitive $p$-th root of unity $\zeta_p$, then one has $\zeta_p \in K$;*

(2) *If $\zeta_4$ is a primitive 4-th root of unity and $M$ contains $1 + \zeta_4$, then one has $\zeta_4 \in K$.*

**Proof.** Kneser's original paper [19] has a short proof. See also [18]. □

We give an application of 4.2 that will prove to be useful in section 6. It is a degree computation for certain radical extensions of a number field $K$. For $W$ a subset of a field $K$, we denote by $K(\sqrt[m]{W})$ the extension of $K$ that is obtained by adjoining to $K$ all elements $\alpha$ in an algebraic closure of $K$ for which $\alpha^m \in W$.

**4.3 Proposition.** *Let $K$ be a number field, and $r$ the free rank of the unit group $E$ of its ring of integers. Suppose $l$ is an odd prime, and $L = K(\sqrt[l^k]{E})$ for some integer $k \geq 1$. Then*

$$[L:K] = \begin{cases} l^{k(r+1)} & \text{if } \zeta_l \in K; \\ l^{k(r+1)} \frac{[K(\zeta_l):K]}{\#(\langle \zeta_{l^k} \rangle \cap K(\zeta_l))} & \text{if } \zeta_l \notin K. \end{cases}$$

*In particular, if $l$ does not divide $2 \cdot \Delta(K/\mathbb{Q})$ one has $[L:K] = (l-1)l^{k(r+1)-1}$.*

*For $L = K(\zeta_{2^k}, \sqrt[2^k]{E})$ the degree is given by*

$$[L:K] = \begin{cases} 2^{k(r+1)} & \text{if } \zeta_4 \in K; \\ 2^{k(r+1)} \frac{2a_{K,k}}{\#(\langle \zeta_{2^k} \rangle \cap K(\zeta_4))} & \text{if } \zeta_4 \notin K. \end{cases}$$

*Here $a_{K,k} = 1$ if all $2^k$-th roots of unity in $K(\zeta_4)$ are of the form $\epsilon/\bar{\epsilon}$, with $\epsilon$ a unit in $K(\zeta_4)$ and $\bar{\epsilon}$ its $K$-conjugate, and $a_{K,k} = 2$ otherwise.*

**Proof.** If $\zeta_l \in K$, Kneser's theorem gives

$$[L:K] = [K^* \cdot \sqrt[l^k]{E} : K^*] = [\sqrt[l^k]{E} : \sqrt[l^k]{E} \cap K^*] = [\sqrt[l^k]{E} : E] = l^{k(r+1)}.$$

This also works for $l = 2$ when $\zeta_4 \in K$.

If $\zeta_l \notin K$, we apply Kneser's theorem over $K(\zeta_l)$ to obtain

$$[L:K(\zeta_l)] = [\sqrt[l^k]{E} : \sqrt[l^k]{E} \cap K(\zeta_l)^*] = [\sqrt[l^k]{E} : E] \cdot [\sqrt[l^k]{E} \cap K(\zeta_l)^* : E]^{-1}.$$

Let $\sigma$ be a generator of $\mathrm{Gal}(K(\zeta_l)/K)$. Then the homomorphism

$$\begin{aligned} \sqrt[l^k]{E} \cap K(\zeta_l)^* &\longrightarrow \langle \zeta_{l^k} \rangle \cap K(\zeta_l)^* \\ \alpha &\longmapsto \sigma(\alpha)/\alpha \end{aligned}$$

has kernel $E$, so $[\sqrt[l^k]{E} \cap K(\zeta_l)^* : E]$ is bounded by the order of $\langle \zeta_{l^k} \rangle \cap K(\zeta_l)^*$. The latter group intersects $E$ in $\{1\}$, so the inclusion $\langle \zeta_{l^k} \rangle \cap K(\zeta_l)^* \subset \sqrt[l^k]{E} \cap K(\zeta_l)$ shows that we have equality. The desired formula follows immediately. If $l \nmid \Delta(K/\mathbb{Q})$ we have $[K(\zeta_l):K] = l-1$ and $\langle \zeta_{l^k} \rangle \cap K(\zeta_l) = \langle \zeta_l \rangle$.

We are left with the case that $L = K(\zeta_{2^k}, \sqrt[2^k]{E})$ and $\zeta_4 \notin K$. As above, we have

$$[L:K(\zeta_4)] = [\sqrt[2^k]{E} : \sqrt[2^k]{E} \cap K(\zeta_4)^*] = 2^{k(r+1)} \cdot [\sqrt[2^k]{E} \cap K(\zeta_4)^* : E]^{-1}.$$

With $\mathrm{Gal}(K(\zeta_4)/K) = \langle \sigma \rangle$, we have again a homomorphism

$$\phi : \sqrt[2^k]{E} \cap K(\zeta_4)^* \longrightarrow \langle \zeta_{2^k} \rangle \cap K(\zeta_4)$$

with kernel $E$. The index $[\sqrt[2^k]{E} \cap K(\zeta_4)^* : E]$ is bounded by the order of $\langle \zeta_{2^k} \rangle \cap K(\zeta_4)$, but this group now intersects $E$ in $\langle -1 \rangle$. It follows that the index equals $a_{K,k}^{-1} \#(\langle \zeta_{2^k} \rangle \cap K(\zeta_4))$,

with $a_{K,k} = 1$ when $\phi$ is surjective and $a_{K,k} = 2$ otherwise. Surjectivity of $\phi$ means that all elements in $\langle \zeta_{2^k} \rangle \cap K(\zeta_4)$ have the form $\epsilon/\bar{\epsilon}$, with $\epsilon$ a unit in $K(\zeta_4)$ and $\bar{\epsilon}$ its $K$-conjugate. Note that $a_{K,k}$ only depends on $K$ for $k$ sufficiently large. □

In the following theorem, we write $F^{\#}$ to denote the multiplicative group of a field $F$ modulo its torsion elements. In other words, $F^{\#} = F^*/Z_F$, where $Z_F$ is the subgroup of roots of unity in $F^*$. Note that $F^{\#} \subset E^{\#}$ if $F \subset E$ is an extension of $F$. The following result was originally proved by Van Tieghem in [36]. We give a proof that is much shorter. See also [18].

**4.4 Theorem.** *Let $L/K$ be a finite separable field extension. Then the torsion subgroup of $L^{\#}/K^{\#}$ is a finite group of order dividing $[L : K]$.*

**Proof.** Let $t(L/K)$ be the torsion subgroup of $L^{\#}/K^{\#} = L^*/Z_L K^*$. An element $x$ mod $Z_L K^*$ is in $t(L/K)$ if and only if $x^n \in K^*$ for some integer $n \geq 1$, and this is equivalent to saying that any quotient of $x$ by one of its $K$-conjugates is a root of unity. Looking at the action of the norm $L \to K$ on $t(L/K)$, one concludes that the group $t(L/K)$ is annihilated by $[L : K]$.

If $L/K$ is abelian with group $G$, one takes the Galois cohomology sequence for

$$0 \longrightarrow Z_L \longrightarrow L^* \longrightarrow L^{\#} \longrightarrow 0.$$

By Hilbert 90, this gives

$$0 \longrightarrow Z_K \longrightarrow K^* \longrightarrow (L^{\#})^G \longrightarrow H^1(G, Z_L) \longrightarrow 0,$$

and the argument above implies that $t(L/K) \cong H^1(G, Z_L)$. In particular, if $G$ is cyclic, generated by $\sigma$, one has

$$H^1(G, Z_L) \cong \hat{H}^{-1}(G, Z_L) = \{x \in Z_L : N_{L/K}(x) = 1\}/Z_L^{\sigma - 1}.$$

Now any subgroup of $Z_L$ is an injective limit of finite cyclic groups, and $\{x \in Z_L : N_{L/K}(x) = 1\}/Z_L^{\sigma-1}$ is annihilated by $[L : K]$. We conclude that in this case $H^1(G, Z_L)$ is finite cyclic of order dividing $[L : K]$ and the theorem holds for $L/K$.

If there is an intermediate field $M$ in the extension $L/K$, we have an exact sequence

$$0 \longrightarrow t(M/K) \longrightarrow t(L/K) \longrightarrow t(L/M),$$

so the theorem is true for $L/K$ if it holds for $L/M$ and $M/K$. We give two different ways to finish the proof.

First method. We may assume that there are no intermediate fields between $K$ and $L$ different from $K$ and $L$. In particular, $K(Z_L) = L$ or $K(Z_L) = K$. If $K(Z_L) = L$,

the extension $L/K$ is abelian, even cyclic of prime degree, and we are done. Let now $K(Z_L) = K$. In this case $t(L/K)$ is the torsion subgroup of $L^*/K^*$. We may assume that there exists $x$ mod $K^*$ in $L^*/K^*$ of prime order $p$, since otherwise $t(L/K) = 1$ and there is nothing to prove. Thus $L = K(x)$ is an extension of $K$ of degree $p$. As $L/K$ is separable, we let $L' = L(\zeta_p)$ be the normal closure of $L$, and write $K' = K(\zeta_p)$. The extension $L'/K'$ is cyclic of order $p$, so $|t(L'/K')|$ divides $p$. We are done if we show that the composite map $t(L/K) \to t(L'/K) \to t(L'/K')$ is injective. Now the first arrow is injective, and the kernel of the second is isomorphic to $t(K'/K)$. Our claim follows from the fact that $t(L/K)$ has exponent $p$ and $t(K'/K)$ has order dividing $p-1$ by the theorem for cyclic extensions.

Second method. It suffices to prove the theorem for the $p$-part of $t(L/K)$, with $p$ an arbitrary prime. Let $N$ be the normal closure of $L$ over $K$, and $H \subset G = \mathrm{Gal}(N/K)$ the subgroup corresponding to $L$. Let $H_p$ and $G_p \supset H_p$ be $p$-Sylow subgroups of $H$ and $G$, and $L'$ and $K'$ the corresponding fixed fields. By the solvability of $p$-groups, $L'$ can be obtained from $K'$ by repeated cyclic extensions of degree $p$, so the theorem holds for $L'/K'$. As $K'/K$ is of degree prime to $p$, the theorem trivially holds for $K'/K$ if we restrict our attention to $p$-parts. It follows that the order of the $p$-part of $t(L'/K)$ divides $[L' : K]$ and, as $[L' : L]$ is coprime to $p$, it even divides $[L : K]$. The same is now true for the subgroup $t(L/K) \subset t(L'/K)$, and the proof is finished. □

## 5. Main theorem

We now come to the main result of this chapter, theorem 5.6. Before we can formulate the theorem, we need some introductory remarks that lead to a precise description (5.5) of the extensions we will consider.

Let $K$ be a number field, $\mathfrak{d}$ a cycle in $K$ and $m \in \mathbb{Z}_{>0}$ an integer. For a finite prime $\mathfrak{p} \nmid \mathfrak{d}$ in $K$, we let $L(\mathfrak{p}) = L(\mathfrak{p}, \mathfrak{d}, m)$ be the maximal abelian extension of $K$ of conductor dividing $\mathfrak{d}\mathfrak{p}$ in which the ramification indices at primes over $\mathfrak{p}$ in $L(\mathfrak{p})$ divide $m$. As $L(\mathfrak{p})$ contains the ray class field $H_\mathfrak{d}$ of $K$ of conductor $\mathfrak{d}$, there is an exact sequence

$$0 \longrightarrow \mathrm{Gal}(L(\mathfrak{p})/H_\mathfrak{d}) \longrightarrow \mathrm{Gal}(L(\mathfrak{p})/K) \longrightarrow \mathrm{Gal}(H_\mathfrak{d}/K) \longrightarrow 0. \tag{5.1}$$

The group $\mathrm{Gal}(L(\mathfrak{p})/H_\mathfrak{d})$ is the inertia group of the prime $\mathfrak{p}$. Under the Artin map $J \to \mathrm{Gal}(L(\mathfrak{p})/K)$ on the idèle group $J$ of $K$, it is the image of the unit group $U_\mathfrak{p}$ of the ring of integers in the local field $K_\mathfrak{p}$. As $\mathfrak{p}$ divides $\mathfrak{d}\mathfrak{p}$ to the first power, the ramification at $\mathfrak{p}$ is tame and the homomorphism $U_\mathfrak{p} \to \mathrm{Gal}(L(\mathfrak{p})/H_\mathfrak{d})$ factors via the unit group $k_\mathfrak{p}^* = U_\mathfrak{p}/U_\mathfrak{p}^{(1)}$ of the residue class field $k_\mathfrak{p}$ at $\mathfrak{p}$. Our hypothesis that the ramification indices at $\mathfrak{p}$ divide $m$ implies that $\mathrm{Gal}(L(\mathfrak{p})/H_\mathfrak{d})$ is the image under the Artin map of $k_\mathfrak{p}^*/k_\mathfrak{p}^{*m}$. In particular, it is a cyclic group of order dividing $m$.

We want to rewrite the exact sequence above in terms of ray class groups. As $L(\mathfrak{p})$ is a subfield of the ray class field $H_{\mathfrak{d}\mathfrak{p}}$ of $K$, we start by rewriting the surjection $\mathrm{Gal}(H_{\mathfrak{d}\mathfrak{p}}/K) \twoheadrightarrow \mathrm{Gal}(H_{\mathfrak{d}}/K)$ as a surjection of ray class groups $C_{\mathfrak{d}\mathfrak{p}} \to C_{\mathfrak{d}}$. By the argument above, the kernel of this map is the homomorphic image of $k_{\mathfrak{p}}^* = U_{\mathfrak{p}}/U_{\mathfrak{p}}^{(1)}$. Using the definition of the ray class groups, we see that the kernel equals

$$Y \;=\; \frac{\{\text{principal ideals } (x) \text{ with } x \equiv 1 \bmod^* \mathfrak{d} \text{ and } |x|_{\mathfrak{p}} = 1\}}{\{\text{principal ideals } (x) \text{ with } x \equiv 1 \bmod^* \mathfrak{d}\mathfrak{p}\}}.$$

Mapping ideals to the residue class of a generator that is $1 \bmod^* \mathfrak{d}$ in $k_{\mathfrak{p}}^*$, we obtain an isomorphism $Y \xrightarrow{\sim} k_{\mathfrak{p}}^*/\mathrm{im}[E_{\mathfrak{d}}]$, where $E_{\mathfrak{d}}$ denotes the group of global units that are $1 \bmod^* \mathfrak{d}$. Note however that the composition of the homomorphism $k_{\mathfrak{p}}^* = U_{\mathfrak{p}}/U_{\mathfrak{p}}^{(1)} \to Y$ induced by the canonical map $J \to C_{\mathfrak{d}\mathfrak{p}}$ with the isomorphism $Y \xrightarrow{\sim} k_{\mathfrak{p}}^*/\mathrm{im}[E_{\mathfrak{d}}]$ just given sends $x \bmod \mathfrak{p}$ to the residue class of $x^{-1}$ in $k_{\mathfrak{p}}^*/\mathrm{im}[E_{\mathfrak{d}}]$. We have proved the following.

**5.2 Lemma.** *Let $\mathfrak{d}$ be a cycle in $K$ and $\mathfrak{p}$ a finite prime not in $\mathfrak{d}$. Then there is an exact sequence*

$$0 \longrightarrow k_{\mathfrak{p}}^*/\mathrm{im}[E_{\mathfrak{d}}] \xrightarrow{\alpha} C_{\mathfrak{d}\mathfrak{p}} \xrightarrow{\mathrm{can}} C_{\mathfrak{d}} \longrightarrow 0.$$

*Here $E_{\mathfrak{d}}$ is the group of global units that are $1 \bmod^* \mathfrak{d}$, and $\alpha$ sends the residue class of a global element $x \equiv 1 \bmod^* \mathfrak{d}$ satisfying $|x|_{\mathfrak{p}} = 1$ to the class of $(x)$ in $C_{\mathfrak{d}\mathfrak{p}}$.* □

By the lemma above, we can rewrite the exact sequence of Galois groups (5.1) as

$$0 \longrightarrow k_{\mathfrak{p}}^*/(\mathrm{im}[E_{\mathfrak{d}}] \cdot k_{\mathfrak{p}}^{*m}) \longrightarrow C_{\mathfrak{d}\mathfrak{p}}/\alpha[k_{\mathfrak{p}}^{*m}] \longrightarrow C_{\mathfrak{d}} \longrightarrow 0. \tag{5.3}$$

We can view this 'arithmetical extension' as an element of an Ext-group $\mathrm{Ext}(C_{\mathfrak{d}}, -)$ that does not depend on $\mathfrak{p}$ if we identify the group $k_{\mathfrak{p}}^*/(\mathrm{im}[E_{\mathfrak{d}}] \cdot k_{\mathfrak{p}}^{*m})$ with some fixed cyclic group. For any divisor $n$ of $m$, one has

$$\begin{aligned} n \mid \#(k_{\mathfrak{p}}^*/(\mathrm{im}[E_{\mathfrak{d}}] \cdot k_{\mathfrak{p}}^{*m})) &\iff \mathrm{N}\mathfrak{p} \equiv 1 \bmod n \text{ and } \mathrm{im}[E_{\mathfrak{d}}] \subset k_{\mathfrak{p}}^{*n} \\ &\iff \mathfrak{p} \text{ splits completely in } K(\zeta_n, \sqrt[n]{E_{\mathfrak{d}}})/K \text{ and } \mathfrak{p} \nmid n. \end{aligned}$$

It follows that the primes $\mathfrak{p}$ for which the order is $m$ are exactly those primes $\mathfrak{p} \nmid m$ that split completely in $K(\zeta_m, \sqrt[m]{E_{\mathfrak{d}}})/K$. We will further restrict our attention to these primes. In order to study the behaviour of the sequence for primes $\mathfrak{p}$ for which the order of $k_{\mathfrak{p}}^*/(\mathrm{im}[E_{\mathfrak{d}}] \cdot k_{\mathfrak{p}}^{*m})$ is $n < m$, one has to replace $m$ by $n$ in the definition of $L(\mathfrak{p})$.

Given a prime $\mathfrak{p}$ that splits completely in $K(\zeta_m, \sqrt[m]{E_{\mathfrak{d}}})/K$, we choose an extension $\mathfrak{P}|\mathfrak{p}$ in $K_m = K(\zeta_m)$ and consider the $m$-th power residue symbol $\left(\frac{\cdot}{\mathfrak{P}}\right)_m$ on the unit group of the residue class field $k_{\mathfrak{P}}$ at $\mathfrak{P}$. This symbol is the homomorphism $k_{\mathfrak{P}}^* \to \langle \zeta_m \rangle$ that is defined by

$$\left(\frac{x}{\mathfrak{P}}\right)_m \equiv x^{(\mathrm{N}\mathfrak{P}-1)/m} \bmod \mathfrak{P}.$$

In accordance with the name of the symbol, the kernel consists of the $m$-th powers in $k_{\mathfrak{P}}^*$. Our splitting assumption on $\mathfrak{p}$ implies that we have an isomorphism

$$k_{\mathfrak{p}}^*/\mathrm{im}[E_{\mathfrak{d}}] \cdot k_{\mathfrak{p}}^{*m} = k_{\mathfrak{p}}^*/k_{\mathfrak{p}}^{*m} = k_{\mathfrak{P}}^*/k_{\mathfrak{P}}^{*m} \xrightarrow{\left(\frac{\cdot}{\mathfrak{P}}\right)_m} \langle \zeta_m \rangle$$

for each prime $\mathfrak{P}|\mathfrak{p}$ in $K_m$. Thus, by the choice of a prime $\mathfrak{P}|\mathfrak{p}$, our arithmetical extension gives rise to a well defined element $E_{\mathfrak{P}} \in \mathrm{Ext}(\mathcal{C}_{\mathfrak{d}}, \langle \zeta_m \rangle)$.

If $\mathfrak{P}'$ is also an extension of $\mathfrak{p}$ to $K_m$, there exists $\sigma \in \mathrm{Gal}(K_m/K)$ such that $\mathfrak{P}' = \sigma\mathfrak{P}$. The commutative diagram

$$\begin{array}{ccc} k_{\mathfrak{P}}^*/k_{\mathfrak{P}}^{*m} & \xrightarrow{\left(\frac{\cdot}{\mathfrak{P}}\right)_m} & \langle \zeta_m \rangle \\ \downarrow \sigma & & \downarrow \sigma \\ k_{\sigma\mathfrak{P}}^*/k_{\sigma\mathfrak{P}}^{*m} & \xrightarrow{\left(\frac{\cdot}{\sigma\mathfrak{P}}\right)_m} & \langle \zeta_m \rangle \end{array}$$

shows that $E_{\sigma\mathfrak{P}} = E_{\mathfrak{P}}^{\sigma}$, where $\sigma \in \mathrm{Gal}(K_m/K)$ acts on $\mathrm{Ext}(\mathcal{C}_{\mathfrak{d}}, \langle \zeta_m \rangle)$ via its action on $\langle \zeta_m \rangle$.

If we compose the natural surjection from the idèle group $J$ of $K$ onto $\mathcal{C}_{\mathfrak{d}\mathfrak{p}}$ with the canonical map $\mathcal{C}_{\mathfrak{d}\mathfrak{p}} \to \mathcal{C}_{\mathfrak{d}}$, we obtain the natural surjection $J \twoheadrightarrow \mathcal{C}_{\mathfrak{d}}$. This implies that our extension (5.3) admits a lift of the canonical map $J \to \mathcal{C}_{\mathfrak{d}}$ to a homomorphism $J \to \mathcal{C}_{\mathfrak{d}\mathfrak{p}}/\alpha[k_{\mathfrak{p}}^{*m}]$. This lifting property exists for the restriction of $J \to \mathcal{C}_{\mathfrak{d}}$ to any local component $K_{\mathfrak{q}}^*$, but it is special to our arithmetic extension only at components $K_{\mathfrak{q}}^*$ for which $\mathfrak{q}$ divides $\mathfrak{d}$. This is because the homomorphism $K_{\mathfrak{q}}^* \to \mathcal{C}_{\mathfrak{d}}$ factors via the group $K_{\mathfrak{q}}^*/U_{\mathfrak{q}}^{(\mathrm{ord}_{\mathfrak{q}}(\mathfrak{d}))}$, which is isomorphic to $\mathbb{Z}$ at finite primes outside $\mathfrak{d}$ and trivial at the infinite primes outside $\mathfrak{d}$. Let $S$ be an arbitrary finite set of primes of $K$. Then our arithmetic extension has the special property that for any prime $\mathfrak{p} \nmid \mathfrak{d}$ outside $S$, it admits a lift of the canonical map

$$f_S : \Sigma = \prod_{\mathfrak{q} \in S} K_{\mathfrak{q}}^*/U_{\mathfrak{q}}^{(\mathrm{ord}_{\mathfrak{q}}(\mathfrak{d}))} \longrightarrow \mathcal{C}_{\mathfrak{d}} \tag{5.4}$$

to $\phi_S : \Sigma \to \mathcal{C}_{\mathfrak{d}\mathfrak{p}}/\alpha[k_{\mathfrak{p}}^{*m}]$. The map $\phi_S$ is the composition

$$\Sigma \rightarrowtail J/W_{\mathfrak{d}\mathfrak{p}} \xrightarrow{\mathrm{can}} J/K^*W_{\mathfrak{d}\mathfrak{p}} = \mathcal{C}_{\mathfrak{d}\mathfrak{p}} \xrightarrow{\mathrm{can}} \mathcal{C}_{\mathfrak{d}\mathfrak{p}}/\alpha[k_{\mathfrak{p}}^{*m}].$$

Here $W_{\mathfrak{d}\mathfrak{p}}$ is defined as in (2.6). Note that $\Sigma$ and $f_S$ do not change if we add the infinite primes outside $\mathfrak{d}$ to $S$. We summarize the preceding discussion in the following way.

**5.5 Proposition.** *Let $K$ be a number field, $\mathfrak{d}$ a cycle in $K$ and $m \in \mathbb{Z}_{>0}$ an integer. Denote for a finite set $S$ of primes by $f_S$ the canonical map in* (5.4). *Suppose $\mathfrak{p} \nmid m\mathfrak{d}$ is a prime of $K$ outside $S$ that splits completely in $K_m(\sqrt[m]{E_{\mathfrak{d}}})/K$. Then the isomorphism class of the extension* (5.3) *is an element $\mathcal{E}(\mathfrak{P}) \in \mathrm{Ext}(f_S; \langle \zeta_m \rangle)$ for each prime $\mathfrak{P}|\mathfrak{p}$ in $K_m = K(\zeta_m)$ by the identification $k_{\mathfrak{p}}^*/(\mathrm{im}[E_{\mathfrak{d}}] \cdot k_{\mathfrak{p}}^{*m}) \cong \langle \zeta_m \rangle$ via $\left(\frac{\cdot}{\mathfrak{P}}\right)_m$ and the canonical*

*lift* $\phi_S : \Sigma \to C_{\mathfrak{d}\mathfrak{p}}/\alpha[k_{\mathfrak{p}}^{*m}]$. *Under the natural action of* $\mathrm{Gal}(K_m/K)$ *on* $\mathrm{Ext}(f_S;\langle\zeta_m\rangle)$, *one has* $\mathcal{E}(\mathfrak{P})^\sigma = \mathcal{E}(\sigma\mathfrak{P})$.

We are ready to formulate the main theorem of this chapter.

**5.6 Theorem.** *Let* $K$ *be a number field,* $\mathfrak{d}$ *a cycle in* $K$ *and* $m \in \mathbb{Z}_{>0}$ *an integer. Write* $K_m$ *for* $K(\zeta_m)$ *and* $E_{\mathfrak{d}}$ *for the group of units in* $\mathcal{O}_K$ *that are* $1 \bmod^* \mathfrak{d}$. *Let* $S$ *be a finite set of primes and* $f_S$ *the canonical map from* (5.4). *Denote by* $D$ *the set of primes in* $\mathfrak{d}$ *and define* $W \subset K^*$ *by*

$$W = W_{S,\mathfrak{d},m} = \{x \in K^* : \ \mathrm{ord}_{\mathfrak{q}}(x) \equiv 0 \bmod m \text{ for all finite } \mathfrak{q} \notin S \text{ and } x \equiv 1 \bmod^* \mathfrak{q}^{\mathrm{ord}_{\mathfrak{q}}(\mathfrak{d})} \text{ for all } \mathfrak{q} \in D \setminus S\}.$$

*Then there is a canonical* $\mathrm{Gal}(K_m/K)$*-linear injection*

$$\omega : \ \mathrm{Gal}(K_m(\sqrt[m]{W})/K_m(\sqrt[m]{E_{\mathfrak{d}}})) \longrightarrow \mathrm{Ext}(f_S;\langle\zeta_m\rangle)$$

*such that for a prime* $\mathfrak{P}$ *in* $K_m$ *lying over a prime* $\mathfrak{p}$ *of* $K$ *not in* $m\mathfrak{d}$ *or* $S$ *that splits completely in* $K_m(\sqrt[m]{E_{\mathfrak{d}}})/K$, *one has*

$$(\mathfrak{P}, K_m(\sqrt[m]{W})/K_m) \longmapsto \mathcal{E}(\mathfrak{P})$$

*with* $\mathcal{E}(\mathfrak{P})$ *as in* 5.5. *If* $\mathfrak{P}$ *ranges over the extensions of* $\mathfrak{p}$ *to* $K_m$, *then* $\mathcal{E}(\mathfrak{P})$ *ranges over a* $\mathrm{Gal}(K_m/K)$*-orbit in* $\mathrm{Ext}(f_S;\langle\zeta_m\rangle)$. *If* $\zeta_m$ *is in* $K$ *and* $S$ *contains* $D$, *then* $\omega$ *is an isomorphism.*

**Remarks.** It should be noted that the Artin symbol $(\mathfrak{P}, K_m(\sqrt[m]{W})/K_m)$ in 5.6 is indeed an element of $\mathrm{Gal}(K_m(\sqrt[m]{W})/K_m(\sqrt[m]{E_{\mathfrak{d}}}))$, because $\mathfrak{P}$ splits completely in $K_m(\sqrt[m]{E_{\mathfrak{d}}})/K_m$. Further any element of $\mathrm{Gal}(K_m(\sqrt[m]{W})/K_m(\sqrt[m]{E_{\mathfrak{d}}}))$ is of this form by the Čebotarev density theorem, so $\omega$ is uniquely determined by its values on Artin symbols.

For the prime $\mathfrak{p}$ in 5.6, there is no unique Artin symbol but only a *Artin class* in $\mathrm{Gal}(K_m(\sqrt[m]{W})/K_m(\sqrt[m]{E_{\mathfrak{d}}}))$, consisting of the Frobenius symbols of primes $\mathfrak{P}$ over $\mathfrak{p}$. It is a conjugacy class in $\mathrm{Gal}(K_m(\sqrt[m]{W})/K)$ that is an orbit under the natural action by inner automorphisms of $\mathrm{Gal}(K_m/K)$. We see that $\omega$ maps this class to the $\mathrm{Gal}(K_m/K)$-orbit consisting of the elements $\mathcal{E}(\mathfrak{P})$ for $\mathfrak{P}|\mathfrak{p}$. Thus, the Artin symbol of $\mathfrak{p}$ in $\mathrm{Gal}(K_m(\sqrt[m]{W})/K)$ and the isomorphism class of the extension (5.3) in $\mathrm{Ext}(f_S,\langle\zeta_m\rangle)$ are not uniquely determined in exactly the same way.

In theorem 5.13, we will give several conditions under which $\omega$ is an isomorphism.

**Proof.** The main idea is to use the isomorphism from 3.3(b) to realize the group $\mathrm{Ext}(f_S;\langle\zeta_m\rangle)$ as a group of homomorphisms of the form $\mathrm{Hom}(A,\langle\zeta_m\rangle)$ with $A$ a certain subquotient of $K^*$. Kummer theory can then be used to make the transition to a Galois

group of an extension over $K_m$. The problem is that our map $f_S$ need not satisfy the requirement of surjectivity that is essential for 3.3(b). Note however that $f_S$ is surjective if $S \supset D$ and the classes of the finite primes in $S$ generate the ideal class group of $K$. Our proof deals with this problem by 'extending' $f_S$ to a surjective map, applying 3.3(b) and going back to $f_S$.

As we observed just before proposition 5.5, we may assume that $S$ contains all infinite primes outside $\mathfrak{d}$. This will allow us to write '$\mathfrak{q} \notin S \cup D$' instead of '$\mathfrak{q} \notin S \cup D$ and $\mathfrak{q}$ finite' in the rest of the proof.

Let $W_{\mathfrak{d}}$ be defined as in (2.6), and consider the subgroup $T \subset J/W_{\mathfrak{d}}$ containing $\Sigma$ defined by

$$T = \bigoplus_{\mathfrak{q} \notin D \setminus S} K_{\mathfrak{q}}^* / U_{\mathfrak{q}}^{(\mathrm{ord}_{\mathfrak{q}}(\mathfrak{d}))} \cong \Sigma \times \bigoplus_{\mathfrak{q} \notin S \cup D} \mathbf{Z}.$$

It is clear that the restriction $f_T$ of the canonical map $\psi : J/W_{\mathfrak{d}} \to \mathcal{C}_{\mathfrak{d}}$ to $T$ is surjective. If $S \supset D$ we have $T = J/W_{\mathfrak{d}}$. More generally, there is an exact sequence

$$0 \longrightarrow T \longrightarrow J/W_{\mathfrak{d}} \longrightarrow \bigoplus_{\mathfrak{q} \in D \setminus S} K_{\mathfrak{q}}^* / U_{\mathfrak{q}}^{(\mathrm{ord}_{\mathfrak{q}}(\mathfrak{d}))} \longrightarrow 0.$$

As $E_{\mathfrak{d}} = W_{\mathfrak{d}} \cap K^*$, there is a derived sequence

$$0 \longrightarrow \ker f_T \longrightarrow \ker \psi \cong K^*/E_{\mathfrak{d}} \longrightarrow \bigoplus_{\mathfrak{q} \in D \setminus S} K_{\mathfrak{q}}^* / U_{\mathfrak{q}}^{(\mathrm{ord}_{\mathfrak{q}}(\mathfrak{d}))}$$

that shows that $\ker f_T = X/E_{\mathfrak{d}}$, where

$$X = \{x \in K^* : \ x \equiv 1 \bmod^* \mathfrak{q}^{\mathrm{ord}_{\mathfrak{q}}(\mathfrak{d})} \text{ for all } \ \mathfrak{q} \in D \setminus S\}.$$

Note that $X = K^*$ if $S \supset D$.

Analogously, the sequence $0 \to \Sigma \to T \to \oplus_{\mathfrak{q} \notin S \cup D} \mathbf{Z} \to 0$ gives

$$0 \longrightarrow \ker f_S \longrightarrow \ker f_T = X/E_{\mathfrak{d}} \longrightarrow \bigoplus_{\mathfrak{q} \notin S \cup D} \mathbf{Z} \longrightarrow \mathrm{cok}\, f_S \longrightarrow 0. \tag{5.7}$$

This shows that $\ker f_S = X_S/E_{\mathfrak{d}}$, where $X_S$ denotes the group of $S$-units in $X$:

$$X_S = \{x \in X : \ |x|_{\mathfrak{q}} = 1 \text{ if } \mathfrak{q} \notin S\}.$$

We now apply theorem 3.4, with $F = \oplus_{\mathfrak{q} \notin S \cup D} \mathbf{Z}$ and $A = \langle \zeta_m \rangle$ and homomorphisms $f = f_S$ and $f' = f_T$. As $\ker f_T = X/E_{\mathfrak{d}}$, we obtain isomorphisms

$$\begin{aligned} \mathrm{Ext}(f_S; \langle \zeta_m \rangle) &\cong \mathrm{cok}\left[\mathrm{Hom}(\bigoplus_{\mathfrak{q} \notin S \cup D} \mathbf{Z}, \langle \zeta_m \rangle) \longrightarrow \mathrm{Hom}(X/E_{\mathfrak{d}}, \langle \zeta_m \rangle)\right] \\ &\cong \mathrm{cok}\left[\mathrm{Hom}(\bigoplus_{\mathfrak{q} \notin S \cup D} \mathbf{Z}/m\mathbf{Z}, \langle \zeta_m \rangle) \longrightarrow \mathrm{Hom}(X/E_{\mathfrak{d}} X^m, \langle \zeta_m \rangle)\right]. \end{aligned}$$

If $f_S$ is surjective, (5.7) and projectivity of $\oplus_{\mathfrak{q}\notin S\cup D}\mathbf{Z}$ show that this is the isomorphism

$$\mathrm{Ext}(f_S;\langle\zeta_m\rangle) \;\cong\; \mathrm{Hom}(X_S/E_\mathfrak{d},\langle\zeta_m\rangle), \tag{5.8}$$

in accordance with 3.3(b). For the general case, we use our group $W = W_{S,\mathfrak{d},m}$ and consider the exact sequence of $\mathbf{Z}/m\mathbf{Z}$-modules

$$0 \longrightarrow W/E_\mathfrak{d}X^m \longrightarrow X/E_\mathfrak{d}X^m \longrightarrow \bigoplus_{\mathfrak{q}\notin S\cup D} \mathbf{Z}/m\mathbf{Z}.$$

Application of $\mathrm{Hom}(-,\langle\zeta_m\rangle)$ to this sequence gives

$$\mathrm{Hom}(\bigoplus_{\mathfrak{q}\notin S\cup D} \mathbf{Z}/m\mathbf{Z},\langle\zeta_m\rangle) \longrightarrow \mathrm{Hom}(X/E_\mathfrak{d}X^m,\langle\zeta_m\rangle) \longrightarrow \mathrm{Hom}(W/E_\mathfrak{d}X^m,\langle\zeta_m\rangle) \longrightarrow 0$$

because $\langle\zeta_m\rangle$ is injective as a $\mathbf{Z}/m\mathbf{Z}$-module. We conclude that an isomorphism

$$\mathrm{Ext}(f_S;\langle\zeta_m\rangle) \xrightarrow{\sim} \mathrm{Hom}(W/E_\mathfrak{d}X^m,\langle\zeta_m\rangle) \tag{5.9}$$

is induced. Inspection of the various homomorphisms leads to the following explicit description. Given an extension of $f_S$ with $\langle\zeta_m\rangle$, lift it to an extension $(E,\phi_T)$ of $f_T$ with $\langle\zeta_m\rangle$. By restriction, a homomorphism $W \to \langle\zeta_m\rangle$ is obtained that is trivial on $E_\mathfrak{d}X^m$. Note that $\phi_T(w)$ for $w \in W$ does not depend on the choice of $\phi_T$ because $\mathrm{ord}_\mathfrak{q}(w) = 0 \bmod m$ at $\mathfrak{q} \notin S \cup D$. In particular, for the extension class $\mathcal{E}(\mathfrak{P})$ in $\mathrm{Ext}(f_S;\langle\zeta_m\rangle)$, we have $E = \mathcal{C}_{\mathfrak{d}\mathfrak{p}}/\alpha[k_\mathfrak{p}^{*m}]$ and we can choose for $\phi_T$ the composition of an embedding

$$T = \Sigma \times \bigoplus_{\mathfrak{q}\notin S\cup D} K_\mathfrak{q}^*/U_\mathfrak{q} \longrightarrow \Sigma \times \bigoplus_{\substack{\mathfrak{q}\notin S\cup D\\ \mathfrak{q}\neq\mathfrak{p}}} K_\mathfrak{q}^*/U_\mathfrak{q} \times K_\mathfrak{p}^*$$

with the canonical map to $\mathcal{C}_{\mathfrak{d}\mathfrak{p}}/\alpha[k_\mathfrak{p}^{*m}]$. If $w$ is an element of $W$, it can be multiplied by an element of $X^m$ to ensure that $w$ is a local unit at $\mathfrak{p}$. In that case, we see that the homomorphism $\rho_\mathfrak{P} \in \mathrm{Hom}(W/E_\mathfrak{d}X^m,\langle\zeta_m\rangle)$ corresponding to $\mathcal{E}(\mathfrak{P})$ sends $w$ to

$$\rho_\mathfrak{P}(w) = \phi_T\big((w)_{\mathfrak{q}\notin D\setminus S,\mathfrak{q}\neq\mathfrak{p}} \times (1)_\mathfrak{p}\big).$$

As we have $w \equiv 1 \bmod^* \mathfrak{q}^{\mathrm{ord}_\mathfrak{q}(\mathfrak{d})}$ at all primes in $D \setminus S$, this is the image under $\phi : J/W_\mathfrak{d} \to \mathcal{C}_{\mathfrak{d}\mathfrak{p}}/\alpha[k_\mathfrak{p}^{*m}]$ of the element $\big((w)_{\mathfrak{q}\neq\mathfrak{p}} \times (1)_\mathfrak{p}\big)$. Using the fact that $K^*/E_\mathfrak{d}$ is in the kernel of $\phi$, we arrive at

$$\phi\big((w)_{\mathfrak{q}\neq\mathfrak{p}} \times (1)_\mathfrak{p}\big) = \phi\big((1)_{\mathfrak{q}\neq\mathfrak{p}} \times (w^{-1})_\mathfrak{p}\big) = \alpha(w \bmod \mathfrak{p}).$$

In the last equation, we used the observation preceding lemma 5.2. Finally, our identification of $k_\mathfrak{p}/k_\mathfrak{p}^{*m}$ with $\langle\zeta_m\rangle$ implies that

$$\rho_\mathfrak{P}(w) = \left(\frac{w}{\mathfrak{P}}\right)_m.$$

From the surjection $W/E_{\mathfrak{d}}X^m \twoheadrightarrow WK_m^{*\,m}/E_{\mathfrak{d}}K_m^{*\,m}$ we obtain an injection that is the lower horizontal arrow in the diagram

$$\begin{array}{ccc} \mathrm{Gal}(K_m(\sqrt[m]{W})/K_m(\sqrt[m]{E_{\mathfrak{d}}})) & \xrightarrow{\omega} & \mathrm{Ext}(f_S;\langle\zeta_m\rangle) \\ \downarrow\wr & & \downarrow\wr \\ \mathrm{Hom}(WK_m^{*\,m}/E_{\mathfrak{d}}K_m^{*\,m},\langle\zeta_m\rangle) & \longrightarrow & \mathrm{Hom}(W/E_{\mathfrak{d}}X^m,\langle\zeta_m\rangle). \end{array}$$

The left vertical isomorphism comes from Kummer theory, the right vertical isomorphism has just been derived. Note that the induced injection $\omega$ is an isomorphism if and only if

$$W \cap E_{\mathfrak{d}}K_m^{*\,m} = E_{\mathfrak{d}}X^m. \tag{5.10}$$

This condition is trivially satisfied when $\zeta_m$ is in $K$ and $S$ contains $D$, since then $X = K^* = K_m^*$.

We still have to show that $\omega$ satisfies the description given in the theorem. The image of the Artin symbol $\sigma_{\mathfrak{P}} = (\mathfrak{P}, K_m(\sqrt[m]{W})/K_m) \in \mathrm{Gal}(K_m(\sqrt[m]{W})/K_m(\sqrt[m]{E_{\mathfrak{d}}}))$ under the left vertical arrow is the homomorphism

$$w \mapsto \frac{\sigma_{\mathfrak{P}}(\sqrt[m]{w})}{\sqrt[m]{w}} \equiv w^{(\mathrm{N}\mathfrak{P}-1)/m} \bmod \mathfrak{P}.$$

As all $m$-th roots of unity are distinct modulo $\mathfrak{P}$, this congruence shows that $\sigma_{\mathfrak{P}}(w) = \rho_{\mathfrak{P}}(w)$ for each $\mathfrak{p}$-adic unit $w \in W$, hence for all $w \in W$. It follows that $\omega$ maps $\sigma_{\mathfrak{P}}$ to $\mathcal{E}(\mathfrak{P})$.

The fact that $\omega$ respects the action of $\mathrm{Gal}(K_m/K)$ is a direct consequence of the canonicity of all arrows in this proof. Alternatively, one can check that the action on $\mathrm{Gal}(K_m(\sqrt[m]{W})/K_m(\sqrt[m]{E_{\mathfrak{d}}}))$ and $\mathrm{Ext}(f_S;\langle\zeta_m\rangle)$ are the same by observing that

$$\omega\big((\tau\mathfrak{P}, K_m(\sqrt[m]{W})/K_m)\big) = \mathcal{E}(\tau\mathfrak{P}) = \mathcal{E}(\mathfrak{P})^{\tau}$$

for any $\tau \in \mathrm{Gal}(K_m/K)$.

This finishes the proof of theorem 5.6. □

**Remark.** Suppose that $m = 2$ in 5.6 and that $\mathfrak{p} \nmid \mathfrak{d}$ is a real prime of $K$ that splits completely in $K_m(\sqrt[m]{E_{\mathfrak{d}}}) = K(\sqrt{E_{\mathfrak{d}}})$. Then $\mathfrak{p}$ gives rise to an element $\mathcal{E}(\mathfrak{p}) \in \mathrm{Ext}(f_S;\langle -1\rangle)$ by the sign map $k_{\mathfrak{p}}^*/k_{\mathfrak{p}}^{*2} \xrightarrow{\sim} \langle -1\rangle$. As might be expected, this element is the $\omega$-image of the Artin symbol $\sigma_{\mathfrak{p}} = (\mathfrak{p}, K(\sqrt{W})/K)$, which is by definition the element of the Galois group that induces the non-trivial automorphism on the local extensions $K(\sqrt{W})_{\mathfrak{q}}/K_{\mathfrak{p}} \cong \mathbb{C}/\mathbb{R}$ at $\mathfrak{q}|\mathfrak{p}$. The verification of this fact comes down that to the fact that, in the terminology of the proof of 5.6, the elements $\rho_{\mathfrak{p}}(w) = \mathrm{sign}_{\mathfrak{p}}(w)$ and $\sigma_{\mathfrak{p}}(\sqrt{w})/\sqrt{w}$ coincide for all $w \in W$.

There are other descriptions of the field $K_m(\sqrt[m]{W})$ in the preceding theorem in case $S$ satisfies additional conditions.

**5.11 Proposition.** *Let $W$ be as in 5.6, with $S$ containing the primes in $\mathfrak{d}$ and the infinite primes, and set $M = K_m(\sqrt[m]{W})$. Then the following holds.*

(i) *If the class group of $K$ is generated by the classes of the finite primes in $S$, then $M = K_m(\sqrt[m]{K_S})$, where $K_S$ denotes the group of $S$-units*

$$\{x \in K^* : |x|_\mathfrak{q} = 1 \text{ if } \mathfrak{q} \notin S\}.$$

(ii) *If $K$ contains the $m$-th roots of unity and $S$ contains the primes dividing $(m)$, then $M$ is the maximal abelian extension of $K$ of exponent dividing $m$ that is unramified outside $S$.*

**Proof.** The conditions in (i) imply that the map $f_S$ is surjective. In that case the proof of 5.6 is much easier: one can use equation (5.8) to see that $M = K_m(\sqrt[m]{X_S})$, and the inclusion $S \supset D$ implies $X_S = K_S$. Of course, one can also be prove directly that $W = K_S K^{*m}$. Indeed, suppose $\alpha$ has order divisible by $m$ at all primes not in $S$. Then we can write $(\alpha) = \mathfrak{s} \cdot \mathfrak{a}^m$ with $\mathfrak{s}$ a fractional ideal built up from the finite primes in $S$. By assumption, there is an ideal $\mathfrak{b}$ built up from the finite primes in $S$ that is in the same ideal class as $\mathfrak{a}$. Write $(\beta) = \mathfrak{a} \cdot \mathfrak{b}^{-1}$, then $\alpha\beta^{-m} \in K_S$, as required.

For (ii), note that any abelian extension of $K$ is of the form $K(\sqrt[m]{V})$ for some $V \subset K^*$ by Kummer theory. Further an extension $K(\sqrt[m]{x})/K$ is unramified at a prime $\mathfrak{q} \nmid (m) \cdot \infty$ if and only if $\mathrm{ord}_\mathfrak{q}(x) \equiv 0 \bmod m$. The assertion follows. □

Making the choices $\mathfrak{d} = 1$, $S = \emptyset$, we obtain a theorem of which 2.4 is a special case.

**5.12 Corollary.** *Let $K$ be a number field, $Cl$ its class group, $E$ the unit group of the ring of integers of $K$ and $W$ the subset of elements $\alpha \in K^*$ for which $(\alpha)$ is an $m$-th ideal power. Then there is a canonical $\mathrm{Gal}(K_m/K)$-linear injection*

$$\mathrm{Gal}(K_m(\sqrt[m]{W})/K_m(\sqrt[m]{E})) \longrightarrow \mathrm{Ext}(Cl, \langle\zeta_m\rangle)$$

*that is an isomorphism when $K = K_m$. It maps the Artin symbol of a prime $\mathfrak{P}$ of $K_m$ lying over a prime $\mathfrak{p} \nmid m$ in $K$ that splits completely in $K_m(\sqrt[m]{E})/K$ to the class of the extension*

$$\mathcal{E}_\mathfrak{p} : \ 0 \longrightarrow k_\mathfrak{p}^*/k_\mathfrak{p}^{*m} \longrightarrow \mathcal{C}_\mathfrak{p}/\alpha[k_\mathfrak{p}^{*m}] \longrightarrow \mathcal{C} \longrightarrow 0,$$

*where $k_\mathfrak{p}^*/k_\mathfrak{p}^{*m} \cong \langle\zeta_m\rangle$ via the norm residue symbol at $\mathfrak{P}$.* □

The following theorem shows that if $S$ contains the primes in $\mathfrak{d}$, the hypothesis $\zeta_m \in K$ in the last statement of theorem 5.6 can be substantially weakened without losing the isomorphy of $\omega$.

**5.13 Theorem.** *Suppose the set $S$ in theorem 5.6 contains $D$. Then the injection*

$$\omega : \mathrm{Gal}(K_m(\sqrt[m]{W})/K_m(\sqrt[m]{E_\mathfrak{d}})) \longrightarrow \mathrm{Ext}(f_S; \langle \zeta_m \rangle)$$

*in theorem 5.6 and the injection*

$$\mathrm{Gal}(K_m(\sqrt[m]{W})/K_m(\sqrt[m]{E})) \longrightarrow \mathrm{Ext}(Cl, \langle \zeta_m \rangle)$$

*in 5.12 are isomorphisms in each of the following cases:*

(1) $\zeta_m \in K$;

(2) $\langle \zeta_m \rangle \cap K = 1$;

(3) *$m$ is prime;*

(4) *$m$ is an odd prime power;*

(5) *$K$ contains a primitive $r$-th root of unity, where $r$ is the product of all odd primes in $m$, and a primitive 4-th root of unity in case $4 \mid m$.*

**Proof.** As 5.12 is a corollary of 5.6, it suffices to look at the injection $\omega$ from 5.6. By our assumption on $S$, condition (5.10) that is necessary and sufficient for isomorphy of $\omega$ can be rewritten as

$$E_\mathfrak{d}(W \cap {K_m^*}^m) = E_\mathfrak{d} {K^*}^m,$$

with $W = W_{S,\mathfrak{d},m}$ and $E_\mathfrak{d}$ as in 5.6. Note that the inclusion $\supset$ is always valid, and that equality follows when $W \cap {K_m^*}^m = {K^*}^m$.

For (1) there is nothing to prove.

If $\langle \zeta_m \rangle \cap K = 1$, we use Schinzel's theorem 4.1. Take $x \in W \cap {K_m^*}^m$. Then one has a $K$-homomorphism $K(\sqrt[m]{x}) \to K_m$, so $K \subset K(\sqrt[m]{x})$ is abelian. It follows that $x \in {K^*}^m$ by 4.1, and we are done.

If $m$ is prime we are either in case (1) or in case (2), so (3) follows immediately.

In case (5) we have the necessary roots of unity to apply Kneser's theorem 4.2. It follows that

$$[\sqrt[m]{W} : K^*] = [K_m(\sqrt[m]{W}) : K]$$

and that

$$[K^* \cdot \sqrt[m]{E_\mathfrak{d}} : K^*] = [K_m(\sqrt[m]{E_\mathfrak{d}}) : K].$$

Consequently, one has $[K_m(\sqrt[m]{W}) : K_m(\sqrt[m]{E_\mathfrak{d}})] = \#(\sqrt[m]{W}/(K^* \cdot \sqrt[m]{E_\mathfrak{d}})) = \#(W/E_\mathfrak{d}{K^*}^m)$, so that the natural map $\mathrm{Gal}(K_m(\sqrt[m]{W})/K_m(\sqrt[m]{E_\mathfrak{d}})) \longrightarrow \mathrm{Hom}(W/E_\mathfrak{d}{K^*}^m, \langle \zeta_m \rangle)$ is an isomorphism. This group is just $\mathrm{Ext}(f_S; \langle \zeta_m \rangle)$ by (5.9).

We finally treat case (4). If $m = p^k$ is an odd prime power, then $\langle \zeta_m \rangle$ is cyclic and $K \cap \langle \zeta_m \rangle$ is either trivial or a subgroup of $\langle \zeta_m \rangle$ containing $\zeta_p$. Thus we are either in case (2) or in case (5). □

The case that $m$ is a power of 2 larger than 2 is not covered by 5.13. The following example shows that we do not necessarily have an isomorphism for such $m$, not even in the special case 5.12.

**5.14 Example.** Take $K = \mathbb{Q}(\sqrt{-5})$ and $m = 4$ in 5.12. Then $Cl$ is cyclic of order 2, generated by the class of the prime ideal over 2 in $K$, so one has $W = \langle 4 \rangle EK^{*4}$. Further $E = \langle -1 \rangle$, so $K(\sqrt[4]{W}) = K(\sqrt{2}, \zeta_8) = K(\zeta_8) = K(\sqrt[4]{E})$. The injection $\omega$ becomes

$$1 = \mathrm{Gal}(K(\sqrt[4]{W})/K(\sqrt[4]{E})) \to \mathrm{Ext}(Cl, \langle \zeta_4 \rangle) \cong \mathbb{Z}/2\mathbb{Z},$$

which is not surjective.

Theorem 5.13 shows that the generalized Ext-group $\mathrm{Ext}(f_S; \langle \zeta_m \rangle)$ is appropriate in describing 'arithmetical extensions'. That is, if we take into account that arithmetical extensions have the special property of admitting lifts of decomposition groups at primes in $\mathfrak{d}$ by including such primes in $S$, mild conditions ensure that all elements of $\mathrm{Ext}(f_S; \langle \zeta_m \rangle)$ are realized as extensions of this type. One might ask to which extent the same is true for the ordinary Ext-group $\mathrm{Ext}(\mathcal{C}_\mathfrak{d}, \langle \zeta_m \rangle)$. First of all, there is the following special case of 5.6.

**5.15 Theorem.** *Let $K, m$ and $\mathfrak{d}$ be as in 5.6, and define $W_0 \subset K^*$ by*

$$W_0 = \{\alpha \in K^* : \ \alpha \equiv 1 \bmod^* \mathfrak{d} \text{ and } \mathrm{ord}_\mathfrak{q}(\alpha) \equiv 0 \bmod m \text{ for all finite } \mathfrak{q} \nmid \mathfrak{d}\}.$$

*Then there is a canonical $\mathrm{Gal}(K_m/K)$-linear injection*

$$\omega' : \ \mathrm{Gal}(K_m(\sqrt[m]{W_0})/K_m(\sqrt[m]{E_\mathfrak{d}})) \longrightarrow \mathrm{Ext}(\mathcal{C}_\mathfrak{d}, \langle \zeta_m \rangle)$$

*that maps the Artin symbol of a prime $\mathfrak{P}$ of $K_m$ lying over a prime $\mathfrak{p} \nmid m\mathfrak{d}$ in $K$ that splits completely in $K_m(\sqrt[m]{E_\mathfrak{d}})/K$ to the class of the extension*

$$0 \longrightarrow k_\mathfrak{p}^*/k_\mathfrak{p}^{*m} \longrightarrow C_{\mathfrak{d}\mathfrak{p}}/\alpha[k_\mathfrak{p}^{*m}] \longrightarrow \mathcal{C} \longrightarrow 0,$$

*where $k_\mathfrak{p}^*/k_\mathfrak{p}^{*m} \cong \langle \zeta_m \rangle$ via the norm residue symbol at $\mathfrak{P}$. It is an isomorphism if and only if*

$$W_0 \cap E_\mathfrak{d} K_m^{*\,m} = E_\mathfrak{d} K_{1 \bmod^* \mathfrak{d}}^m.$$

*Here $K_{1 \bmod^* \mathfrak{d}}$ denotes the subgroup of $K^*$ consisting of those elements $x \in K^*$ that satisfy $x \equiv 1 \bmod^* \mathfrak{d}$.*

**Proof.** Take $S$ to be empty in 5.6 and use (5.10). □

One can compare the ordinary Ext-group to our modified Ext-group by looking at the explicit description of the natural map

$$\mathrm{Ext}(f_S; \langle \zeta_m \rangle) \to \mathrm{Ext}(\mathcal{C}_\mathfrak{d}, \langle \zeta_m \rangle)$$

for a set $S$ containing the primes in $\mathfrak{d}$. If we define, in the situation of theorem 5.6, a subgroup $W_1 \subset K^*$ containing $W_0$ by

$$W_1 = \{\alpha \in K^* : \operatorname{ord}_{\mathfrak{q}}(\alpha) \equiv 0 \bmod m \text{ for all finite } \mathfrak{q} \nmid \mathfrak{d}\},$$

then (5.9) gives a natural commutative diagram

$$\begin{array}{ccc} \operatorname{Hom}(W_1/E_{\mathfrak{d}}K^{*m}, \langle\zeta_m\rangle) & \xrightarrow{\sim} & \operatorname{Ext}(f_D; \langle\zeta_m\rangle) \\ \downarrow & & | \\ \operatorname{Hom}(W_0K^{*m}/E_{\mathfrak{d}}K^{*m}, \langle\zeta_m\rangle) & & \\ \downarrow & & \downarrow \\ \operatorname{Hom}(W_0/E_{\mathfrak{d}}K^m_{1 \bmod^* \mathfrak{d}}, \langle\zeta_m\rangle) & \xrightarrow{\sim} & \operatorname{Ext}(C_{\mathfrak{d}}, \langle\zeta_m\rangle), \end{array}$$

in which the first vertical arrow is surjective and the second injective. If the inclusion $W_0 \cap E_{\mathfrak{d}}K^{*m} \subset E_{\mathfrak{d}}K^m_{1 \bmod^* \mathfrak{d}}$ is strict, there are elements of $\operatorname{Ext}(C_{\mathfrak{d}}, \langle\zeta_m\rangle)$ that cannot be realized by extensions (5.3) because they do not have the required lifting properties. Examples of this phenomenon are easily given, even if $K$ contains the $m$-th roots of unity.

If the inclusion $W_0K^{*m} \subset W_1$ is strict, the extension group $\operatorname{Ext}(f_D; \langle\zeta_m\rangle)$ gives a finer equivalence relation on the structure of the extensions (5.3) than the ordinary Ext-group.

**5.16 Example.** Take $K = \mathbb{Q}$ and $m = 2$ in 5.15, and choose $\mathfrak{d} = (4) \cdot \infty$. Then one has $C_{\mathfrak{d}} = (\mathbb{Z}/4\mathbb{Z})^* \cong \operatorname{Gal}(\mathbb{Q}(\zeta_4)/\mathbb{Q})$ and on the other hand $W_0 = \mathbb{Q}^{*2} \cap \mathbb{Z}_2^*$ and $E_{\mathfrak{d}} = 1$. The injection

$$1 = \operatorname{Gal}(K(\sqrt{W_0})/K(\sqrt{E_{\mathfrak{d}}})) \to \operatorname{Ext}(C_{\mathfrak{d}}, \langle -1\rangle) \cong \mathbb{Z}/2\mathbb{Z}$$

is strict. In fact, it is well known that there are no cyclic extensions of $\mathbb{Q}$ of degree 4 that have $\mathbb{Q}(\zeta_4)$ as quadratic subfield. If we take $S = \infty$ in this case, we have $\operatorname{Ext}(f_S; \langle -1\rangle) = 1$: the lifting property of the decomposition group of the infinite prime forces the extension to be split.

We conclude this section with a reformulation of our main theorem 5.6 that will be taken up in the more general context of the next chapter. It expresses the fact that the field $K_m(\sqrt[m]{W})$ is a governing field for *all* extensions (5.3), independent of the order of the group $k_{\mathfrak{p}}^*/(\operatorname{im}[E_{\mathfrak{d}}] \cdot k_{\mathfrak{p}}^{*m})$. It has the advantage of dealing with all primes $\mathfrak{p} \nmid m\mathfrak{d}$ outside $S$ at the same time, but lacks the sharp formulation of 5.6 in terms of a canonical injection.

**5.17 Theorem.** *Let $K$ be a number field, $\mathfrak{d}$ a cycle in $K$ and $m \in \mathbb{Z}_{>0}$ an integer. For each prime $\mathfrak{p}$ of $K$, write $L(\mathfrak{p}) = L(\mathfrak{p}, \mathfrak{d}, m)$ for the maximal abelian extension of conductor dividing $\mathfrak{d}\mathfrak{p}$ of $K$ in which the ramification indices at $\mathfrak{p}$ divide $m$. Write $H_{\mathfrak{d}}$ for the ray class field of conductor $\mathfrak{d}$ of $K$. Let $S$ be a finite set of primes of $K$ and define $W \subset K^*$ by*

$$W = W_{S,\mathfrak{d},m} = \{x \in K^* : \operatorname{ord}_{\mathfrak{q}}(x) \equiv 0 \bmod m \text{ for all finite } \mathfrak{q} \notin S \text{ and } x \equiv 1 \bmod^* \mathfrak{q}^{\operatorname{ord}_{\mathfrak{q}}(\mathfrak{d})} \text{ for all } \mathfrak{q} \in D \setminus S\}.$$

*If $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are primes of $K$ not in $m\mathfrak{d}$ or $S$ that have the same Frobenius class in* $\mathrm{Gal}(K_m(\sqrt[n]{W})/K)$, *there exists an isomorphism*

$$f:\ \mathrm{Gal}(L(\mathfrak{p}_1)/K)\xrightarrow{\sim}\mathrm{Gal}(L(\mathfrak{p}_2)/K)$$

*that respects the projections onto* $\mathrm{Gal}(H_{\mathfrak{d}}/K)$ *such that the following is satisfied:*

(a) *when $n$ denotes the order of the inertia groups $I_{\mathfrak{p}_i}$ and one takes $k_{\mathfrak{p}_i}^*/{k_{\mathfrak{p}_i}^*}^n \cong I_{\mathfrak{p}_i}$ via the local Artin map, there is for any choice of prime elements $\mathfrak{P}_i|\mathfrak{p}_i$ in $K_n(\sqrt[n]{E_{\mathfrak{d}}})$ a commutative diagram*

$$\begin{array}{ccc} I_{\mathfrak{p}_1} & \cong k_{\mathfrak{p}_1}^*/{k_{\mathfrak{p}_1}^*}^n & \xrightarrow{\left(\frac{\cdot}{\mathfrak{P}_1}\right)_n} \langle\zeta_n\rangle \\ \downarrow f & & \downarrow \tau \\ I_{\mathfrak{p}_2} & \cong k_{\mathfrak{p}_2}^*/{k_{\mathfrak{p}_2}^*}^n & \xrightarrow{\left(\frac{\cdot}{\mathfrak{P}_2}\right)_n} \langle\zeta_n\rangle. \end{array}$$

*with $\tau \in \mathrm{Gal}(K(\zeta_n)/K)$ suitably chosen.*

(b) *for each prime $\mathfrak{q}$ of $K$ in $S$, there is an isomorphism of $K_{\mathfrak{q}}$-algebras*

$$L(\mathfrak{p}_1)\otimes_K K_{\mathfrak{q}} \cong L(\mathfrak{p}_2)\otimes_K K_{\mathfrak{q}}$$

*such that the group actions of* $\mathrm{Gal}(L(\mathfrak{p}_1)/K)$ *on* $L(\mathfrak{p}_2)\otimes K_{\mathfrak{q}}$ *via this isomorphism and via $f$ coincide. Here $K_{\mathfrak{q}}$ is the completion of $K$ at $\mathfrak{q}$.*

*Conversely, primes $\mathfrak{p}_1$ and $\mathfrak{p}_2$ of $K$ outside $m\mathfrak{d}$ or $S$ for which there exists an isomorphism $f$ satisfying* (a) *and* (b) *have the same Frobenius class in* $\mathrm{Gal}(K_n(\sqrt[n]{W})/K)$, *where $n$ is the number occurring in* (a).

**Proof.** Assume first that we have primes $\mathfrak{p}_1$ and $\mathfrak{p}_2$ as above having the same Frobenius class in $\mathrm{Gal}(K_m(\sqrt[n]{W})/K)$. The order $n$ of the group $\#(k_{\mathfrak{p}_i}^*/(\mathrm{im}[E_{\mathfrak{d}}]\cdot {k_{\mathfrak{p}_i}^*}^m))$ is the same for $i=1$ and $i=2$ because $n$ is the largest divisor of $m$ for which $\mathfrak{p}_i$ splits completely in $K(\zeta_n,\sqrt[n]{E_{\mathfrak{d}}})/K$. Replacing $m$ by $n$ if necessary—this does not change the fields $L(\mathfrak{p}_i)$, and we have an inclusion $K_n(\sqrt[n]{W_{\mathfrak{d},S,n}}) \subset K_m(\sqrt[n]{W_{\mathfrak{d},S,m}})$—we may assume that $n=m$.

By theorem 5.6 and our assumption, we can choose primes $\mathfrak{P}_i|\mathfrak{p}_i$ in $K_m$ such that $\mathcal{E}(\mathfrak{P}_1)=\mathcal{E}(\mathfrak{P}_2)\in \mathrm{Ext}(f_S;\langle\zeta_m\rangle)$. Writing down the isomorphism of group extensions in terms of the exact sequence of Galois groups (5.1) gives the isomorphism of Galois groups and condition (a) (with $\tau=\mathrm{id}$) for this specific choice of $\mathfrak{P}_i$. If we replace the $\mathfrak{P}_i$ by $\mathrm{Gal}(K_m/K)$-conjugates, there is a choice of $\tau$ that makes the diagram commute. The fact that we have an isomorphism of extensions with $f_S$ implies that the isomorphism $f:\mathrm{Gal}(L(\mathfrak{p}_1)/K)\xrightarrow{\sim}\mathrm{Gal}(L(\mathfrak{p}_2)/K)$ respects the Artin map $K_{\mathfrak{q}}^*\to\mathrm{Gal}(L(\mathfrak{p}_i)/K)$ for each $\mathfrak{q}\in S$. Let the local field $F\supset L(\mathfrak{p}_i)$ be the extension of $K_{\mathfrak{q}}$ that corresponds by local class field theory to the kernel of this map, and $D_i\subset G_i=\mathrm{Gal}(L(\mathfrak{p}_i)/K)$ the image of $K_{\mathfrak{q}}^*$ under the Artin map. Then $D_i\cong\mathrm{Gal}(F/K_{\mathfrak{q}})$ acts naturally on $F$, and with the natural

left action of $D_i$ on $G_i$ we have a $\mathrm{Gal}(L(\mathfrak{p}_i)/K)$-isomorphism

$$\begin{aligned} L(\mathfrak{p}_i) \otimes_K K_\mathfrak{q} &\cong_{G_i} \mathrm{Map}_{D_i}(G_i, F) \\ \alpha \otimes x &\longmapsto (g \mapsto g(\alpha) \cdot x). \end{aligned}$$

Here $G_i = \mathrm{Gal}(L(\mathfrak{p}_i)/K)$ acts on the left hand side via the first factor, and on the right hand side by $(g\phi)(g') = \phi(g'g)$. As $f : G_1 \xrightarrow{\sim} G_2$ maps $D_1$ to $D_2$, condition (b) follows.

The argument for the converse is essentially the same, as the only thing we have done is translating the equivalence in the Ext-group from 5.6 into the existence of an isomorphism $f$ satisfying (a) and (b). □

## 6. Applications

In this section, we use the previous theorems to derive density statements for primes that give rise to a ray class group having some prescribed extension structure.

Let $K$ be a number field and $m$ a positive integer. We start with a question that has been studied by G. Cornell [10]: for which primes $\mathfrak{p}$ does $K$ have a cyclic extension $F$ of degree $m$ that is totally and only ramified at $\mathfrak{p}$, and does the set of such primes have a natural density inside the set of all primes of $K$? The results of the previous sections allow us to answer this question quite precisely for primes $\mathfrak{p} \nmid m$, because such an extension is then contained in the extension $L(\mathfrak{p}) = L(\mathfrak{p}, \mathfrak{d}, m) \supset K$ from the previous section with $\mathfrak{d} = 1$. More precisely, the question is whether there exists a totally ramified extension of degree $m$ of $K$ such that the compositum with the Hilbert class field $H$ of $K$ yields $L(\mathfrak{p})$. By looking at the corresponding exact sequence of Galois groups in the ray class group formulation (5.3), we see that there exists a cyclic extension of degree $m$ that is totally and only ramified at $\mathfrak{p} \nmid m$ if and only if $k_\mathfrak{p}^*/(\mathrm{im}[E]k_\mathfrak{p}^{*m})$ has order $m$ and the exact sequence

$$0 \longrightarrow k_\mathfrak{p}^*/(\mathrm{im}[E] \cdot k_\mathfrak{p}^{*m}) \longrightarrow \mathcal{C}_\mathfrak{p}/\alpha[k_\mathfrak{p}^{*m}] \longrightarrow Cl \longrightarrow 0$$

is split. We saw already that the set of primes $\mathcal{S}$ satisfying the first condition is the set of primes splitting completely in $K_m(\sqrt[m]{E})/K$. In particular, its density is

$$\delta(\mathcal{S}) = [K_m(\sqrt[m]{E}) : K]^{-1}$$

by Čebotarev's density theorem.

**6.1 Theorem.** *Let $K$ be a number field, $E$ the unit group of its ring of integers, $m \in \mathbb{Z}_{>0}$ an integer and $\mathfrak{p}$ a finite prime of $K$ that does not divide $m$. Define $W \subset K^*$ by*

$$W = \{\alpha \in K^* : (\alpha) \text{ is an } m\text{-th ideal power}\}$$

*and write $S$ for the set of primes of $K$ that split completely in $K_m(\sqrt[m]{E})/K$. Then there exists a cyclic extension of degree $m$ of $K$ that is totally and only ramified at $\mathfrak{p}$ if and only if $\mathfrak{p}$ splits completely in the field $M = K(\zeta_m, \sqrt[m]{W})$.*

*If $\Sigma$ denotes the set of such primes, its density satisfies*

$$\delta(\Sigma) \geq \frac{1}{\mu}\delta(S),$$

*where $\mu$ is the order of $m$-torsion subgroup of the class group of $K$. Equality holds when $m$ is prime or an odd prime power, and also when $K$ contains a root of unity of order $r$, with $r$ the product of the odd primes in $m$ and, when $4|m$, a factor 4.*

**Proof.** In view of the remark preceding the theorem, the first statement is just a rewording of 5.12. For the second statement, we apply Čebotarev's density theorem to get

$$\delta(\Sigma) = [M : K]^{-1} = [M : K_m(\sqrt[m]{E})]^{-1}\delta(S).$$

Again by 5.12, the degree $[M : K_m(\sqrt[m]{E})] = \#\mathrm{Gal}(M/K_m(\sqrt[m]{E}))$ is bounded by (and in the cases from theorem 5.13 that are mentioned equal to) $\#\mathrm{Ext}(C, \langle\zeta_m\rangle)$. It follows from theorem 3.5 that the latter order equals $\mu$. The result follows. □

One can also ask for which primes $\mathfrak{p}$ of $K$ the full ray class field of conductor $\mathfrak{p}$ of $K$ is the compositum of the Hilbert class field of $K$ and an extension of $K$ that is totally ramified at the prime $\mathfrak{p}$. This comes down to studying the splitting behaviour of the exact sequence

$$0 \longrightarrow k_{\mathfrak{p}}^*/\mathrm{im}[E] \longrightarrow C_{\mathfrak{p}} \longrightarrow Cl \longrightarrow 0. \tag{6.2}$$

For varying $\mathfrak{p}$, the behaviour of this sequence cannot be described by a fixed governing field $M$ as in 6.1, so it is not immediately clear that the set of primes $\mathfrak{p}$ for which the sequence splits possesses a natural density. The next theorem answers the most obvious questions concerning the splitting behaviour of (6.2). It turns out that for any $K$ having a non-trivial class group, there is always a set of primes $\mathfrak{p}$ of positive density for which the ray class field $H_{\mathfrak{p}}$ is not the compositum of the Hilbert class field and an extension that is totally ramified at $\mathfrak{p}$. The complementary set of primes already has positive lower density for simple coprimality reasons.

**6.3 Theorem.** *The following holds for the exact sequence $\mathcal{E}_{\mathfrak{p}}$ in (6.2).*

(a) *For any integer $h > 0$, the set of primes $\mathfrak{p}$ for which the order of $k_{\mathfrak{p}}^*/\mathrm{im}[E]$ and $h$ are coprime has positive density.*

(b) *The set of primes $\mathfrak{p}$ for which $\mathcal{E}_{\mathfrak{p}}$ splits has a natural density, and this density is positive.*

(c) *If the class group $C$ of $K$ is non-trivial, the set of primes $\mathfrak{p}$ for which $\mathcal{E}_{\mathfrak{p}}$ does not split has positive density.*

(d) *Suppose $m > 1$ divides the order of $C$. Then the set of primes $\mathfrak{p}$ for which $m$ divides $\#(k_\mathfrak{p}^*/\mathrm{im}[E])$ and $\mathcal{E}_\mathfrak{p}$ does not split has positive density.*

**Proof.** (a) Write $L_k$ for $K_k(\sqrt[k]{E})$. We have already seen in the preceding section that an integer $k$ divides the order of $k_\mathfrak{p}^*/\mathrm{im}[E]$ if and only if $\mathfrak{p}$ splits completely in $L_k/K$ and does not divide $k$. Thus, the order of $k_\mathfrak{p}^*/\mathrm{im}[E]$ is coprime to a given number $h$ if and only if the prime $\mathfrak{p}$ does not split completely in any of the fields $L_q$ for which $q$ is a prime divisor of $h$ and $\mathfrak{p} \nmid q$. There are only finitely many primes $\mathfrak{p}$ dividing $h$, which we further exclude from consideration since they are irrelevant for density statements. By the Čebotarev density theorem, the statement in (a) is now reduced to showing that there are elements in the Galois group $\mathrm{Gal}(L_h/K)$ that are not the identity on any of the fields $L_q$ with $q$ a prime divisor of $h$. We prove this by setting $q_0 = 1$, arranging the prime divisors of $h$ in ascending order $q_1 < q_2 < \ldots < q_t$ and showing that the inclusions

$$L_{q_0} \cdot L_{q_1} \cdot L_{q_2} \cdot \ldots \cdot L_{q_{i-1}} \subset L_{q_0} \cdot L_{q_1} \cdot L_{q_2} \cdot \ldots \cdot L_{q_{i-1}} \cdot L_{q_i}$$

are strict for $i = 1, 2, \ldots, t$. We note first that none of the prime factors of the degree $[L_q : K]$ exceeds $q$, and that $q$ is one of them unless $E$ is finite and $\zeta_q \notin K$. As the $i$-th inclusion is strict if $q_i$ divides $[L_{q_i} : K]$, we may further assume that $E$ is finite, so $K = \mathbb{Q}$ or $K$ is imaginary quadratic. If $q_i \geq 5$, the $i$-th inclusion is strict because $q_i$ has ramification indices over $\mathbb{Q}$ that are at most 2 on the left hand side and at least $q_i - 1$ on the right hand side. The inclusion $K \subset L_2$ is strict because $\zeta_2 = -1 \in K$. The inclusion $L_2 \subset L_2 L_3$ is strict for discriminant $\Delta_K = 1$, $-3$ and $-4$ by direct verification and for $\Delta_K < -4$ because $\zeta_3 \notin L_2 = K(\mathrm{i})$. This proves (a).

(b) Let $h$ be the order of $Cl$. In view of (a), we only have to prove that the set of primes for which $\mathcal{E}_\mathfrak{p}$ is split has a density at all. We will only consider $\mathfrak{p}$ that do not divide $h$. Write $M_k$ for $K_k(\sqrt[k]{W_k})$, where $W_k$ is the subgroup of elements of $K^*$ that generate $k$-th ideal powers. Note that $M_k \supset L_k$. Define the infinite field extension $M/K$ by

$$M = K_{h^\infty}(\sqrt[h^\infty]{W_{h^\infty}}) = \bigcup_{i=0}^{\infty} M_{h^i}.$$

For each finite divisor $d$ of $h^\infty$—the notation explains itself—we define conjugation invariant subsets $A_d$ and $B_d$ of $\Gamma = \mathrm{Gal}(M/K)$ as follows. For an element $\sigma \in \Gamma$ we let

$$\sigma \in A_d \iff \sigma|M_d = \mathrm{id} \text{ and } \sigma|L_{dq} \neq \mathrm{id} \text{ for each prime } q|h;$$
$$\sigma \in B_d \iff \sigma|L_d = \mathrm{id},\ \sigma|M_d \neq \mathrm{id} \text{ and } \sigma|L_{dq} \neq \mathrm{id} \text{ for each prime } q|h.$$

Note that each set $A_d$ or $B_d$ is the inverse image of a subset of $\mathrm{Gal}(M_{dh}/K)$ under the canonical surjection. We define $A \subset \Gamma$ as the union of all sets $A_d$, with $d$ ranging over the

finite divisors of $h^\infty$, and $B$ likewise. Then $A$ and $B$ are the disjoint union of open subsets of $\Gamma$, and $A \cap B = \emptyset$. The complement of $A \cup B$ in $\Gamma$ consists of those $\sigma \in \mathrm{Gal}(M/K)$ that are the identity on $\cup_{i=0}^{\infty} L_{q^i}$ for at least one prime divisor $q$ of $h$, so they belong to a finite union of closed subgroups of infinite index in $\Gamma$.

Let $\nu$ be the Haar measure on $\Gamma$, normalized such that $\nu(\Gamma) = 1$. The primes $\mathfrak{p}$ of $K$ with $\gcd(\#(k_\mathfrak{p}^*/\mathrm{im}[E]), h^\infty) = d$ such that $\mathcal{E}_\mathfrak{p}$ splits (does not split) are exactly those primes that have Frobenius elements in $A_d$ ($B_d$). Thus, the splitting of $\mathcal{E}_\mathfrak{p}$ depends on whether the Frobenius elements of $\mathfrak{p}$ in $\Gamma$ are in $A$ or in $B$. It is easily seen that the sets of primes with Frobenius in $A$ and $B$ have respective lower densities $\geq \nu(A)$ and $\geq \nu(B)$. We have $\nu(A) + \nu(B) = 1$ because $\nu(\Gamma \setminus (A \cap B)) = 0$, such that these lower densities are in fact densities, equal to $\nu(A)$ and $\nu(B)$. This proves (b).

(c) Rather than deducing (c) from (d), we give a short proof. Take a prime divisor $m$ of $\#\mathcal{C}$. Then we have an isomorphism in corollary 5.12 by 5.13 (3). As $\mathrm{Ext}(\mathcal{C}, \langle \zeta_m \rangle)$ is non-trivial, there is a set of primes of positive density in $K$ for which the sequence $\mathcal{E}_\mathfrak{p}$ 'modulo $m$-th powers' has a well defined, non-trivial image in $\mathrm{Ext}(\mathcal{C}, \langle \zeta_m \rangle)$ by the choice of a prime over $\mathfrak{p}$ in $K_m$. It follows that $\mathcal{E}_\mathfrak{p}$ does not split for these $\mathfrak{p}$. We know from (b) that the set of $\mathfrak{p}$ for which $\mathcal{E}_\mathfrak{p}$ does not split has a natural density, and the argument above shows that it is positive.

(d) We use the argument in (c), but instead of isomorphy in 5.12, which need not hold for arbitrary $m$, we use the fact that—in the terminology of the proof of (b)—there are non-trivial Artin symbols in $\mathrm{Gal}(M_m/L_m)$. Primes $\mathfrak{p} \nmid m$ that have a Frobenius in $\mathrm{Gal}(M_m/K)$ that is a non-trivial element of $\mathrm{Gal}(M_m/L_m)$ satisfy $m | \#(k_\mathfrak{p}^*/\mathrm{im}[E])$ and give rise to a sequence $\mathcal{E}_\mathfrak{p}$ that does not split. We now have to prove that the extension $M_m \supset L_m$ has degree $> 1$. By Kummer theory, the degree is equal to the order of $W_m {K_m^*}^m / E {K_m^*}^m \cong W_m / (W_m \cap E {K_m^*}^m)$. We have a surjective map

$$g : W_m / E {K^*}^m \to W_m / (W_m \cap E {K_m^*}^m)$$

and the first group, which is isomorphic to the $m$-torsion subgroup in $\mathcal{C}$, has order divisible by $m$ by assumption. We are done if we can show that $\ker g$ has order $< m$. Let $A \subset K_m^*$ be the subgroup of elements whose $m$-th power lies in $K^*$. By van Tieghem's theorem 4.4, the image $A^\#$ of $A$ in $K_m^\# / K^\#$ has order dividing $[K_m : K]$, and $[K_m : K] < m$ because $m > 1$. From the inclusion

$$\ker g = (W_m \cap E {K_m^*}^m) / E {K^*}^m \subset (K^* \cap E {K_m^*}^m) / E {K^*}^m$$

and the fact that the natural surjection

$$A \xrightarrow{m} (K^* \cap E {K_m^*}^m) / E {K^*}^m$$

factors via $A/(A \cap Z_{K_m} K^*) = A^{\#}$, we conclude that $\#\ker g < m$. $\square$

**Remarks.** It is not true that there are always infinitely many primes $\mathfrak{p}$ in $K$ for which $\gcd(\#(k_{\mathfrak{p}}^*/\mathrm{im}[E]), h)$ has a prescribed value. For $K = \mathbb{Q}(\sqrt{-2})$ one has $K(\sqrt{E}) = K_4(\sqrt[4]{E}) = \mathbb{Q}(\zeta_8)$, so $\#(k_{\mathfrak{p}}^*/\mathrm{im}[E])$ is either odd or divisible by 4.

If $C$ is the $p$-primary part of $\mathcal{C}$ and $B$ is realized as the $p$-primary part of $k_{\mathfrak{p}}^*/\mathrm{im}[E]$ for a set of primes $\mathfrak{p}$ of positive density, it does not follow that $B \times C$ is the $p$-primary part of the extension $\mathcal{E}_{\mathfrak{p}}$ for infinitely many $\mathfrak{p}$. For $K = \mathbb{Q}(\sqrt{-5})$ one has $\mathcal{C} \cong \mathbb{Z}/2\mathbb{Z}$ and

$$\begin{gathered} K(\sqrt{E}) = K(\mathrm{i}) \\ K(\sqrt{W_2}) = K(\mathrm{i}, \sqrt{2}) = K(\zeta_8) = K_4(\sqrt[4]{E}) = K_4(\sqrt[4]{W_4}) \\ K_8(\sqrt[8]{E}) = K_8(\sqrt[8]{W_8}) = K(\zeta_{16}), \end{gathered}$$

so for this $K$ we can realize $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ as the 2-primary part of infinitely many $\mathcal{E}_{\mathfrak{p}}$, but not $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/8\mathbb{Z}$.

The examples above show that there may be 'unexpected inclusions' between the fields $M_m$ and $L_m$ in case the unit group $E$ of $K$ is finite. Even if $E$ is infinite, this may happen.

Take $K = \mathbb{Q}(\sqrt{3 \cdot 13}, \sqrt{-3 \cdot 7 \cdot 61})$. The quadratic subfields of $K$ of discriminant $-4 \cdot 3 \cdot 7 \cdot 61$ and $-7 \cdot 13 \cdot 61$ have class numbers $2^3 \cdot 3$ and $2^2 \cdot 13$, so $h_K$ is divisible by $2^3 \cdot 3 \cdot 13$. We claim that

$$L_2 \subset K(\zeta_{39}) \subset L_{3 \cdot 13},$$

so that $k_{\mathfrak{p}}^*/\mathrm{im}[E]$ cannot have odd order if 3 and 13 divide it. Note that all these primes are relevant for the splitting behaviour of $\mathcal{E}_{\mathfrak{p}}$.

The fundamental unit $\epsilon = 25 + 4\sqrt{39}$ of $\mathbb{Q}(\sqrt{39})$ is also a fundamental unit in $K$, and one has $L_2 = K(\mathrm{i}, \sqrt{\epsilon})$. The equation

$$\epsilon = \frac{1+\epsilon}{1+\epsilon^{-1}} = N_{\mathbb{Q}(\sqrt{39})/\mathbb{Q}}(1+\epsilon) \cdot (1+\epsilon^{-1})^{-2} = 4 \cdot 13 \cdot (1+\epsilon^{-1})^{-2}$$

shows that

$$L_2 = K(\mathrm{i}, \sqrt{13}) = K(\sqrt{-3}, \sqrt{13}) \subset K(\zeta_{39}).$$

The following theorem that shows that unexpected inclusions between the fields $L_k$ can only arise for certain small values of $k$ that contain some 'bad primes' to a low exponent. More precisely, we can find infinitely many $\mathfrak{p}$ for which the order of $k_{\mathfrak{p}}^*/\mathrm{im}[E]$ has a prescribed $q$-part at finitely many primes $q$, provided that this $q$-part is sufficiently large when $q$ is bad.

We write $m_{\mathfrak{p}}$ for the order of the group $k_{\mathfrak{p}}^*/\mathrm{im}[E]$.

**6.4 Theorem.** *Given a number field $K$, there exists a positive integer $t|2^\infty \cdot \Delta(K/\mathbb{Q})^\infty$ such that, given any two positive integers $k$ and $s|k^\infty$ satisfying $\gcd(t,k^\infty)|s$, the set of primes $\mathfrak{p}$ for which*

$$\gcd(m_\mathfrak{p}, k^\infty) = s$$

*has positive density.*

**Proof.** Let $V$ be the set of primes dividing $2 \cdot \Delta(K/\mathbb{Q})$ and write $L_n$ for $K_n(\sqrt[n]{E})$. As in the proof of 6.3(a), the problem comes down to finding $\sigma$ in the absolute Galois group of $K$ for which

$$\sigma|L_s = \mathrm{id}, \text{ but } \sigma|L_{qs} \neq \mathrm{id} \text{ for each prime divisor } q \text{ of } k.$$

Suppose first that $q \notin V$. We claim that then for each number $d$ that is coprime to $q$, we have

$$L_d \cap L_{q^a} = K.$$

Observe first that $K(\zeta_{q^a})$ is the largest abelian subextension of $L_{q^a}/K$. As $L_d/K$ is unramified at $q$ and $K(\zeta_{q^a})/K$ is totally ramified at $q$ by our hypotheses, the largest abelian subextension of $(L_d \cap L_{q^a})/K$ is $K$ itself. As $(L_d \cap L_{q^a})/K$ is solvable, the claim follows. (This elegant argument is taken from [22].)

It is immediate from the definition that $L_m L_n = L_{\mathrm{lcm}(m,n)}$. Further $L_{q^a} \neq L_{q^{a+1}}$ for $q \notin V$ and $a \geq 1$ by proposition 4.3. Thus, the claim above implies that $L_{q^a}$ is not contained in a compositum of fields $L_d$ with $\mathrm{ord}_q(d) < a$ when $q \notin V$. Consequently, we can further assume that all prime divisors of $k$ are in $V$.

Let $m$ be the product of the primes in $V$. As 4.3 implies that all inclusions $L_{q^a} \subset L_{q^{a+1}}$ are strict for $a$ sufficiently large, we can define an integer $a(q)$ for each $q \in V$ by

$$a \geq a(q) \Rightarrow L_{mq^{a-1}} \subsetneq L_{mq^a}.$$

Note that the degrees of these extensions are powers of $q$. They remain strict when $m$ is multiplied by some divisor of $k^\infty$, because the primes $q' \neq q$ in this divisor give extensions of both sides of the inclusion of degree coprime to $q$.

Set $t = \prod_{q \in V} q^{a(q)}$, and denote by $q_1, q_2, \ldots, q_r$ the prime divisors of $k$. The assumption on $s$ implies that the inclusions in

$$L_s \subset L_{sq_1} \subset L_{sq_1q_2} \subset \ldots \subset L_{sq_1q_2\ldots q_r}$$

are strict. It follows that we can find an element $\sigma$ in the absolute Galois group of $K$ that satisfies our requirements. □

Rather than restricting ourselves to the ray class field of $K$ of conductor $\mathfrak{p}$ as an extension of the Hilbert class field $H$ of $K$, we may as well consider the ray class field $H_{\mathfrak{d}\mathfrak{p}}$ of $K$ of

conductor $\mathfrak{d}\mathfrak{p}$ as an extension of the ray class field $H_\mathfrak{d}$ of $K$ for arbitrary conductor $\mathfrak{d}$. The exact sequence

$$0 \longrightarrow k_\mathfrak{p}^*/\mathrm{im}[E_\mathfrak{d}] \xrightarrow{\alpha} C_{\mathfrak{d}\mathfrak{p}} \longrightarrow C_\mathfrak{d} \longrightarrow 0 \tag{6.5}$$

corresponding to this extension of Galois groups was derived in lemma 5.2. If we are only interested in the subfield $L(\mathfrak{p})$ of $H_{\mathfrak{d}\mathfrak{p}}$ in which all ramification indices at $\mathfrak{p}$ divide $m$, we have our familiar sequence

$$0 \longrightarrow k_\mathfrak{p}^*/(\mathrm{im}[E_\mathfrak{d}] \cdot k_\mathfrak{p}^{*m}) \longrightarrow C_{\mathfrak{d}\mathfrak{p}}/k_\mathfrak{p}^{*m} \longrightarrow C_\mathfrak{d} \longrightarrow 0. \tag{6.6}$$

We have seen in examples 5.14 and 5.16 that there are choices of $m$ and $\mathfrak{d}$ such that the extension groups $\mathrm{Ext}(C_\mathfrak{d}, k_\mathfrak{p}^*/\langle\zeta_m\rangle)$ contain elements that cannot be realized by sequences of the form (6.6). It is not in general an easy matter to determine which extensions are arithmetical extensions. The proof of theorem 6.3 shows that roughly speaking, arithmetical obstructions to group theoretically possible extension types occur when there are 'unexpected inclusions' between the fields $L_k = K_k(\sqrt[k]{E_\mathfrak{d}})$ and $M_k = K_k(\sqrt[k]{W_{k,\mathfrak{d}}})$ for certain values of $k$. The situation is less transparent than for $\mathfrak{d} = 1$, and generalizations of theorem 6.3 for the sequence (6.5) are no longer true for all choices of $K$ and $\mathfrak{d}$.

For instance, if $K$ contains $\zeta_m$ and $\mathfrak{d}$ is chosen (cf. 7.1) such that $E_\mathfrak{d} \subset E^m$, then the order of $k_\mathfrak{p}^*/(\mathrm{im}[E_\mathfrak{d}] \cdot k_\mathfrak{p}^{*m})$ is obviously divisible by $m$ for all $\mathfrak{p}|m$. This shows that 6.3 (a) can be false if one replaces $E$ by $E_\mathfrak{d}$.

Also, 6.3 (c) can be wrong with $C_\mathfrak{d}$ in the place of $C$. An example of this phenomenon is given by example 5.16.

We prove that theorem 6.3 (b) holds unchanged for the sequence (6.5).

**6.7 Theorem.** *Let $K$ be a number field and $\mathfrak{d}$ a cycle of $K$. Then the set of primes $\mathfrak{p}$ of $K$ for which the ray class field $H_{\mathfrak{d}\mathfrak{p}}$ is a compositum of the ray class field $H_\mathfrak{d}$ modulo $\mathfrak{d}$ of $K$ and an extension of $K$ that is totally and only ramified at $\mathfrak{p}$ possesses a natural density inside the set of all primes of $K$, and this density is positive.*

**Proof.** We may exclude the primes $\mathfrak{p}$ that are archimedean or divide $\mathfrak{d}$. Then the primes $\mathfrak{p}$ considered in the theorem are the primes for which the sequence (6.5) is split. The proof is a straightforward generalization of the proof given for $\mathfrak{d} = 1$. One only has to replace $E$ by $E_\mathfrak{d}$ and $W$ by the group $W_0$ from theorem 5.15 in the definition of the fields $L_k$ and $M_k$ to obtain the density result. Positivity is slightly more subtle because we do not have the equivalent of 6.3 (a) for the sequence 6.5.

Let $h$ be the order of $C_\mathfrak{d}$. In the notation from the proof of 6.3 (b), it suffices to prove that there is a finite divisor $d|h^\infty$ for which the subset $A_d$ of $\mathrm{Gal}(M/K)$ is non-empty. This can be done by showing that the inclusions in

$$M_d \subset M_d L_{dq_1} \subset M_d L_{dq_1 q_2} \subset \ldots \subset M_d L_{dq_1 q_2 \ldots q_r}$$

are strict for some $d|h^\infty$, where $q_1, q_2, \ldots, q_r$ are the prime divisors of $h$.

The degree of the extensions $L_{q^a}$ for $q$ a prime number can be computed as in 4.3. We do not need the precise result, only the fact that the extensions $L_{q^a} \subset L_{q^{a+1}}$ is a non-trivial extension of $q$-power degree for $a$ sufficiently large. This implies that the inclusions

$$(*) \qquad L_d \subset L_{dq_1} \subset L_{dq_1q_2} \subset \ldots \subset L_{dq_1q_2\ldots q_r}$$

are strict for $d$ sufficiently divisible by each of the $q_i$. We may assume $h|d$. As the elements $w \in W_0 = W_0(d)$ are generators of ideals $\mathfrak{a}^d$ for which $[\mathfrak{a}]$ is a $d$-torsion element in $C_\mathfrak{d}$, we have $W_0(d) = E_\mathfrak{d} W_0(h)^{d/h}$. This implies that $M_d = M_h L_d$, so we want the inclusions in $(*)$ to remain strict when composites are taken with $M_h$. As $M_h/K$ is finite, it can only destroy the strictness of finitely many inclusions $L_{q^a} \subset L_{q^{a+1}}$ under taking composites with $M_h$. We conclude that we obtain strict inclusions in our original chain of fields by taking $d$ divisible by a sufficiently high power of each of the $q_i$. □

The argument above also shows that the proof of theorem 6.4 remains valid when $m_\mathfrak{p}$ is taken to be the order of $k_\mathfrak{p}^*/\mathrm{im}[E_\mathfrak{d}]$. We see that 6.3 (a) fails when we replace $E$ by arbitrary $E_\mathfrak{d}$, but not the related statement 6.4.

# CHAPTER III

# Ray class group extensions

## 7. Equivalence of ray class group extensions.

In the preceding chapter, we have considered group extensions depending on a single variable prime $\mathfrak{p}$. The theorems given there can be extended to extensions depending on a fixed number of primes. The proof of such a theorem consists of a reduction to the one-variable case based on the following lemma. We use the notation $W_{\mathfrak{f}}$ from (2.6).

**7.1 Lemma.** *Let $T$ be a finite set of primes of a number field $K$, and $m$ a positive integer. Then there exists a cycle $\mathfrak{f}$ of $K$ that is not divisible by any of the primes in $T$, and for which all units in $E_{\mathfrak{f}} = E \cap W_{\mathfrak{f}}$ are $m$-th powers in $K$.*

**Proof.** This has been proved by Chevalley for an arbitrary finitely generated subgroup of $K^*$ in the place of $E$, see [8]. □

We now come to our more variable generalization of 5.17.

**7.2 Theorem.** *Let $K$ be a number field, $\mathfrak{d}$ a cycle in $K$ and $m, t \in \mathbb{Z}_{>0}$ two positive integers. For each set of $t$ primes $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_t$ of $K$, write $L(\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_t) = L(\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_t, \mathfrak{d}, m)$ for the maximal abelian extension of conductor dividing $\mathfrak{d}\mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_t$ of $K$ in which the ramification indices at all $\mathfrak{p}_i$ divide $m$. Write $H_{\mathfrak{d}}$ for the ray class field of conductor $\mathfrak{d}$ of $K$. Let $S$ be a finite set of primes of $K$ and define $W \subset K^*$ by*

$$W = W_{S,\mathfrak{d},m} = \{x \in K^* : \operatorname{ord}_{\mathfrak{q}}(x) \equiv 0 \bmod m \text{ for all finite } \mathfrak{q} \notin S \text{ and } x \equiv 1 \bmod^* \mathfrak{q}^{\operatorname{ord}_{\mathfrak{q}}(\mathfrak{d})} \text{ for all } \mathfrak{q} \in D \setminus S\}.$$

*If $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_t$ and $\mathfrak{p}'_1, \mathfrak{p}'_2, \ldots, \mathfrak{p}'_t$ are two sequences of $t$ distinct finite primes of $K$ not in $m\mathfrak{d}$ or $S$, and the primes $\mathfrak{p}_i$ and $\mathfrak{p}'_i$ have the same Artin class in $\operatorname{Gal}(K_m(\sqrt[m]{W})/K)$ for each $i = 1, 2, \ldots, t$, then there exists an isomorphism*

$$f : \operatorname{Gal}(L(\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_t)/K) \xrightarrow{\sim} \operatorname{Gal}(L(\mathfrak{p}'_1, \mathfrak{p}'_2, \ldots, \mathfrak{p}'_t)/K)$$

*that respects the projections onto $\operatorname{Gal}(H_{\mathfrak{d}}/K)$ such that the following is satisfied:*

(a) *for $i = 1, 2, \ldots, t$, the $f$-image of the inertia group of $\mathfrak{p}_i$ is the inertia group of $\mathfrak{p}'_i$.*

(b) *for each prime $\mathfrak{q}$ of $K$ in $S$, there is an isomorphism of $K_{\mathfrak{q}}$-algebras*

$$L(\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_t) \otimes_K K_{\mathfrak{q}} \cong L(\mathfrak{p}'_1, \mathfrak{p}'_2, \ldots, \mathfrak{p}'_t) \otimes_K K_{\mathfrak{q}}$$

*such that the group actions of $\operatorname{Gal}(L(\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_t)/K)$ on $L(\mathfrak{p}'_1, \mathfrak{p}'_2, \ldots, \mathfrak{p}'_t) \otimes K_{\mathfrak{q}}$ via this isomorphism and via $f$ coincide. Here $K_{\mathfrak{q}}$ is the completion of $K$ at $\mathfrak{q}$.*

**Proof.** As in (5.1), there is an exact sequence

$$0 \longrightarrow \operatorname{Gal}(L(\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_t)/H_{\mathfrak{d}}) \longrightarrow \operatorname{Gal}(L(\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_t)/K) \longrightarrow \operatorname{Gal}(H_{\mathfrak{d}}/K) \longrightarrow 0.$$

When we rewrite this sequence in terms of ray class groups, we arrive at an analogue of (5.3) in which the group $k_{\mathfrak{p}}^*/(\mathrm{im}[E_{\mathfrak{d}}]\cdot k_{\mathfrak{p}}^{*m})$ gets replaced by $(\prod_{i=1}^t k_{\mathfrak{p}_i}^*)\ /\ (\mathrm{im}[E_{\mathfrak{d}}]\prod_{i=1}^t {k_{\mathfrak{p}_i}^*}^m)$. Assume first that $E_{\mathfrak{d}} \subset E^m$. Then our Galois group fits in an exact sequence

$$0 \longrightarrow \prod_{i=1}^{t}(k_{\mathfrak{p}_i}^*/{k_{\mathfrak{p}_i}^*}^m) \longrightarrow \mathrm{Gal}(L(\mathfrak{p}_1,\mathfrak{p}_2,\ldots,\mathfrak{p}_t)/K) \longrightarrow \mathcal{C}_{\mathfrak{d}} \longrightarrow 0.$$

Moreover, the homomorphism $f_S : \Sigma \to \mathcal{C}_{\mathfrak{d}}$ from (5.4) admits a canonical lift to $\phi_S : \Sigma \to \mathrm{Gal}(L(\mathfrak{p}_1,\mathfrak{p}_2,\ldots,\mathfrak{p}_t)/K)$. Denote by $m_i$ the order of $k_{\mathfrak{p}_i}^*/{k_{\mathfrak{p}_i}^*}^m$. Then we obtain an element $\mathcal{E}(\mathfrak{P}_1,\mathfrak{P}_2,\ldots,\mathfrak{P}_t) \in \mathrm{Ext}(f_S;\prod_{i=1}^t\langle\zeta_{m_i}\rangle)$ for every choice of primes $\mathfrak{P}_i|\mathfrak{p}_i$ in $K_{m_i} = K(\zeta_{m_i})$. By functorial properties of the Ext-functor, we have a canonical isomorphism

$$\mathrm{Ext}(f_S;\prod_{i=1}^{t}\langle\zeta_{m_i}\rangle) \cong \prod_{i=1}^{t}\mathrm{Ext}(f_S;\langle\zeta_{m_i}\rangle).$$

Under this isomorphism, the extension $\mathcal{E}(\mathfrak{P}_1,\mathfrak{P}_2,...,\mathfrak{P}_t)$ corresponds to $(\mathcal{E}(\mathfrak{P}_i))_{i=1}^t$, where $\mathcal{E}(\mathfrak{P}_i)$ is an extension of the type studied in section 5. This shows that isomorphism of 'multi-variable extensions' is the same as isomorphism of the 'one-variable extensions' for each of the $t$ components. Our assumptions on the primes $\mathfrak{p}_i$ and $\mathfrak{p}_i'$ now show that

$$\#(k_{\mathfrak{p}_i'}^*/{k_{\mathfrak{p}_i'}^*}^m) = \#(k_{\mathfrak{p}_i}^*/{k_{\mathfrak{p}_i}^*}^m) = m_i$$

and that $\mathrm{Gal}(L(\mathfrak{p}_1,\mathfrak{p}_2,\ldots,\mathfrak{p}_t)/K)$ and $\mathrm{Gal}(L(\mathfrak{p}_1',\mathfrak{p}_2',\ldots,\mathfrak{p}_t')/K)$ are isomorphic extensions of $f_S$ with $\prod_{i=1}^t\langle\zeta_{m_i}\rangle$ for a suitable choice of primes $\mathfrak{P}_i$ and $\mathfrak{P}_i'$ in $K_{m_i}$. The corresponding isomorphism $f$ between the Galois groups sends the inertia group $\langle\zeta_{m_i}\rangle$ at $\mathfrak{p}_i$ in $L(\mathfrak{p}_1,\mathfrak{p}_2,\ldots,\mathfrak{p}_t)$ to the inertia group at $\mathfrak{p}_i'$ in $L(\mathfrak{p}_1',\mathfrak{p}_2',\ldots,\mathfrak{p}_t')$, and property (b) follows as in the proof of 5.17.

For the general case, we enlarge $\mathfrak{d}$ to a cycle $\mathfrak{f} = \mathfrak{d}\mathfrak{g}$ such that $E_{\mathfrak{f}} \subset E^m$. By lemma 5.1, the cycle $\mathfrak{g}$ can be chosen to be coprime to $m\mathfrak{d}$ and the primes in $S$. Let $S'$ be the set of primes occurring either in $S$ or in $\mathfrak{g}$. Then we know by what we just proved that there exists an isomorphism $f$ satisfying the requirements of the theorem with $\mathfrak{f}$ and $S'$ instead of $\mathfrak{d}$ and $S$ whenever $\mathfrak{p}_i$ and $\mathfrak{p}_i'$ are not in $m\mathfrak{d}\mathfrak{g}$ or $S$ and have the same Artin class in $\mathrm{Gal}(K_m(\sqrt[m]{W_{S',\mathfrak{f},m}})/K)$. Under this isomorphism, inertia groups at primes dividing $\mathfrak{g}$ correspond because of condition (b) for the primes in $S'$. If we divide out the subgroup generated by the inertia subgroups of primes in $\mathfrak{g}$ on both sides, we obtain the isomorphism needed for the original problem.

In order to show that we do not need the larger extension $K_m(\sqrt[m]{W_{S',\mathfrak{f},m}})$ of $K$ as a governing field, but only $K_m(\sqrt[m]{W_{S,\mathfrak{d},m}})/K$, we use the freedom we have in the choice of $\mathfrak{g}$. This will also free us of the restriction that $\mathfrak{p}_i$ and $\mathfrak{p}_i'$ be coprime to $\mathfrak{g}$. If $\mathfrak{g}_1$ and $\mathfrak{g}_2$ are

coprime cycles that each satisfy the requirements for $\mathfrak{g}$ above, we have, with corresponding definitions of $S_i'$ and $\mathfrak{f}_i$, an equality

$$K_m(\sqrt[m]{W_{S_1',\mathfrak{f}_1,m}}) \cap K_m(\sqrt[m]{W_{S_2',\mathfrak{f}_2,m}}) = K_m(\sqrt[m]{W_{S,\mathfrak{d},m}}).$$

Indeed, the intersection is unramified at all primes occurring in $\mathfrak{g}_1\mathfrak{g}_2$ and $K_m(\sqrt[m]{W_{S,\mathfrak{d},m}})$ is the largest subextension of $K_m(\sqrt[m]{W_{S_i',\mathfrak{f}_i,m}})/K$ that is unramified at the primes in $\mathfrak{g}_i$. The proof may now be finished by the generality on governing fields that follows. □

**7.3 Theorem.** *Let a cofinite set $A$ of primes of $K$ and an equivalence relation on $A^t$ be given, and suppose that $M_1$ and $M_2$ are normal extensions of $K$ that are unramified at the primes in respective cofinite subsets $A_1$ and $A_2$ of $A$. If $M_1$ and $M_2$ are governing fields for the equivalence relation on $A_1^t$ and $A_2^t$, respectively, then $M_1 \cap M_2$ is a governing field for the equivalence relation on $A_1^t \cup A_2^t$.*

**Proof.** We clearly may take $t = 1$. Write $M = M_1 \cap M_2$, and let $\mathfrak{p}$ and $\mathfrak{q}$ be primes in $A_1 \cup A_2$ that have the same Artin class in $\mathrm{Gal}(M/K)$. Then $\mathfrak{p}$ is unramified in either $M_1/K$ or $M_2/K$, say in $M_1/K$. As $A_1 \cap A_2$ is a cofinite set of primes of $K$, the Čebotarev density theorem implies that there exists $\mathfrak{p}'$ in $A_1 \cap A_2$ that has the same Artin class in $\mathrm{Gal}(M_1/K)$ as $\mathfrak{p}$, which gives an equivalence $\mathfrak{p} \sim \mathfrak{p}'$. Analogously, $\mathfrak{q} \sim \mathfrak{q}' \in A_1 \cap A_2$. As $\mathfrak{p}'$ and $\mathfrak{q}'$ have the same Artin class in $\mathrm{Gal}(M/K)$, we can find a prime $\mathfrak{r} \in A_1 \cap A_2$ that has the same Artin class in $\mathrm{Gal}(M_1/K)$ as $\mathfrak{p}'$, and the same Artin class in $\mathrm{Gal}(M_2/K)$ as $\mathfrak{q}'$. Our assumptions imply that we have equivalences $\mathfrak{p}' \sim \mathfrak{r}$ and $\mathfrak{r} \sim \mathfrak{q}'$. Thus $\mathfrak{p}$ and $\mathfrak{q}$ are equivalent. □

An interesting case of 7.2 arises when we take for $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_t$ the prime factors in $K$ of a prime $\mathfrak{p}$ from a subfield $k$ of $K$. We have to assume here that $\mathfrak{p}$ is unramified in $K/k$. If $K/k$ happens to be Galois, say with group $\Gamma$, and $\mathfrak{d}$ is invariant under $\Gamma$, then the field $L(\mathfrak{p}) = L(\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_t)$ is not only Galois over $K$, but also over the smaller field $k$. Note however that the extension $L(\mathfrak{p})/k$ is not necessarily abelian.

The obvious question that arises is: is there a governing field for the structure of the extensions $L(\mathfrak{p})/k$, when $\mathfrak{p}$ ranges over the primes of $k$ that are coprime to $m\mathfrak{d}$ and $\Delta(K/k)$? More precisely: define for such $\mathfrak{p}$ the field $L(\mathfrak{p})$ as the maximal abelian extension of $K$ of conductor dividing $\mathfrak{d}\mathfrak{p}$ in which the ramification indices over $\mathfrak{p}$ divide $m$, and call $\mathfrak{p}_1$ and $\mathfrak{p}_2$ equivalent if there exists an isomorphism of the Galois groups $\mathrm{Gal}(L(\mathfrak{p}_i)/k)$ that respects the projection onto $\mathrm{Gal}(H_{\mathfrak{d}}/k)$, and realizes analogues of 7.2(a) and (b) over $k$ for a set $S$ of primes of $k$. Does there exist a normal extension $M/k$ that governs this equivalence relation?

The field $K_m(\sqrt[m]{W})$ is a normal extension of $k$ that governs these extensions in a weaker sense by 7.2. It only gives isomorphisms of Galois groups over $K$, and in 7.2(b) a

Galois isomorphism of algebras over $K_{\mathfrak{Q}}$ for each prime $\mathfrak{Q}$ of $K$ lying over a prime in $S$ at a time.

A possible approach to this problem would be via cohomological class field theory, using canonical classes. Canonical classes are elements in the cohomology groups $H^2(\Gamma, \mathrm{Gal}(L(\mathfrak{p})/K))$ that describe the extension of $\Gamma$ with $\mathrm{Gal}(L(\mathfrak{p})/K)$ that is given by $\mathrm{Gal}(L(\mathfrak{p})/k)$. So far, I have not been able to deal with the problem in this way.

A second method is to explicitly construct a group isomorphism $\mathrm{Gal}(L(\mathfrak{p}_1)/k) \xrightarrow{\sim} \mathrm{Gal}(L(\mathfrak{p}_2)/k)$ for $\mathfrak{p}_i$ that have the same Artin class in an extension $K_m(\sqrt[m]{W})/k$, using class field theory over $K$. This can be done if we consider extensions $L(\mathfrak{p})/k$ for which the $L(\mathfrak{p})K_m$ is abelian of exponent $m$ over $K_m = K(\zeta_m)$. This restriction finds its reasons in the fact that extensions of exponent $m$ over $K_m$ can be described by Kummer theory. We will therefore work with the maximal subfield of $L(\mathfrak{p})$ that satisfies this condition instead of $L(\mathfrak{p})$ itself. It should however be noted that this restriction does not affect the problem as far as the mere existence of a governing field is concerned: upon replacing $K$ by $H_{\mathfrak{d}}$, our redefined fields $L(\mathfrak{p})$ contain the original fields $L(\mathfrak{p})$ defined over $K$. The governing field that is obtained remains unramified outside $m\mathfrak{d}$ and $S$, but it will be an extension defined over $H_{\mathfrak{d}}$ instead of over $K$.

Summarizing, we arrive at the following definition of equivalence of fields $L(\mathfrak{p})$ over the field $k$.

**7.4 Definition.** *Suppose $K/k$ is a Galois extension of number fields with group $\Gamma$. Let a $\Gamma$-invariant cycle $\mathfrak{d}$ of $K$, an integer $m \geq 1$ and a finite set $S$ of primes in $k$ be given. For each prime $\mathfrak{p}$ of $k$, write $L(\mathfrak{p}) = L_{K,\mathfrak{d},m}(\mathfrak{p})$ for the maximal abelian extension of $F$ of $K$ such that $FK_m/K_m$ has exponent dividing $m$ and $F/K$ has conductor dividing $\mathfrak{d}\mathfrak{p}$. The maximal subextension of $L(\mathfrak{p})/K$ that has conductor dividing $\mathfrak{d}$ does not depend on $\mathfrak{p}$ and is denoted by $L$. Then two finite primes $\mathfrak{p}_1$ and $\mathfrak{p}_2$ of $k$ that are not in $S$ or $\mathfrak{d}$ and do not divide $m\Delta_{K/k}$ are defined to be $(\mathfrak{d}, m, S)$-equivalent when there exists an isomorphism*

$$f : \mathrm{Gal}(L(\mathfrak{p}_1)/k) \xrightarrow{\sim} \mathrm{Gal}(L(\mathfrak{p}_2)/k)$$

*that respects the projections onto $\mathrm{Gal}(L/k)$ such that the following is satisfied:*

(a) *the $f$-image of the inertia group of any prime above $\mathfrak{p}_1$ is the inertia group of a prime above $\mathfrak{p}_2$.*

(b) *for each prime $\mathfrak{q}$ of $k$ in $S$, there is an isomorphism of $k_{\mathfrak{q}}$-algebras*

$$L(\mathfrak{p}_1) \otimes_k k_{\mathfrak{q}} \cong L(\mathfrak{p}_2) \otimes_k k_{\mathfrak{q}}$$

*such that the group actions of $\mathrm{Gal}(L(\mathfrak{p}_1)/k)$ on $L(\mathfrak{p}_2) \otimes k_{\mathfrak{q}}$ via this isomorphism and via $f$ coincide. Here $k_{\mathfrak{q}}$ is the completion of $k$ at $\mathfrak{q}$.*

It should be pointed out that condition (b) is a strong local condition at the primes $\mathfrak{q} \in S$. If $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are equivalent in the sense of 7.4 and $\mathfrak{q}$ splits as $\mathfrak{r}_1^e \mathfrak{r}_2^e \dots \mathfrak{r}_k^e$ in $L(\mathfrak{p}_1)$, then

$$L(\mathfrak{p}_1) \otimes_k k_{\mathfrak{q}} \cong \prod_{i=1}^{k} L(\mathfrak{p}_1)_{\mathfrak{r}_i}$$

and the existence of the local isomorphism in 7.4(b) implies that there exist primes $\mathfrak{s}_1, \mathfrak{s}_2, \dots, \mathfrak{s}_k$ in $L(\mathfrak{p}_2)$ such that $\mathfrak{q} = \mathfrak{s}_1^e \mathfrak{s}_2^e \dots \mathfrak{s}_k^e$ and $L(\mathfrak{p}_1)_{\mathfrak{r}_i} \cong L(\mathfrak{p}_2)_{\mathfrak{s}_i}$. As in the proof of theorem 5.17 we conclude that $f$ induces isomorphisms between the inertia and decomposition groups at the primes lying over $\mathfrak{q}$ in $L(\mathfrak{p}_1)$ and $L(\mathfrak{p}_2)$.

The isomorphism $f$ establishes a correspondence between the subfields of $L(\mathfrak{p}_1)/k$ containing $k$ and those of $L(\mathfrak{p}_2)/k$, where correspondence of $E_i \subset L(\mathfrak{p}_i)$ for $i = 1$ and 2 means that $f[\mathrm{Gal}(L(\mathfrak{p}_1)/E_1)] = \mathrm{Gal}(L(\mathfrak{p}_2)/E_2)$. An important implication of 7.4(b) is that for an abelian subextension $E_1 \subset F_1$ of $L(\mathfrak{p}_1)/k$ of conductor $\mathfrak{f}$, the corresponding subextension $E_2 \subset F_2$ of $L(\mathfrak{p}_2)/k$ is abelian with a conductor that is locally 'equal' to $\mathfrak{f}$ at primes in $S$ upon identification of $\mathfrak{r}_i$ and $\mathfrak{s}_i$ in the situation above. This equality is a direct consequence of the fact that the extension $E_1 \subset F_1$ completed at the restriction of $\mathfrak{r}_i$ is isomorphic to the extension $E_2 \subset F_2$ completed at the restriction of $\mathfrak{s}_i$. These observations will prove to be useful in chapter IV.

## 8. Construction of governing fields

We will prove an existence theorem for fields governing the equivalence relation 7.4 that does not impose any condition on $K$ or $S$. Just as in 5.11 and 5.12, there are more elegant descriptions of these governing fields under additional hypotheses.

As in section 2, we let $\infty$ be the product of the real primes of $K$. In order to avoid a complicated notation, the set of primes occurring either in a given set or in a certain cycle is denoted in a simple way, e.g. $S \cdot \mathfrak{d} \cdot \infty$ stands for the set of primes occurring in either $S$, $\mathfrak{d}$ or $\infty$ and $\mathfrak{d} \setminus S$ is the set of primes in $\mathfrak{d}$ that are not in $S$. We will also use notations for sets of primes for base field and extension field alike. For instance, depending on the context, $S$ can stand for the set of primes of $K$ that lie over a prime of $k$ that is in $S$. The notation $U_{\mathfrak{p}}^{(k)}$ for the filtration of the local units in the completion—archimedean or non-archimedean—of a number field at $\mathfrak{p}$ is as defined in section 2.

**8.1 Theorem.** *Let a $\Gamma$-invariant cycle $\mathfrak{d}$ of $K$, an integer $m \geq 1$ and a finite set $S$ of primes in $k$ be given, and let $K_m$ be the field obtained from $K$ by adjoining a primitive $m$-th root of unity. Write $S_m$ for the set of primes of $k$ that are either in $S$ or have extensions to $K$ that ramify in $K_m/K$. Define $M$ to be the maximal abelian extension of $K_m$ that satisfies the following conditions:*

(a) $\mathrm{Gal}(M/K_m)$ *is of exponent dividing $m$;*

(b) $M/K_m$ *is unramified outside* $S \cdot (m) \cdot \mathfrak{d} \cdot \infty$;

(c) *for all primes* $\mathfrak{Q}$ *of* $K_m$ *in* $((m) \cdot \mathfrak{d}) \setminus S_m$, *there exists a homomorphism of* $K_m$*-algebras*

$$M \longrightarrow K_{m,\mathfrak{Q}}(\sqrt[m]{U_{\mathfrak{Q}}^{(\mathrm{ord}_{\mathfrak{Q}}(\mathfrak{d}))}})$$

*into the local field that is obtained from the completion of* $K_m$ *at* $\mathfrak{Q}$ *by adjoining all* $m$*-th roots of the local units in* $U_{\mathfrak{Q}}^{(\mathrm{ord}_{\mathfrak{Q}}(\mathfrak{d}))} \subset K_{m,\mathfrak{Q}}^*$.

*Then any two primes* $\mathfrak{p}_1$ *and* $\mathfrak{p}_2$ *of* $k$ *that are not in* $S \cdot (m) \cdot \Delta_{K/k}$ *and have the same Artin class in* $M/k$ *are* $(\mathfrak{d}, m, S)$*-equivalent.*

We will prove a lemma that enables us to reduce to the case that $K$ contains a primitive $m$-th root of unity. It is preceded by an elementary lemma from class field theory.

**8.2 Lemma.** *Let* $L/K$ *be a finite abelian extension of number fields of conductor* $\mathfrak{f}$ *and* $\mathfrak{p}$ *a finite prime of* $K$. *If* $M/K$ *is an arbitrary finite extension that is unramified at* $\mathfrak{p}$, *then* $LM/M$ *is an abelian extension and the maximal divisor of the conductor of* $LM/M$ *consisting of primes over* $\mathfrak{p}$ *only equals* $\mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{f})}$.

**Proof.** Let $\mathfrak{p}$ be a finite prime of $K$ that is unramified in $M/K$, and suppose $k$ is the number of factors $\mathfrak{p}$ in the conductor of $L/K$. It is clear that $LM/M$ is abelian. We have to prove that $\mathfrak{r}^k$ is the exact power of $\mathfrak{r}$ dividing the conductor of $LM/M$ for each prime $\mathfrak{r} \mid \mathfrak{p}$ in $M$. This is equivalent to proving that $U_{\mathfrak{r}}^{(t)}$ is in the kernel of the local Artin map for $LM/M$ at $\mathfrak{r}$ if and only if $t \geq k$. By class field theory [7, 21], there is a commutative diagram

$$\begin{array}{ccc} M_{\mathfrak{r}}^* & \longrightarrow & \mathrm{Gal}((LM)_{\mathfrak{s}}/M_{\mathfrak{r}}) \\ \Big\downarrow{\scriptstyle N_{M_{\mathfrak{r}}/K_{\mathfrak{p}}}} & & \Big\downarrow{\scriptstyle \mathrm{can}} \\ K_{\mathfrak{p}}^* & \longrightarrow & \mathrm{Gal}(L_{\mathfrak{q}}/K_{\mathfrak{p}}). \end{array}$$

The vertical map between the Galois groups is injective, so it suffices to show that one has $N_{M_{\mathfrak{r}}/K_{\mathfrak{p}}}[U_{\mathfrak{r}}^{(t)}] = U_{\mathfrak{p}}^{(t)}$ for all $t \geq 0$. As $M_{\mathfrak{r}}/K_{\mathfrak{p}}$ is unramified, this equality is an elementary fact that can be found in [34, V.3 proposition 3a]. □

**8.3 Lemma.** *It suffices to prove* 8.1 *under the assumption that* $K = K_m$.

**Proof.** Assume the theorem for $K_m$, and let $\mathfrak{d}$, $m$ and $S$ be as in 8.1. If $K = K_m$ there is nothing to prove, so assume that this is not the case. We then observe that the governing field that is given by 8.1 for $(\mathfrak{d}, m, S_m)$-equivalence for the extension $K_m/k$ is exactly the field that 8.1 asserts to be a governing field for $(\mathfrak{d}, m, S)$-equivalence for the extension $K/k$. Thus we are are done if we can show that two primes $\mathfrak{p}_1$ and $\mathfrak{p}_2$ of $k$ that are $(\mathfrak{d}, m, S_m)$-equivalent for the extension $K_m/k$ are $(\mathfrak{d}, m, S)$-equivalent for $K/k$. Obviously, the maximal abelian extension $L(\mathfrak{p}_i)$ of $K$ such that $L(\mathfrak{p}_i)K_m/K_m)$ is of exponent dividing

$m$ and such that $L(\mathfrak{p}_i)/K$ conductor dividing $\mathfrak{d}\mathfrak{p}_i$ is a subfield of the maximal abelian extension $L'(\mathfrak{p}_i)$ of $K_m$ that is of exponent dividing $m$ and conductor dividing $\mathfrak{d}\mathfrak{p}_i$. We are done if we can show that the isomorphism $f'$ : $\mathrm{Gal}(L'(\mathfrak{p}_1)/k) \xrightarrow{\sim} \mathrm{Gal}(L'(\mathfrak{p}_2)/k)$ induces the corresponding isomorphism $f$ for the field extensions $L(\mathfrak{p}_i)/k$. The maximal subextensions $F_i/k$ of $L'(\mathfrak{p}_i)/k$ that are abelian over $K$ certainly correspond under $f$. The field $F_iK_m$ is contained in $L'(\mathfrak{p}_i)$ and the conductor $\mathfrak{f}_{F_i/K}$ equals $\mathfrak{f}_{F_iK_m/K_m}$ at the primes that are unramified in $K_m/K$ by lemma 8.2. Consequently, $\mathfrak{f}_{F_i/K}$ divides $\mathfrak{d}\mathfrak{p}_i$ at the primes that are unramified in $K_m/K$. The fields $L(\mathfrak{p}_i)$ are the maximal subfields of $F_i$ that are of conductor dividing $\mathfrak{d}\mathfrak{p}_i$. These fields correspond under $f$ for $i = 1, 2$, since 7.4(b) and the definition of $S_m$ imply that we have local isomorphisms of the extensions $F_i/K$ at all primes that ramify in $K_m/K$. □

In the rest of the proof we will assume that $K$ contains a primitive $m$-th root of unity, which implies that $S_m = S$. Under this assumption, no confusion will arise from our notation $\sqrt[m]{V}$ for a subset $V$ of $K$ to denote the set of all elements $x$ in some algebraic closure of $K$ that satisfy $x^m \in V$.

For the proof of 8.1, we take two distinct finite primes $\mathfrak{p}_1$ and $\mathfrak{p}_2$ of $k$ outside $(m\Delta_{K/k})\cdot \mathfrak{d}\cdot S$ for which $[\mathfrak{p}_1, M/k] = [\mathfrak{p}_2, M/k]$. For brevity of notation, we write $L_i = L(\mathfrak{p}_i)$, $i = 1, 2$. Note that $L_1 \cap L_2 = L$. By Kummer theory, there exist subgroups $W_i$ of $K^*$ containing $K^{*m}$ such that $L_i = K(\sqrt[m]{W_i})$. There is a perfect pairing

$$\begin{aligned} \kappa : \quad \mathrm{Gal}(L_i/K) \times W_i/K^{*m} &\to \langle \zeta_m \rangle, \\ (\sigma, w) &\mapsto \sigma(\sqrt[m]{w})/\sqrt[m]{w}. \end{aligned}$$

By the normality of $L_i$ over $k$, the Galois group $\Gamma$ acts on $W_i$. We clearly have $L_i = k(\sqrt[m]{W_i})$. As $\mathrm{Gal}(L_i/k)$ acts on $\sqrt[m]{W_i}$, there is a natural inclusion

$$\mathrm{Gal}(L_i/k) \subset \{\sigma \in \mathrm{Aut}\sqrt[m]{W_i} : \ \sigma \mid K^* \in \Gamma\}.$$

For each $\gamma \in \Gamma$, there are $\#\sqrt[m]{W_i}/K^* = \#W_i/K^{*m} = \#\mathrm{Gal}(L_i/K)$ elements $\sigma \in \mathrm{Aut}\sqrt[m]{W_i}$ with $\sigma \mid K^* = \gamma$, so there is in fact an equality

$$\mathrm{Gal}(L_i/k) \ = \ \{\sigma \in \mathrm{Aut}\sqrt[m]{W_i} : \ \sigma \mid K^* \in \Gamma\}.$$

Define $W \subset W_1 \cap W_2$ to be the group

$$W \ = \ \{x \in W_1 \cap W_2 : \mathrm{ord}_{\mathfrak{P}}(x) = 0 \text{ for each prime } \mathfrak{P} \mid \mathfrak{p}_1\mathfrak{p}_2 \text{ of } K\}.$$

We claim that $L = K(\sqrt[m]{W})$, although obviously $W \not\supset K^{*m}$, so $W$ is not the maximal subgroup of $K^*$ with this property. The inclusion $L \supset K(\sqrt[m]{W})$ is the trivial part of our

claim. For the other inclusion, one only needs to observe that if $K(\sqrt[m]{x})/K$ has conductor dividing $\mathfrak{d}$, then $m \mid \mathrm{ord}_{\mathfrak{P}}(x)$ for all $\mathfrak{P} \mid \mathfrak{p}_1\mathfrak{p}_2$, so there exists $y \in K^{*m}$ such that $yx$ is a unit at all primes in $\mathfrak{p}_1\mathfrak{p}_2$, i.e. $yx \in W$.

The idea of the proof is as follows. We use the main theorem of class field theory to translate the equality $[\mathfrak{p}_1, M/k] = [\mathfrak{p}_2, M/k]$ into an idèlic statement that furnishes an element of $K^*$ having certain local properties. This element will be used to construct a $\Gamma$-isomorphism $\phi : K^* \xrightarrow{\sim} K^*$ that is the identity on $\sqrt[m]{W} \cap K^*$, maps $W_1$ onto $W_2$ and has a prescribed behaviour at primes in $S$ (lemma 8.7). By general facts (lemma 8.4) there then exists an extension of $\phi$ to $m$-th roots that induces the isomorphism from 7.4 for the Galois groups (lemma 8.5). The local conditions on $\phi$ establish the isomorphisms from 7.4(b) for the completions (lemma 8.6), and condition 7.4(a) comes automatically with the construction (corollary 8.8).

**8.4 Lemma.** *Let $\overline{K}$ be an algebraic closure of $K$ and write $\sqrt[m]{K^*} = \{x \in \overline{K} : x^m \in K^*\}$. Then every automorphism of the group $K^*$ that is the identity on $\sqrt[m]{W} \cap K^*$ can be extended to an automorphism of $\sqrt[m]{K^*}$ that is the identity on $\sqrt[m]{W}$, and such an extension is unique up to multiplication by a character $\sqrt[m]{K^*} \,/\, K^* \cdot \sqrt[m]{W} \to \langle \zeta_m \rangle$.*

**Proof.** Let $\phi$ be an automorphism of $K^*$ that is the identity on $\sqrt[m]{W} \cap K^*$. Then the homomorphism $K^* \cdot \sqrt[m]{W} \to \overline{K}^*$ that maps $\alpha\beta$ to $\phi(\alpha)\beta$ is well-defined, and it has an extension to a homomorphism $\psi : \sqrt[m]{K^*} \to \overline{K}^*$ since the group $\overline{K}^*$ is divisible. The map $\psi$ is injective: an element $\alpha \in \ker\psi$ satisfies $\alpha^m \in \ker\phi = \{1\}$, so $\alpha \in \langle \zeta_m \rangle \subset K^*$ and consequently $\alpha = 1$. From the fact that $\psi[K^*] = \phi[K^*] = K^*$ one easily deduces that $\psi$ furnishes an isomorphism $\sqrt[m]{K^*} \xrightarrow{\sim} \sqrt[m]{K^*}$, and that this is an extension of $\phi$ that is the identity on $\sqrt[m]{W}$. If $\psi'$ is another extension of $\phi$ with these properties, then $\frac{\psi'}{\psi}$ is a homomorphism on $\sqrt[m]{K^*}$ that is the identity on $K^* \cdot \sqrt[m]{W}$, so it induces a character on the factor group $\sqrt[m]{K^*}/K^* \cdot \sqrt[m]{W}$ with image in $\langle \zeta_m \rangle$. Conversely, multiplication of $\psi$ by such a character gives another extension of $\phi$. □

**8.5 Lemma.** *Suppose $\phi : K^* \xrightarrow{\sim} K^*$ is a $\Gamma$-isomorphism that is the identity on $\sqrt[m]{W} \cap K^*$ and induces an isomorphism $W_1 \xrightarrow{\sim} W_2$. Then there exist an isomorphism $\psi : \sqrt[m]{W_1} \xrightarrow{\sim} \sqrt[m]{W_2}$ extending $\phi$ and an isomorphism*

$$f : \mathrm{Gal}(L_1/k) \xrightarrow{\sim} \mathrm{Gal}(L_2/k)$$

*induced by $\psi$ that respects the projections $\mathrm{Gal}(L_i/k) \twoheadrightarrow \mathrm{Gal}(L/k)$. Another choice of the extension $\psi$ changes $f$ by an inner automorphism of $\mathrm{Gal}(L_2/k)$ by an element of $\mathrm{Gal}(L_2/L)$.*

**Proof.** By 8.4, there exists an extension of $\phi$ to an automorphism of $\sqrt[m]{K^*}$ that is the identity on $\sqrt[m]{W}$, so we can take $\psi$ to be the restriction of this map to $\sqrt[m]{W_1}$. From the

identification $\mathrm{Gal}(L_i/k) = \{\sigma \in \mathrm{Aut}\sqrt[m]{W_i} : \sigma \mid K^* \in \Gamma\}$ for $i = 1,2$ and the fact that $\psi \mid K = \phi$ is a $\Gamma$-isomorphism it is clear that $\psi$ induces an isomorphism

$$f = f_\psi : \mathrm{Gal}(L_1/k) \xrightarrow{\sim} \mathrm{Gal}(L_2/k)$$
$$\tau \longrightarrow \psi\tau\psi^{-1}$$

that respects the projection onto $\mathrm{Gal}(K/k)$. As $\psi$ is the identity on $\sqrt[m]{W}$, it even respects the projection onto $\mathrm{Gal}(K(\sqrt[m]{W})/k) = \mathrm{Gal}(L/k)$.

Now let $\overline{\psi}$ be another extension of $\phi$ that is that is the identity on $\sqrt[m]{W}$. Then $\overline{\psi}\psi^{-1}$ is an automorphism of $\sqrt[m]{W_2}$ that is the identity on $K^*\sqrt[m]{W}$, so it corresponds to an element $\chi$ of $\mathrm{Gal}(L_2/L)$. For $\tau \in \mathrm{Gal}(L_1/k)$, we find that

$$f_{\overline{\psi}}(\tau) = \overline{\psi}\tau\overline{\psi}^{-1} = \chi\psi\tau\psi^{-1}\chi^{-1} = \chi f_\psi(\tau)\chi^{-1},$$

as asserted. □

Given an extension $\psi : \sqrt[m]{W_1} \to \sqrt[m]{W_2}$ of a $\Gamma$-isomorphism $\phi : K^* \to K^*$ that is the identity on $\sqrt[m]{W} \cap K^*$ as in 8.5, we identify the Galois groups $\mathrm{Gal}(L_1/k)$ and $\mathrm{Gal}(L_2/k)$ by the isomorphism from 8.5 and denote them by $G$.

**8.6 Lemma.** *Let $\phi$, $\psi$, $G$ be as above, and $\mathfrak{q}$ a prime of $k$. Suppose that there exists a $\Gamma$-homomorphism*

$$\chi = \chi_\mathfrak{q} : W_1 \longrightarrow K_\mathfrak{q}^* = (K \otimes k_\mathfrak{q})^*$$

*such that for all $x \in K^*$ we have $\chi(x^m) = (\phi(x)/x) \otimes 1$. Then there is an isomorphism of $k_\mathfrak{q}$-algebras*

$$L_1 \otimes_k k_\mathfrak{q} \xrightarrow{\sim} L_2 \otimes_k k_\mathfrak{q}$$

*that respects the action of $G$.*

**Proof.** For $i = 1,2$, let $K[\sqrt[m]{W_i}]$ be the group ring of $\sqrt[m]{W_i}$ with coefficients in $K$. The Galois group $G$ acts on this group ring by its natural action on $K$ and $\sqrt[m]{W_i}$. We claim that there is a $G$-isomorphism of $K$-algebras $L_i \cong_G K[\sqrt[m]{W_i}]/I_i$, where $I_i$ is the ideal generated by the elements of the form $1 \cdot x - x \cdot 1$ for $x \in K^*$. In this expression the two $x$'s are viewed as an element of the group $\sqrt[m]{W_i}$ and a coefficient from $K$, respectively. As $I_i$ is certainly contained in the kernel of the canonical surjective ring homomorphism $K[\sqrt[m]{W_i}] \to K$, the claim follows from the observation that $\dim_K K[\sqrt[m]{W_i}]/I_i \leq [\sqrt[m]{W_i} : K^*] = [L_i : K]$.

We let $G$ act on $K_\mathfrak{q} = K \otimes_k k_\mathfrak{q}$ via $\Gamma$ and on the group ring $K_\mathfrak{q}[\sqrt[m]{W_i}]$ via its actions on $K_\mathfrak{q}$ and $\sqrt[m]{W_i}$. Now define a homomorphism of $K_\mathfrak{q}$-algebras

$$g : K_\mathfrak{q}[\sqrt[m]{W_1}] \longrightarrow K_\mathfrak{q}[\sqrt[m]{W_2}]$$

by its action on the generators $w_1 \in \sqrt[m]{W_1}$ over $K_\mathfrak{q}$ as

$$w_1 = 1 \cdot w_1 \longmapsto \chi(w_1^m)^{-1} \cdot \psi(w_1).$$

From the fact that $\chi$ is a $\Gamma$-homomorphism it follows that $g$ is a $G$-homomorphism. Further $g$ has a two-sided inverse sending a group element $w_2 \in \sqrt[m]{W_2}$ to $\chi(w_1^m) \cdot w_1$ with $w_1 = \psi^{-1}(w_2)$, so it is an isomorphism. For $x \in K^* \subset K_\mathfrak{q}$ we have

$$\begin{aligned} g(x \cdot 1 - 1 \cdot x) &= x \cdot 1 - \chi(x^m)^{-1} \cdot \psi(x) \\ &= x \cdot 1 - x\phi(x)^{-1} \cdot \phi(x) \\ &= (x \cdot \phi(x))(1 \cdot \phi(x)^{-1} - \phi(x)^{-1} \cdot 1), \end{aligned}$$

from which it follows easily that $g(I_1) = I_2$. We conclude that $g$ induces a $G$-isomorphism

$$K_\mathfrak{q}[\sqrt[m]{W_1}]/I_1 \xrightarrow{\sim} K_\mathfrak{q}[\sqrt[m]{W_2}]/I_2.$$

But this is exactly the isomorphism we need, since

$$\begin{aligned} K_\mathfrak{q}[\sqrt[m]{W_i}]/I_i &= K[\sqrt[m]{W_i}]/I_i \otimes_K K_\mathfrak{q} \\ &= L_i \otimes_K K_\mathfrak{q} = L_i \otimes_K K \otimes_k k_\mathfrak{q} = L_i \otimes_k k_\mathfrak{q}. \end{aligned}$$ □

Since $\mathfrak{p}_1$ and $\mathfrak{p}_2$ have the same Artin class in $M/k$, we can choose primes over $\mathfrak{p}_1$ and $\mathfrak{p}_2$ in $M$ that have the same Frobenius in $\mathrm{Gal}(M/k)$. The common decomposition group of the restrictions $\mathfrak{P}_1$ and $\mathfrak{P}_2$ of these primes to $K$ in $\Gamma$ is denoted by $D$. Write $E$ for the fixed field $K^D$ of $D$. In the sequel, we will denote primes in $K$ by $\mathfrak{P}$, $\Omega$, primes in $E$ by $\mathcal{P}$, $\mathcal{Q}$ and primes in $k$ by $\mathfrak{p}$, $\mathfrak{q}$.

**8.7 Lemma.** *Suppose there exists $b \in E$ satisfying the following conditions:*
(a) *$b \in {E_\mathcal{Q}^*}^m$ if $\mathcal{Q}$ is a prime of $E$ that lies in $S$;*
(b) *$\mathrm{ord}_{\mathfrak{P}_1}(b) = -1$, $\mathrm{ord}_{\mathfrak{P}_2}(b) = 1$ and $\mathrm{ord}_\mathfrak{P}(b) = 0$ for all other primes $\mathfrak{P} \mid \mathfrak{p}_1\mathfrak{p}_2$ in $K$;*
(c) *the local conductor of $K_\Omega(\sqrt[m]{b})/K_\Omega$ divides $\Omega^{\mathrm{ord}_\Omega(\mathfrak{d})}$ for all primes $\Omega \nmid \mathfrak{p}_1\mathfrak{p}_2$ in $K$.*

*Then there exist a $\Gamma$-isomorphism $\phi : K^* \xrightarrow{\sim} K^*$ that is the identity on $\sqrt[m]{W} \cap K^*$ and maps $W_1$ onto $W_2$. Moreover, for each $\mathfrak{q} \in S$, there is a $\Gamma$-homomorphism $\chi_\mathfrak{q} : W_1 \longrightarrow (K \otimes_k k_\mathfrak{q})^*$ such that for all $x \in K^*$ we have $\chi(x^m) = (\phi(x)/x) \otimes 1$.*

**Proof.** We use the element $b$ to construct an isomorphism $\phi : K^* \to K^*$ such that, for any $x \in K^*$ and $\gamma \in \Gamma$,

$$\begin{aligned} \mathrm{ord}_{\gamma\mathfrak{P}_1}(x) &= \mathrm{ord}_{\gamma\mathfrak{P}_2}(\phi(x)), \\ \mathrm{ord}_{\gamma\mathfrak{P}_2}(x) &= \mathrm{ord}_{\gamma\mathfrak{P}_1}(\phi(x)). \end{aligned}$$

Let $\mathbb{Z}[\Gamma/D]$ be the free abelian group on the left cosets of $D$ in $\Gamma$. This is in a natural way a $\mathbb{Z}[\Gamma]$-module. Define the "valuation maps" $\lambda_i : K^* \to \mathbb{Z}[\Gamma/D]$ at the primes over $\mathfrak{p}_i$ in $K$ as the $\Gamma$-homomorphisms that send $x \in K^*$ to

$$\lambda_i(x) = \sum_{\gamma \in \Gamma/D} \mathrm{ord}_{\gamma\mathfrak{P}_i}(x) \cdot \gamma.$$

The element $b^{\lambda_i(x)}$ is well defined since $b$ is in $E$. Note that $xb^{\lambda_1(x)}$ and $xb^{-\lambda_2(x)}$ are local units at primes over $\mathfrak{p}_1$ and $\mathfrak{p}_2$, respectively. Now we define the homomorphism $\phi : K^* \to K^*$ by

$$\phi(x) = xb^{\lambda_1(x)-\lambda_2(x)}.$$

It is immediate from the construction of $\phi$ that this is a $\Gamma$-homomorphism that interchanges the valuations at primes over $\mathfrak{p}_1$ and $\mathfrak{p}_2$ in the way required above. It is the identity on

$$\sqrt[m]{W} \cap K^* = \{x \in K^* : \mathrm{ord}_{\mathfrak{P}}(x) = 0 \text{ for each prime } \mathfrak{P} \mid \mathfrak{p}_1\mathfrak{p}_2 \text{ of } K\} = \ker \lambda.$$

Further $\phi^2 = \mathrm{id}_K$, so $\phi$ is an isomorphism.

Now take $x \in W_1$. By definition, this means that $K(\sqrt[m]{x})/K$ has conductor dividing $\mathfrak{d}\mathfrak{p}_1$. In particular, it is unramified at $\mathfrak{p}_2$. This implies that all orders of $x$ at primes in $K$ over $\mathfrak{p}_2$ are divisible by $m$. But then $\phi(x)$ has orders divisible by $m$ at primes in $K$ over $\mathfrak{p}_1$, so $K(\sqrt[m]{\phi(x)})/K$ is unramified at $\mathfrak{p}_1$. It follows from condition (c) and the fact that primes of $K$ dividing $\mathfrak{p}_1\mathfrak{p}_2$ are tamely ramified in $K(\sqrt[m]{b})/K$ that the extension $K(\sqrt[m]{b})/K$ has conductor dividing $\mathfrak{d}\mathfrak{p}_1\mathfrak{p}_2$. The $\Gamma$-invariance of $\mathfrak{d}$ implies that $K(\sqrt[m]{b^\gamma})/K$ also has conductor dividing $\mathfrak{d}\mathfrak{p}_1\mathfrak{p}_2$ for any $\gamma \in \mathbb{Z}[\Gamma]$. Consequently, $K(\sqrt[m]{\phi(x)})/K = K(\sqrt[m]{xb^\gamma})/K$ is of conductor dividing $\mathfrak{d}\mathfrak{p}_1\mathfrak{p}_2$. Since we showed it to be unramified over $\mathfrak{p}_1$, its conductor actually divides $\mathfrak{d}\mathfrak{p}_2$, whence $x \in W_2$. We conclude that $\phi[W_1] \subset W_2$. Interchanging the role of $W_1$ and $W_2$ in the argument above, one obtains $\phi[W_2] \subset W_1$. Finally, the observation that $\phi^2 = \mathrm{id}_K$ shows that $\phi$ is a $\Gamma$-isomorphism $K^* \xrightarrow{\sim} K^*$ inducing an isomorphism $W_1 \xrightarrow{\sim} W_2$.

Let $\mathfrak{q}$ be a prime in $S$. Since $b$ is an $m$-th power in the completions of $E$ above $\mathfrak{q}$, there exists $\beta \in E_{\mathfrak{q}}^* = (E \otimes_k k_{\mathfrak{q}})^*$ satisfying $\beta^m = b \otimes 1$. As before, $\Gamma$ acts on $K_{\mathfrak{q}}$ via the first factor. We view the canonical map $E_{\mathfrak{q}} \hookrightarrow K_{\mathfrak{q}}$ as an inclusion. The element $\beta$ is used to define $\chi_{\mathfrak{q}} : W_1 \to K_{\mathfrak{q}}^*$ by

$$\chi_{\mathfrak{q}}(x) = \beta^{\lambda_1(x)-\lambda_2(x)}.$$

This is again a $\Gamma$-homomorphism, and it satisfies

$$\chi_{\mathfrak{q}}(x^m) = b^{\lambda_1(x)-\lambda_2(x)} = \frac{\phi(x)}{x} \otimes 1,$$

which is exactly what we want. □

For a construction in a different context that has the same basic idea as the construction given above we refer to [11].

Before proceeding with the proof of 8.1, we give a corollary of the preceding lemma that shows that the requirement 7.4(a) is automatic in our construction.

**8.8 Corollary.** *Define $\phi$ as in the proof of lemma 8.7. Then the isomorphism*

$$f:\ \mathrm{Gal}(L_2/k)\xrightarrow{\sim}\mathrm{Gal}(L_1/k)$$

*that was constructed from $\phi$ in lemma 8.5 maps the inertia groups of primes above $\mathfrak{p}_1$ in $\mathrm{Gal}(L_1/k)$ to the inertia groups of primes above $\mathfrak{p}_2$ in $\mathrm{Gal}(L_2/k)$.*

**Proof.** The inertia group of $\gamma\mathfrak{P}_i$ in $\mathrm{Gal}(L_i/k)$ consists exactly of those elements in $\mathrm{Gal}(L_i/k)$ that act trivially on $K$ and on

$$\{\sqrt[m]{w}\in\sqrt[m]{W_i}:\mathrm{ord}_{\gamma\mathfrak{P}_i}(w)\equiv 0 \bmod m\}.$$

The construction of $\phi$ in the preceding lemma shows that, for any $\gamma\in\Gamma$,

$$\phi\big[\{w\in W_1:\mathrm{ord}_{\gamma\mathfrak{P}_1}(w)\equiv 0 \bmod m\}\big]=\{w\in W_2:\mathrm{ord}_{\gamma\mathfrak{P}_2}(w)\equiv 0 \bmod m\}.$$

Our claim follows immediately. □

To finish the proof of 8.1, we will show that the condition that $\mathfrak{p}_1$ and $\mathfrak{p}_2$ have the same Artin class in $\mathrm{Gal}(M/k)$ ensures the existence of an element $b\in E$ as in 8.7. This will be done via an idèlic reformulation of this condition.

By class field theory [7, 20], the abelian extension $M/K$ corresponds to the open subgroup $K^*\mathrm{N}_{M/K}J_M$ of the idèle group $J_K$. We claim that this subgroup can be described explicitly as

$$K^*\Big(\prod_{\mathfrak{Q}\in(m\cdot\mathfrak{d}\cdot\infty)\setminus S}(U_{\mathfrak{Q}}^{(\mathrm{ord}_{\mathfrak{Q}}(\mathfrak{d}))})^{\perp}\times\prod_{\mathfrak{Q}\in S}K_{\mathfrak{Q}}^{*\,m}\times\prod_{\text{other }\mathfrak{Q}}{}'\,U_{\mathfrak{Q}}K_{\mathfrak{Q}}^{*\,m}\Big).$$

Here the subgroup of local units in $K_{\mathfrak{Q}}^*$ is written as $U_{\mathfrak{Q}}$. By the symbol $\perp$ we denote orthogonal complements with respect to the $m$-th norm residue symbol, which is defined for any completion $F$ of a number field that contains a primitive $m$-th root of unity $\zeta_m$ as follows (cf. [7, 20]). The norm residue symbol $(\,.\,,\,.\,)_m$ for $F$ is a pairing

$$\begin{aligned}F^*\times F^*&\longrightarrow\langle\zeta_m\rangle\\(\alpha,\beta)&\longmapsto\frac{\sigma_\alpha(\sqrt[m]{\beta})}{\sqrt[m]{\beta}},\end{aligned}$$

where $\sigma_\alpha$ is the Artin symbol of $\alpha$ in the local extension $F(\sqrt[m]{F})/F$. This symbol has the property that $(\alpha,\beta) = (\beta,\alpha)^{-1}$, so the orthogonal complement of any subset of $F^*$ is well defined and contains the open subgroup $F^{*m}$ of $F^*$.

For the proof of our claim, we first observe that for any extension $M/K$ that has a group of exponent $m$ and is unramified outside $S \cdot (m) \cdot \mathfrak{d} \cdot \infty$, the subgroup $K^*\mathbf{N}_{M/K}J_M$ contains $K_{\mathfrak{Q}}^{*\,m}$ for all primes $\mathfrak{Q}$ of $K$ and $\prod_{\mathfrak{Q}} U_{\mathfrak{Q}}$ with $\mathfrak{Q}$ ranging over the primes not in $S \cdot (m) \cdot \mathfrak{d} \cdot \infty$. Recall that for real primes $\mathfrak{Q}$ of $K$—they can only exist when $m \leq 2$—we have $U_{\mathfrak{Q}} = K_{\mathfrak{Q}}^*$.

The requirement that $M$ be contained in $K(\sqrt[m]{U_{\mathfrak{Q}}^{(\mathrm{ord}_{\mathfrak{Q}}(\mathfrak{d}))}})$ at the primes in $(m)\cdot\mathfrak{d}$ outside $S$ is equivalent to saying that $\mathbf{N}_{M/K}J_M$ contains $(U_{\mathfrak{Q}}^{(\mathrm{ord}_{\mathfrak{Q}}(\mathfrak{d}))})^{\perp}$ at the corresponding components. This condition is trivially satisfied for the real primes outside $\mathfrak{d}$. The maximality of $M$ implies that $K^*\mathbf{N}_{M/K}J_M$ does not merely contain the open subgroup of $J_K$ exhibited above, but is actually equal to it.

This open subgroup of $J_K$ remains unaltered if we change the local components $U_{\mathfrak{Q}}K_{\mathfrak{Q}}^{*\,m}$ at finitely many $\mathfrak{Q}$ outside $S \cdot m \cdot \mathfrak{d} \cdot \infty$ into $U_{\mathfrak{Q}}$. Indeed, if the Frobenius elements of almost all primes in an abelian extension are annihilated by $m$, then the group is of exponent dividing $m$ and all $m$-th powers in the idèles are norms. Thus, we can write $K^*\mathbf{N}_{M/K}J_M$ as

$$K^*\Big(\prod_{\mathfrak{Q}\in(m\cdot\mathfrak{d}\cdot\infty)\setminus S} (U_{\mathfrak{Q}}^{(\mathrm{ord}_{\mathfrak{Q}}(\mathfrak{d}))})^{\perp} \times \prod_{\mathfrak{Q}\in S} K_{\mathfrak{Q}}^{*\,m} \times \prod_{\mathfrak{Q}|\mathfrak{p}_1\mathfrak{p}_2} U_{\mathfrak{Q}} \times \prod_{\text{other } \mathfrak{Q}}{}' U_{\mathfrak{Q}}K_{\mathfrak{Q}}^{*\,m}\Big).$$

Since $m$, $\mathfrak{d}$, $S$ and $\mathfrak{p}_1\mathfrak{p}_2$ are invariant under $\Gamma$, this is a subgroup of $J_K$ that is its own $\Gamma$-image. Viewing the canonical map $J_E \to J_K$ as an inclusion, we conclude that the subgroup $K^*\mathbf{N}_{M/K}J_M$ of $J_K$ is mapped to itself by the idèle norm $\mathbf{N}_{K/E}$. It follows that $E^*\mathbf{N}_{M/E}J_M = E^*\mathbf{N}_{K/E}[K^*\mathbf{N}_{M/K}J_M] \subset J_E$ can be embedded in $J_K$ as a subgroup of

$$E^*\Big(\prod_{\mathfrak{Q}\in(m\cdot\mathfrak{d}\cdot\infty)\setminus S} (U_{\mathfrak{Q}}^{(\mathrm{ord}_{\mathfrak{Q}}(\mathfrak{d}))})^{\perp} \times \prod_{\mathfrak{Q}\in S} E_{\mathcal{Q}}^{*\,m} \times \prod_{\mathfrak{Q}|\mathfrak{p}_1\mathfrak{p}_2} U_{\mathcal{Q}} \times \prod_{\text{other } \mathfrak{Q}}{}' U_{\mathfrak{Q}}E_{\mathfrak{Q}}^{*\,m}\Big).$$

Here $\mathcal{Q}$ stands for the restriction $\mathfrak{Q}\cap E$ and the product is taken over the primes $\mathfrak{Q}$ of $K$, so a prime $\mathcal{Q}$ may occur more than once in this product.

Class field theory [7, 20] tells us that $E^*\mathbf{N}_{M/E}J_M$ is the kernel of the Artin map $J_E \to \mathrm{Gal}(M'/E)$, where $M'/E$ is the maximal abelian subextension of $M/E$. Let $\pi_i \in J_E$ denote a prime element at $\mathcal{P}_i = \mathfrak{P}_i \cap E$ for $i = 1, 2$, i.e. an element that has all components equal to 1 outside $\mathcal{P}_i$ and equal to a prime element at $\mathcal{P}_i$ at the prime itself. Under the Artin map $J_E \to \mathrm{Gal}(M'/E)$, the element $\pi_i$ is sent to the Artin symbol of $\mathcal{P}_i$. By our

assumption on $\mathfrak{p}_1$ and $\mathfrak{p}_2$, these are the same for $i = 1$ and $i = 2$, so $\pi_1\pi_2^{-1}$ is in the kernel of the Artin map. Consequently, there exists an element $b \in E^*$ such that

$$\pi_1\pi_2^{-1}b \in \prod_{\Omega\in(m\cdot\mathfrak{d}\cdot\infty)\setminus S} (U_\Omega^{(\mathrm{ord}_\Omega(\mathfrak{d}))})^\perp \times \prod_{\Omega\in S} {E_\mathcal{Q}^*}^m \times \prod_{\Omega\mid\mathfrak{p}_1\mathfrak{p}_2} U_\mathcal{Q} \times \prod_{\text{other } \Omega}{}' U_\Omega {E_\Omega^*}^m.$$

This means that the element $b \in E^*$ satisfies

(a) $b \in {E_\mathcal{Q}^*}^m$ if $\mathcal{Q}$ is a prime of $E$ that lies in $S$;

(b) $\mathrm{ord}_{\mathcal{P}_1}(b) = -1$, $\mathrm{ord}_{\mathcal{P}_2}(b) = 1$ and $\mathrm{ord}_\mathcal{Q}(b) = 0$ for all other $\mathcal{Q} \nmid \mathfrak{p}_1\mathfrak{p}_2$;

(c) $b$ acts trivially via the $m$-th norm residue symbol on $U_\Omega^{(\mathrm{ord}_\Omega(\mathfrak{d}))}$ at primes $\Omega \mid (m)\cdot\mathfrak{d}\cdot\infty$ of $K$;

(d) $\mathrm{ord}_\Omega(b) \equiv 0 \bmod m$ for all finite primes $\Omega$ of $K$ outside $(m)\cdot\mathfrak{d}\mathfrak{p}_1\mathfrak{p}_2$.

We are done if we can show that these conditions imply the conditions on the element $b \in E$ that occur in lemma 8.7. Condition (a) here is identical to condition (a) in 8.7, and the same is true for condition (b) since, by definition of $E$, the prime $\mathcal{P}_i$ is inert in $K/E$.

To finish the proof, we will show that for an element $b$ satisfying the conditions (a)–(d) here, the local extension $K_\Omega(\sqrt[m]{b})/K_\Omega$ has conductor dividing $\Omega^{\mathrm{ord}_\Omega(\mathfrak{d})}$ at primes $\Omega \nmid \mathfrak{p}_1\mathfrak{p}_2$ in $K$. This only needs to be checked at the potentially ramified primes, and by conditions (a) and (d) these are only the primes in $\mathfrak{d}\cdot m\cdot\infty$ that are not in $S$. At these primes, we know that $b$ acts trivially via the $m$-th norm residue symbol on $U_\Omega^{(\mathrm{ord}_\Omega(\mathfrak{d}))}$. This is the same as saying that these subgroups of $K_\Omega^*$ are in the kernel of the Artin map $K_\Omega^* \to \mathrm{Gal}(K_\Omega(\sqrt[m]{b})/K_\Omega)$, and this just means that the local conductor divides $\Omega^{\mathrm{ord}_\Omega(\mathfrak{d})}$.

This finishes the proof of theorem 8.1. □

Proposition 5.11 is again helpful when one needs explicit generators for the governing field $M$ that occurs in 8.1. In fact, the following reformulation of 8.1 for the case $K = K_m$ shows the striking similarity between the governing field construction in this chapter and the construction from 5.6. It suggests that, at least if $\zeta_m \in K$, the isomorphisms in 7.2 automatically hold for the Galois groups over $k$ if we are in the special situation described before 7.4. The situation remains to be clarified.

**8.9 Corollary.** *Let the situation be as in* 8.1, *and define the group* $W \subset K^*$ *by*

$$W = W_{S,\mathfrak{d},m} = \{x \in K^* :\ \mathrm{ord}_\Omega(x) \equiv 0 \bmod m \text{ for all finite } \Omega \notin S \text{ and } x \equiv 1 \bmod^* \Omega^{\mathrm{ord}_\Omega(\mathfrak{d})} \text{ for all } \Omega \in \mathfrak{d}\setminus S\}.$$

*If* $K$ *contains a primitive* $m$*-th root of unity, then* $M = K(\sqrt[m]{W})$ *is a governing field for* $(\mathfrak{d}, m, S)$*-equivalence of primes of* $k$.

**Proof.** This is immediate from 8.1 if one realizes that for the primes $\Omega$ in $m$ outside $\mathfrak{d}\cdot S$ the requirement that $M$ can be obtained by adjoining $m$-th roots of elements $x$ that satisfy $\mathrm{ord}_\Omega(x) \equiv 0 \bmod m$ simply means that $M$ can be embedded in $K_\Omega(\sqrt[m]{U_\Omega})$ over $K$. □

# CHAPTER IV

# The conjectures of Cohn and Lagarias

## 9. Class groups of quadratic orders

In this section, we show how class field theory can be used to study the strict class group $C(\Delta) = \mathcal{I}_\Delta/\mathcal{P}_\Delta$ of the quadratic order $\mathcal{O}_\Delta$. We write $\Delta = f^2 d$ as in section 2.

Let $K = \mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{\Delta})$ be the quadratic field of discriminant $d$ and define the cycle $\mathfrak{f} = f\mathcal{O} \cdot \infty$ of $K$ as the product of $f\mathcal{O}$ and the real primes in $K$. It is easily checked that the canonical injection $\mathcal{I}(f) \to \mathcal{I}_\Delta$ that maps integral $\mathcal{O}$-ideals $\mathfrak{a} \in \mathcal{I}(\mathfrak{f})$ to $\mathfrak{a} \cap \mathcal{O}_\Delta$ induces an isomorphism

$$\mathcal{I}(\mathfrak{f})/\mathcal{R}(\mathfrak{f}) \xrightarrow{\sim} \mathcal{I}_\Delta/\mathcal{P}_\Delta = C(\Delta) \tag{9.1}$$

with

$$\mathcal{R}(\mathfrak{f}) = \{\alpha\mathcal{O} \in \mathcal{I}(\mathfrak{f}) : N_{K/\mathbb{Q}}(\alpha) > 0 \text{ and } \alpha \equiv z \bmod^* f \text{ for some } z \in \mathbb{Z}\}.$$

The group $\mathcal{I}(\mathfrak{f})/\mathcal{R}(\mathfrak{f})$ is called the *(strict) ring class group modulo* $f$ of $\mathbb{Q}(\sqrt{d})$. It is a factor group of the ray class group modulo $\mathfrak{f} = f\mathcal{O} \cdot \infty$, so there is a canonical isomorphism

$$\mathcal{I}(\mathfrak{f})/\mathcal{R}(\mathfrak{f}) \cong \mathrm{Gal}(R_\Delta/\mathbb{Q}(\sqrt{d}))$$

for some subfield $R_\Delta$ of $H_\mathfrak{f}$ by (2.2). The field $R_\Delta$ is called the *(strict) ring class field modulo* $f$. For any ideal $\mathfrak{a} \in \mathcal{I}(\mathfrak{f})$ one has $\mathrm{N}_{K/\mathbb{Q}}\mathfrak{a} \cdot \mathcal{O} \in \mathcal{R}(\mathfrak{f})$, so the non-trivial element $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$ acts on $\mathcal{I}(\mathfrak{f})/\mathcal{R}(\mathfrak{f})$ by inversion. The decomposition group of any prime in $R_\Delta$ that lies over a rational prime $p \nmid f$ that is inert in $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ has order 2. One easily derives that the extension $R_\Delta/\mathbb{Q}$ is dihedral: its Galois group can be written as a semidirect product

$$\mathrm{Gal}(R_\Delta/\mathbb{Q}) \cong \mathcal{I}(\mathfrak{f})/\mathcal{R}(\mathfrak{f}) \rtimes \langle\sigma\rangle \tag{9.2}$$

with $\sigma$ acting on $\mathcal{I}(\mathfrak{f})/\mathcal{R}(\mathfrak{f})$ by inversion. Note that the above splitting is not canonical as it depends on the choice of an extension of $\sigma$ to $H$. In fact, $R_\Delta$ is the maximal abelian extension of $\mathbb{Q}(\sqrt{d})$ of conductor dividing $(f) \cdot \infty$ that is dihedral over $\mathbb{Q}$. It can also be characterized as the maximal subfield of the ray class field modulo $(f) \cdot \infty$ in which all primes $p \nmid f$ of $\mathbb{Q}(\sqrt{d})$ that lie over an inert rational prime split completely [6]. It follows from the discussion in section 2 that the splitting behaviour in $R_\Delta/\mathbb{Q}$ of rational primes that split in $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ can be described in terms of representations by quadratic forms of discriminant $\Delta$. In particular, a rational prime $p \nmid \Delta$ splits completely in the full extension $R_\Delta/\mathbb{Q}$ if and only if it is represented by the *principal form* of discriminant $\Delta$, i.e. the form

$$\begin{aligned} &X^2 + XY - \frac{\Delta - 1}{4}Y^2 && \text{if } \Delta \equiv 1 \bmod 4 \\ &X^2 - \frac{\Delta}{4}Y^2 && \text{if } \Delta \equiv 0 \bmod 4 \end{aligned} \tag{9.3}$$

For $f = 1$, the group $\mathcal{I}(\mathfrak{f})/\mathcal{R}(\mathfrak{f})$ is the strict class group of $\mathbb{Q}(\sqrt{d})$ and $R_\Delta$ is the strict Hilbert class field of $\mathbb{Q}(\sqrt{d})$.

Because of (9.1), we can rewrite (9.2) as

$$\mathrm{Gal}(R_\Delta/\mathbb{Q}) \cong \mathcal{C}(\Delta) \rtimes \langle\sigma\rangle. \tag{9.4}$$

This isomorphism will be exploited to relate the $2^k$-rank of $\mathcal{C}(\Delta)$ to the degree of suitable field extensions.

The invariant subfield $G_\Delta \subset R_\Delta$ of the commutator subgroup of $\mathrm{Gal}(R_\Delta/\mathbb{Q})$ is called the *genus field* of the extension $R_\Delta/\mathbb{Q}(\sqrt{d})$. It is the maximal subextension of $R_\Delta/\mathbb{Q}$ that is abelian over $\mathbb{Q}$. As the commutator subgroup of $\mathcal{C}(\Delta) \rtimes \langle\sigma\rangle$ equals $\mathcal{C}(\Delta)^2$, we see that $\mathrm{Gal}(G_\Delta/\mathbb{Q})$ is an elementary abelian 2-group whose 2-rank exceeds the 2-rank of $\mathcal{C}(\Delta)$ by one. Explicit generators for $G_\Delta$ over $\mathbb{Q}$ can be given as follows [12]. Decompose $d$ as a product $\prod_{j=1}^{s} d_j$ of *fundamental prime power discriminants*. This means that each $d_j$ is a fundamental discriminant whose absolute value is a prime power or, even more explicitly, that $d_j = -4$, $\pm 8$ or $(-1)^{(p-1)/2}p$ with $p$ an odd prime. We assume that $d_1$ has the same parity as $d$. Let $q_1, q_2, \ldots, q_t$ be the odd primes in $f$ that do not divide $d$. Write $E = \mathbb{Q}(\{\sqrt{d_j}\}_{j=1}^{s}, \{\sqrt{q_j^*}\}_{j=1}^{t})$, with $q_j^* = (-1)^{(q_j-1)/2}q_j \equiv 1 \bmod 4$. Then $[E : \mathbb{Q}] = 2^{s+t}$ and one has

$$G_\Delta = \begin{cases} E & \text{if } d_1 = \pm 8 \text{ and } f \text{ is odd, or } 8 \nmid d \text{ and } 4 \nmid f; \\ E(\sqrt{-1}) & \text{if } d_1 = \pm 8 \text{ and } 2 \mid f, \text{ or } d \text{ is odd and } 4 \| f; \\ E(\sqrt{2}) & \text{if } d_1 = -4 \text{ and } 4 \mid f; \\ E(\sqrt{-1}, \sqrt{2}) & \text{if } d \text{ is odd and } 8 \mid f. \end{cases} \tag{9.5}$$

It is easy to check that the field given above is abelian over $\mathbb{Q}$ and of conductor dividing $(f) \cdot \infty$ over $\mathbb{Q}(\sqrt{d})$. In fact, it is the maximal field with these properties, as is easily checked by looking at the quadratic fields that it can contain. Thus, it must be equal to the genus field. We conclude that the 2-rank of $\mathcal{C}(\Delta)$, which is the number of factors 2 in the degree of the extension $[G_\Delta : \mathbb{Q}(\sqrt{d})]$, depends in the following way of the number $u$ of distinct prime factors of $\Delta$:

$$r_2 = \begin{cases} u & \text{if } 32 \mid \Delta; \\ u-2 & \text{if } d \text{ is odd and } 2 \| f; \\ u-1 & \text{in all other cases.} \end{cases} \tag{9.6}$$

We see from (9.6) that the 2-rank of $\mathcal{C}(\Delta)$ for fundamental $\Delta$ is one less than the number of distinct prime factors in $\Delta$. In particular, quadratic fields of (absolute) prime power discriminant have an odd class number.

Equation (9.6) was derived by Gauss by looking at the structure of the 2-torsion subgroup $\mathcal{C}(\Delta)_2$. This group can also be described by class field theory. As we have to

deal with the local behaviour at ramifying primes, it is more convenient to view $\mathcal{C}(\Delta)$ as a factor group of the idèle group $J$ of $K$.

The canonical surjection

$$\phi : \; J_K \twoheadrightarrow \mathcal{C}(\Delta) \;\cong\; \mathrm{Gal}(R_\Delta/\mathbb{Q}(\sqrt{d}))$$

has kernel

$$\begin{aligned} &K^* \cdot \textstyle\prod_{p \text{ prime}} \left( \mathbb{Z}_p^* \prod_{\mathfrak{p}|p} U_{\mathfrak{p}}^{(\mathrm{ord}_p(f))} \right) \times K_c^* && \text{if } \Delta < 0 \\ &K^* \cdot \textstyle\prod_{p \text{ prime}} \left( \mathbb{Z}_p^* \prod_{\mathfrak{p}|p} U_{\mathfrak{p}}^{(\mathrm{ord}_p(f))} \right) \times \prod_{\mathfrak{p}|\infty} K_{\mathfrak{p},>0} && \text{if } \Delta > 0, \end{aligned} \tag{9.7}$$

where $K_c$ stands for the completion of $K$ at the complex prime. The map $\phi$ can be described explicitly in the following way. Let the ring $A_\Delta \cong \varprojlim \mathcal{O}_\Delta/n\mathcal{O}_\Delta$ be the closure of $\mathcal{O}_\Delta$ in the adèle ring of $K$, and $x = (x_\mathfrak{p})_\mathfrak{p}$ an element of $J_K$. Multiplying $x$ by an element of $K^*$, if necessary, we may assume that $x$ has an archimedean component whose local norm to $\mathbb{Q}_\infty^* \cong \mathbb{R}^*$ is positive. Then one has

$$\phi(x) = [(xA_\Delta) \cap \mathbb{Q}(\sqrt{\Delta})] \in \mathcal{C}(\Delta).$$

Restricting the homomorphism $J \twoheadrightarrow \mathcal{C}(\Delta)$ introduced above to the subgroup $J_{\mathrm{fin}}$ of finite idèles—the restricted product over the multiplicative groups of the finite completions of $K$—we obtain a surjective homomorphism $J_{\mathrm{fin}} \twoheadrightarrow \mathcal{C}(\Delta)$ that factors via the homomorphism

$$\begin{aligned} \chi : \; J_{\mathrm{fin}} &\longrightarrow \mathcal{I}_\Delta \\ x &\longmapsto (xA_\Delta) \cap \mathbb{Q}(\sqrt{\Delta}). \end{aligned}$$

We have $A_\Delta = \prod_p \mathcal{O}_{\Delta,p}$, where the semilocal ring

$$\mathcal{O}_{\Delta,p} = \varprojlim_k (\mathcal{O}_\Delta/p^k\mathcal{O}_\Delta) = \mathbb{Z}_p + f \cdot \prod_{\mathfrak{p}|p} \mathcal{O}_{d,\mathfrak{p}}$$

is the completion of $\mathcal{O}_\Delta$ in $K_{(p)} = \prod_{\mathfrak{p}|p} K_\mathfrak{p}$. Correspondingly, $\mathcal{I}_\Delta$ can be written as a direct sum

$$\begin{aligned} \mathcal{I}_\Delta &\cong \textstyle\bigoplus_p \mathcal{I}(\mathcal{O}_{\Delta,p}) \\ &\cong \textstyle\bigoplus_p K_{(p)}^*/\mathcal{O}_{\Delta,p}^* \end{aligned}$$

where $\mathcal{I}(\mathcal{O}_{\Delta,p})$ is the group of invertible $\mathcal{O}_{\Delta,p}$-ideals. Since each invertible ideal in the semilocal ring $\mathcal{O}_{\Delta,p}$ is principal, this local ideal group is isomorphic to $K_{(p)}^*/\mathcal{O}_{\Delta,p}^*$ when we identify each ideal with the class of its generator modulo $\mathcal{O}_{\Delta,p}^*$. Note that $\mathcal{O}_{\Delta,p}$ and

$\mathcal{I}(\mathcal{O}_{\Delta,p})$ coincide with $\mathcal{O}_{d,p}$ and $\mathcal{I}(\mathcal{O}_{d,p})$ at rational primes $p \nmid f$. The homomorphism $\chi$ defined above is a sum $\bigoplus_p \chi_p$, with $p$ ranging over the rational primes and $\chi_p$ the canonical map

$$\chi_p : K^*_{(p)} \longrightarrow K^*_{(p)}/\mathcal{O}^*_{\Delta,p}.$$

The following lemma describes the 2-torsion subgroup $\mathcal{C}(\Delta)_2$ of $\mathcal{C}(\Delta)$ in terms of the homomorphisms $\phi$ and $\chi_p$ defined above.

**9.8 Lemma.** *Let $\sigma$ be a generator of $\mathfrak{G} = \mathrm{Gal}(\mathbb{Q}(\sqrt{\Delta})/\mathbb{Q})$.*

(a) *There is a canonical isomorphism*

$$\mathcal{C}(\Delta)_2 \cong \mathcal{I}_\Delta^{\mathfrak{G}} \,/\, \mathcal{P}_\Delta^{\mathfrak{G}}$$

*where $\mathcal{I}_\Delta^{\mathfrak{G}} = \{\mathfrak{a} \in \mathcal{I}_\Delta : \sigma\mathfrak{a} = \mathfrak{a}\}$ and $\mathcal{P}_\Delta^{\mathfrak{G}} = \{\alpha \cdot \mathcal{O}_\Delta \in \mathcal{P}_\Delta : \sigma(\alpha \cdot \mathcal{O}_\Delta) = \alpha \cdot \mathcal{O}_\Delta\}$. The subgroup $\{\alpha \cdot \mathcal{O}_\Delta \in \mathcal{P}_\Delta : \alpha \in \mathbb{Q}^*\}$ has index 2 in $\mathcal{P}_\Delta^{\mathfrak{G}}$.*

(b) *The subgroup $J_\Delta = \prod_{\mathfrak{p}|\Delta} \mathbb{Q}(\sqrt{\Delta})^*_{\mathfrak{p}}$ of $J$ satisfies $\phi[J_\Delta] \supset \mathcal{C}(\Delta)_2$.*

(c) *Let $p$ be an odd prime number that occurs in $\Delta$ with multiplicity 1, and $J_\infty \subset J$ the product of the archimedean components of $J$. Then the subgroup*

$$H = J_\infty \times \prod_{q|\Delta, q\neq p} \chi_q^{-1}\big((K^*_{(q)}/\mathcal{O}^*_{\Delta,q})^{\mathfrak{G}}\big)$$

*of $J$ satisfies $\phi[H] = \mathcal{C}(\Delta)_2$.*

**Proof.** For (a), we employ Tate cohomology. Recall that for a $\mathfrak{G}$-module $M$, the norm $\mathbf{N}$ on $M$ is the endomorphism $1 + \sigma$ and that the Tate cohomology groups are defined as $H^0(M) = \ker(\sigma - 1)/\mathrm{im}(\mathbf{N}) = M^{\mathfrak{G}}/\mathbf{N}[M]$ and $H^1(M) = \ker(\mathbf{N})/\mathrm{im}(\sigma - 1)$. Write $F$ for $\mathbb{Q}(\sqrt{\Delta})^*$ and let $U$ be the unit group of the ring of integers of $\mathbb{Q}(\sqrt{\Delta})$. We use subscripts $+$ and 1 to denote elements of positive norm and norm equal to 1. The cohomology sequence for the exact sequence

$$0 \longrightarrow U_+ \longrightarrow F_+ \longrightarrow \mathcal{P}_\Delta \longrightarrow 0$$

is an exact hexagon

$$H^1(\mathcal{P}_\Delta) \longrightarrow \langle -1\rangle \longrightarrow \mathbb{Q}^*/\mathbf{N}F_+ \longrightarrow H^0(\mathcal{P}_\Delta) \longrightarrow$$
$$\longrightarrow U_+/U_+^2 \longrightarrow F_1/(\sigma-1)F_+ \longrightarrow H^1(\mathcal{P}_\Delta).$$

Since $\langle -1\rangle \to \mathbb{Q}^*/\mathbf{N}F_+$ is injective, $H^1(F_+) \to H^1(\mathcal{P}_\Delta)$ is surjective. If $\Delta < 0$, then $H^1(F_+) = 0$ by Hilbert 90 and $U_+ = U$ is cyclic of even order, so $H^1(\mathcal{P}_\Delta) = F_1/(\sigma-1)F_+ = 0$ and $H^0(\mathcal{P}_\Delta)$ contains $\mathbb{Q}^*/(\langle -1\rangle \cdot \mathbf{N}F_+)$ as a subgroup of index 2. If $\Delta > 0$ and $x$ is in $F_1$, then $x = (\sigma - 1)\alpha$ and thus $-x = (\sigma - 1)(\alpha\sqrt{\Delta})$ for some $\alpha \in F$ by Hilbert 90. Since $-1$ is not in $(\sigma - 1)F_+$, exactly one of the elements $x$ and $-x$ is in $(\sigma - 1)F_+$. It follows that

$H^1(F_+) = \langle -1 \bmod (\sigma - 1)F_+ \rangle$ is cyclic of order 2, and that the map $U_+/U_+^2 \to H^1(F_+)$ is surjective. Further $U_+ \cong \langle -1 \rangle \times \mathbf{Z}$, so $U_+/U_+^2$ has order 4. We conclude again that $H^0(\mathcal{P}_\Delta)$ contains $\mathbf{Q}^*/(\langle -1 \rangle \cdot \mathbf{N}F_+)$ as a subgroup of index 2 and that $H^1(\mathcal{P}_\Delta) = 0$. This proves the second statement in (a).

From the cohomology sequence for

$$0 \longrightarrow \mathcal{P}_\Delta \longrightarrow \mathcal{I}_\Delta \longrightarrow \mathcal{C}(\Delta) \longrightarrow 0$$

we obtain

$$H^0(\mathcal{P}_\Delta) \longrightarrow H^0(\mathcal{I}_\Delta) \longrightarrow \mathcal{C}(\Delta)_2 \longrightarrow H^1(\mathcal{P}_\Delta) = 0,$$

which gives

$$\mathcal{C}(\Delta)_2 = \mathcal{I}_\Delta^{\mathfrak{G}} \,/\, \mathcal{P}_\Delta^{\mathfrak{G}} = \{\mathfrak{a} \in \mathcal{I}_\Delta : \sigma\mathfrak{a} = \mathfrak{a}\} \,/\, \{(\alpha) \in \mathcal{P}_\Delta : \sigma(\alpha) = (\alpha)\}.$$

This proves (a).

Now suppose $\mathfrak{a} \in \mathcal{I}_\Delta$ satisfies $\sigma\mathfrak{a} = \mathfrak{a}$. Since $\sigma$ acts componentwise on $\mathcal{I}_\Delta \cong \bigoplus_p K_{(p)}^*/\mathcal{O}_{\Delta,p}^*$, all local components of $\mathfrak{a}$ are $\sigma$-invariant. Suppose $p \nmid \Delta$. Then $\mathcal{O}_{\Delta,p} = \mathcal{O}_{d,p}$ and $p$ is unramified in $\mathbf{Q}(\sqrt{\Delta})/\mathbf{Q}$. If $p$ is inert in $\mathbf{Q}(\sqrt{\Delta})/\mathbf{Q}$, then $K_{(p)}^*/\mathcal{O}_{\Delta,p}^* = \langle p \bmod \mathcal{O}_{\Delta,p}^* \rangle$ is invariant under $\sigma$. If $p$ splits in $\mathbf{Q}(\sqrt{\Delta})/\mathbf{Q}$, then $K_{(p)}^*/\mathcal{O}_{\Delta,p}^* = \langle \pi \bmod \mathcal{O}_{\Delta,p}^* \rangle \times \langle \pi' \bmod \mathcal{O}_{\Delta,p}^* \rangle$ and the subgroup of invariant ideals equals $\langle \pi\pi' \bmod \mathcal{O}_{\Delta,p}^* \rangle = \langle p \bmod \mathcal{O}_{\Delta,p}^* \rangle$. It follows that there exists a nonzero rational number $\alpha$ such that $\alpha\mathfrak{a} \in \mathcal{I}_\Delta$ has trivial components at all primes $p \nmid \Delta$. We conclude that the image of

$$\phi : J_\Delta = \prod_{\mathfrak{p}|\Delta} \mathbf{Q}(\sqrt{\Delta})_{\mathfrak{p}}^* \longrightarrow \mathcal{C}(\Delta)$$

contains $\mathrm{im}[\mathcal{I}_\Delta^{\mathfrak{G}} \to \mathcal{C}(\Delta)] = \mathcal{C}(\Delta)_2$. This proves (b).

Suppose $p$ divides $\Delta$ with multiplicity 1. Then $p \nmid f$, so $p$ ramifies in $\mathbf{Q}(\sqrt{\Delta})/\mathbf{Q}$ but not in $R_\Delta/\mathbf{Q}(\sqrt{\Delta})$. It follows from the reasoning above that the $\phi$-image of the group

$$D = \prod_{q|\Delta} \chi_q^{-1}\big((K_{(q)}^*/\mathcal{O}_{\Delta,q}^*)^{\mathfrak{G}}\big) \subset J$$

equals $\mathcal{C}(\Delta)_2$. Thus, it suffices to prove that $\phi[H] = \phi[D]$. The inclusion $\subset$ is clear since $\phi[J_\infty] = \langle [\sqrt{\Delta}\mathcal{O}_\Delta] \rangle \subset \mathcal{C}(\Delta)_2$. Let $\mathcal{P}$ be the prime lying over $p$ in $\mathbf{Q}(\sqrt{\Delta})$, and write $F_\mathcal{P}$ for $\mathbf{Q}(\sqrt{\Delta})_\mathcal{P}^* \subset J$. Then the other inclusion follows if we prove that $\phi[F_\mathcal{P}] \subset \phi[H]$. As $p \nmid f$, the local units in $F_\mathcal{P}$ are in the kernel of $\phi$. Thus, it suffices to show that the $\phi$-image of a prime element at $\mathcal{P}$ is in $\phi[H]$. As a prime element $\pi$ in $F_\mathcal{P}$, we take the idèle that has component $\sqrt{\Delta}$ at $\mathcal{P}$ and 1 elsewhere. Let $x = (x_\mathfrak{p})_\mathfrak{p} \in J$ be the idèle that has components $x_\mathfrak{p} = \sqrt{\Delta}$ at all finite primes $\mathfrak{p}$ in $\Delta$ and 1 elsewhere, and $y \in J$ the idèle that

has components $\sqrt{\Delta}$ at all finite primes and 1 at the infinite primes. Then $yx^{-1} \in \ker\phi$ by (9.7), so we see that $\phi(x) = \phi(y) = [\sqrt{\Delta}\mathcal{O}_\Delta] \in \phi[J_\infty] \subset \phi[H]$. It is clear from the definition of $\pi$ that $\pi x^{-1} \in H$. Consequently, $\phi(\pi) = \phi(\pi x^{-1})\phi(x) \in \phi[H]$, as required. □

**9.9 Corollary.** *Let $\Delta$ be a fundamental discriminant, and $Q \in \mathbf{Z}[X,Y]$ the principal quadratic form of discriminant $\Delta$.*

(a) *The 2-torsion subgroup of $\mathcal{C}(\Delta)$ is generated by the classes of the prime ideals dividing $\Delta$, subject to a single relation.*

(b) *There is a unique divisor $d = d_\Delta > 1$ of $\Delta$ for which the equation $Q(x,y) = d$ is solvable in coprime integers $x, y \in \mathbf{Z}$.*

**Proof.** The statement in (a) is immediate from 9.8.

For (b), we let $q_i$, $i = 1, 2, ..., s$, be the prime divisors of $\Delta$, and $\mathfrak{q}_i$ the unique prime ideal in $\mathbf{Q}(\sqrt{\Delta})$ that lies over $q_i$. By (a), there is a unique non-empty subset $R \subset \{1, 2, ..., s\}$ such that $\prod_{i\in R} \mathfrak{q}_i = \alpha\mathcal{O}_\Delta$, with $\alpha \in \mathcal{O}_\Delta$ an element of norm $d > 1$. It is clear that $d \mid \Delta$. If $x$, $y$ are the coordinates of $\alpha$ on a $\mathbf{Z}$-basis 1, $\delta$ of $\mathcal{O}_\Delta$, with $\delta = (1 + \sqrt{\Delta})/2$ if $\Delta$ is odd and $\delta = \sqrt{\Delta}/2$ if $\Delta$ is even, then $x$ and $y$ are coprime and $\mathbf{N}\alpha = Q(x,y) = d$. Conversely, if $d > 1$ divides $\Delta$ and $Q(x,y) = d$ for coprime integers $x$ and $y$, then $x + y\delta \in \mathcal{O}_\Delta$ has norm $d$. The prime ideal factorization of $x + y\delta$ reads $(x + y\delta)\mathcal{O}_\Delta = \prod_{i\in R} \mathfrak{q}_i$ for some non-empty subset $R \subset \{1, 2, ..., s\}$ because $\mathfrak{q}_i^2 \mid (x + y\delta)\mathcal{O}_\Delta$ would imply that $q_i$ divides both $x$ and $y$. It follows that $d$ is uniquely determined by $R$, and (b) is proved. □

If $\Delta < 0$, the relation in (a) is obtained by factoring the ideal $\sqrt{\Delta}\mathcal{O}_\Delta$ that is in the unit class of $\mathcal{C}(\Delta)$. Consequently, the element $d_\Delta$ in (b) then equals

$$d_\Delta = \begin{cases} -\Delta & \text{if } \Delta \text{ is odd;} \\ -\Delta/2 & \text{if } 4\|\Delta; \\ -\Delta/4 & \text{if } 8 \mid \Delta \end{cases}$$

and is an uninteresting quantity. If $\Delta > 0$, the ideal $\sqrt{\Delta}\mathcal{O}_\Delta$ is not necessarily in the unit class. One can obtain the relation between the ramifying ideals in the class group by taking the smallest power $\eta$ of the fundamental unit of $\mathcal{O}_\Delta$ that has positive norm and factor the ideal $(1+\eta)\mathcal{O}_\Delta$. In this case the divisor $d_\Delta$ depends on the fundamental unit of $\mathcal{O}_\Delta$. Here $d_\Delta = \Delta$ (or $\Delta/2$ and $\Delta/4$ when $4\|\Delta$ and $8 \mid \Delta$, respectively) occurs only when the fundamental unit of $\mathcal{O}_\Delta$ has norm $-1$.

Part (a) of the lemma is also true for non-fundamental discriminants, in the sense that the kernel of the canonical surjection

$$\prod_{q|\Delta} (K_{(q)}^*/\mathcal{O}_{\Delta,q}^*)^{\mathfrak{G}} \longrightarrow \mathcal{C}(\Delta)_2 \tag{9.10}$$

from lemma 9.8 is generated by $\prod_{q|\Delta}\langle q\mathcal{O}_{\Delta,q}^*\rangle$ and *one* $\mathfrak{G}$-invariant ideal in this group that does not come from a rational number. As in the fundamental case, this is the ideal $\sqrt{\Delta}\mathcal{O}_\Delta$

for negative $\Delta$ and $(1+\eta)\mathcal{O}_\Delta$ for positive $\Delta$. However, the relation obtained by factoring $(1+\eta)\mathcal{O}_\Delta$ for positive $\Delta$ cannot be described in terms of a divisor of $\Delta$ that is represented by the principal form. The statement in [9] that 9.9(b) is true for non-fundamental $\Delta$ is wrong. For $\Delta = 3^2 \cdot 12$, the principal form $Q = X^2 - 27Y^2$ satisfies $Q(6,1) = 3^2$ and $Q(9,1) = 2 \cdot 3^3$. A meaningful way to generalize 9.9(b) is furnished by the following lemma.

**9.11 Lemma.** *Let $\Delta$ be a discriminant, and write $\mathfrak{G} = \mathrm{Gal}(\mathbb{Q}(\sqrt{\Delta})/\mathbb{Q})$. Then there is a unique integral divisor $\mathfrak{d}_\Delta \neq 1$ of $\sqrt{\Delta}\mathcal{O}_\Delta$ in $\mathcal{I}_\Delta^{\mathfrak{G}}$ that is not contained in $k\mathcal{O}_\Delta$ for any integer $k > 1$ and is in the unit class of $\mathcal{C}(\Delta)$.*

**Proof.** It is clear from the discussion preceding the lemma that there is a unique integral ideal $\mathfrak{d}_\Delta \neq 1$ in $\mathcal{I}_\Delta$ that is not contained in $k\mathcal{O}_\Delta$ for any integer $k > 1$ and is in the unit class of $\mathcal{C}(\Delta)$. Let $x \in \mathcal{O}_\Delta$ be a generator of $\mathfrak{d}_\Delta$. Then $\mathcal{O}_\Delta/x\mathcal{O}_\Delta$ is cyclic as an additive group, since otherwise it would be a product of two cyclic groups $C_m \times C_n$ with $k = \gcd(m,n) > 1$, which entails $x\mathcal{O}_\Delta \subset k\mathcal{O}_\Delta$, contradicting the assumptions. The group $\mathfrak{G}$ acts on $\mathcal{O}_\Delta/x\mathcal{O}_\Delta$ since $x\mathcal{O}_\Delta \in \mathcal{I}_\Delta^{\mathfrak{G}}$, and this action is trivial as the generator $1 + x\mathcal{O}_\Delta$ is $\mathfrak{G}$-invariant. Let $1, \delta$ be an integral basis for $\mathcal{O}_\Delta$. Then $\delta$ and its conjugate $\bar{\delta}$ have the same image in $\mathcal{O}_\Delta/x\mathcal{O}_\Delta$, and consequently $\sqrt{\Delta} = \delta - \bar{\delta}$ is in $x\mathcal{O}_\Delta$. It follows that $\mathfrak{d}_\Delta$ divides $\sqrt{\Delta}\mathcal{O}_\Delta$, as required. □

The ideal $\mathfrak{d}_\Delta$ is generated by $\sqrt{\Delta}/k$ when $\Delta$ is negative and $(1+\eta)/k$ when $\Delta$ is positive, where $k \in \mathbb{Z}$ is the maximal integer for which these elements are in $\mathcal{O}_\Delta$.

The explicit form of the 2-torsion subgroup of $\mathcal{C}(\Delta)$ for fundamental discriminants $\Delta$ was used by Rédei [30] to find the 4-rank of $\mathcal{C}(\Delta)$ in terms of quadratic residue criteria between the prime factors of $\Delta$. By elementary group theory one has an exact sequence of elementary abelian 2-groups

$$\mathcal{C}(\Delta)_2 \longrightarrow \mathcal{C}(\Delta)/\mathcal{C}(\Delta)^2 \xrightarrow{\square} \mathcal{C}(\Delta)^2/\mathcal{C}(\Delta)^4 \longrightarrow 0.$$

Viewing these groups as vector spaces over the field of two elements $\mathbb{F}_2$, it follows immediately that

$$r_4 \;=\; r_2 - \dim_{\mathbb{F}_2} \mathrm{im}[h : \mathcal{C}(\Delta)_2 \to \mathcal{C}(\Delta)/\mathcal{C}(\Delta)^2].$$

An element of $\mathcal{C}(\Delta)/\mathcal{C}(\Delta)^2 = \mathrm{Gal}(H_2/\mathbb{Q}(\sqrt{\Delta}))$ can be specified by giving its action on the elements $\sqrt{d_i}$, $i = 1, 2, ..., s$, that generate the field extension $G_\Delta = H_2$ over $\mathbb{Q}(\sqrt{\Delta})$ in 4.9. Let $\epsilon_{i,\sigma} \in \mathbb{F}_2$ be the exponent of $-1$ that describes the action of $\sigma \in \mathcal{C}(\Delta)/\mathcal{C}(\Delta)^2$ on $\sqrt{d_i}$, i.e.

$$\frac{\sigma(\sqrt{d_i})}{\sqrt{d_i}} = (-1)^{\epsilon_{i,\sigma}}.$$

Using the relation $\prod d_i = \Delta$, one obtains an isomorphism

$$\mathcal{C}(\Delta)/\mathcal{C}(\Delta)^2 \xrightarrow{\sim} H = \{(\epsilon_i)_{i=1}^s : \textstyle\sum \epsilon_i = 0\} \subset \mathbb{F}_2{}^s$$

that sends $\sigma$ to $(\epsilon_{i,\sigma})_i$. If $\mathfrak{p}_i$ is the prime in $\mathbb{Q}(\sqrt{\Delta})$ that lies over $d_i$—for even $d_i$ we take $\mathfrak{p}_i$ to be the prime over 2—the image of $h$ is generated by the Artin symbols $(\mathfrak{p}_i, H_2/\mathbb{Q}(\sqrt{\Delta}))$. Denoting the element $\epsilon_{i,\sigma}$ for $\sigma = (\mathfrak{p}_j, H_2/\mathbb{Q}(\sqrt{\Delta}))$ by $\epsilon_{i,j}$, one has

$$r_4 \;=\; r_2 - \operatorname{rank}_{\mathbb{F}_2}\big(\epsilon_{i,j}\big)_{i,j=1}^{s}.$$

The elements $\epsilon_{i,j}$ are easily computed. If $i \neq j$, the definition of the Artin symbol implies that

$$(-1)^{\epsilon_{i,j}} = \left(\frac{d_i}{d_j}\right)$$

since both expressions are powers of $-1$ that are congruent to $d_i^{(d_j-1)/2} \bmod d_j$, and $\epsilon_{i,i} = \sum_{j\neq i} \epsilon_{j,i}$. For even $d_j$ we have to read the Legendre symbol $\left(\frac{d_i}{d_j}\right)$ as the Kronecker symbol $\left(\frac{d_i}{8}\right) = (-1)^{(d_i-1)/4}$. This gives Rédei's description of $r_4$.

It is easily seen that the Cohn-Lagarias conjecture for $w = 4$ and fundamental discriminants $Dp$ follows immediately from this description. We will state and prove the general 4-rank case in as another direct application of the existence theorem 7.4 in the next section.

## 10. Proof of the 8-rank conjecture

Before we come to the main theorem 10.4 of this section, we construct for any nonzero integer $D \not\equiv 2 \bmod 4$ a number field $K_D$ such that for a prime number $p$, the genus field $H_2$ of $R_{Dp}/\mathbb{Q}(\sqrt{Dp})$ equals $K_D(\sqrt{p^*})$, where $p^* = (-1)^{(p-1)/2}p$. Some cumbersome bookkeeping is necessary to ensure that $K_D$ has the right ramification at 2 for the various values of $D$ and $p$ mod 4.

For each odd prime $p$ satisfying $Dp \equiv 0, 1 \bmod 4$, there is a unique decomposition

$$Dp \;=\; f^2\Big(\prod_{i=1}^{s} d_i\Big)p^* \tag{10.1}$$

in which $f > 0$ and the $d_i$ are distinct fundamental prime power discriminants. If there is an even $d_i$ among them, we will assume that this is $d_1$. If $D$ is odd, the congruence $Dp \equiv 1 \bmod 4$ determines $p$ modulo 4, and $f$ and the $d_i$ do not depend on $p$. If $D$ is even, there are two essentially different decompositions, depending on whether $p \equiv 1 \bmod 4$ or $p \equiv -1 \bmod 4$. The indeterminacy is restricted to the sign of $d_1 = \pm 8$ in case the number of factors 2 in $D$ is odd, and concerns the presence of a fundamental discriminant $-4$ versus an extra factor 2 in $f$ if the number of factors 2 in $D$ is even. This phenomenon gives rise to a definition of the fields $K_D$ that depends on the number of factors 2 in $D$ and the possible choices of $p$ mod 4.

**10.2 Definition.** *Let $D \not\equiv 2 \bmod 4$ be a non-zero integer, $c$ the number of factors 2 in $D$ and define*

$$E = \mathbb{Q}(\sqrt{q^*};\ q \mid D \text{ an odd prime}).$$

*If $c = 0$, i.e. $D$ is odd, we take*

$$K_D^+ = K_D^- = E.$$

*If $c = 2$, we take*

$$\begin{aligned} K_D^+ &= E \text{ and } K_D^- = E(\sqrt{-1}) \quad \text{if } D/4 \equiv 1 \bmod 4 \\ K_D^- &= E \text{ and } K_D^+ = E(\sqrt{-1}) \quad \text{if } D/4 \equiv -1 \bmod 4. \end{aligned}$$

*If $c = 3$, we take*

$$\begin{aligned} K_D^+ &= E(\sqrt{2}) \text{ and } K_D^- = E(\sqrt{-2}) \quad \text{if } D/8 \equiv 1 \bmod 4 \\ K_D^- &= E(\sqrt{2}) \text{ and } K_D^+ = E(\sqrt{-2}) \quad \text{if } D/8 \equiv -1 \bmod 4. \end{aligned}$$

*If $c = 4$, we take*

$$K_D^+ = K_D^- = E(\sqrt{-1}).$$

*If $c \geq 5$, we take*

$$K_D^+ = K_D^- = E(\sqrt{-1}, \sqrt{2}).$$

The following lemma shows that this is exactly the definition we need.

**10.3 Lemma.** *Let $D \not\equiv 2 \bmod 4$ be a non-zero integer and $p$ an odd prime number satisfying $Dp \equiv 0, 1 \bmod 4$. Then the genus field $H_2$ of $R_{Dp}/\mathbb{Q}(\sqrt{Dp})$ equals*

$$\begin{aligned} H_2 &= K_D^+(\sqrt{p}) \quad \text{if } p \equiv 1 \bmod 4 \\ H_2 &= K_D^-(\sqrt{-p}) \quad \text{if } p \equiv -1 \bmod 4. \end{aligned}$$

**Proof.** This is a straightforward deduction from (9.5). □

If $a \in \{\pm 1\}$, we will use the notation $K_D^a$ to denote that field from $K_D^+$ and $K_D^-$ that has "sign" $a$.

We can now formulate and prove our answer to the Cohn-Lagarias conjectures 2.8 for $w = 8$.

**10.4 Theorem.** *Let $D \not\equiv 2 \bmod 4$ be a nonzero integer, and suppose $a \in \{\pm 1\}$ satisfies $Da \equiv 0, 1 \bmod 4$. Define $K = K_D^a$ as in 10.2, and let $M$ be the maximal abelian extension of $K$ that*

(a) *is of exponent dividing 2;*

(b) *is unramified outside $2D \cdot \infty$;*

(c) *can locally at primes over 2 be obtained from $K$ by adjoining square roots of local units in case $D$ is odd.*

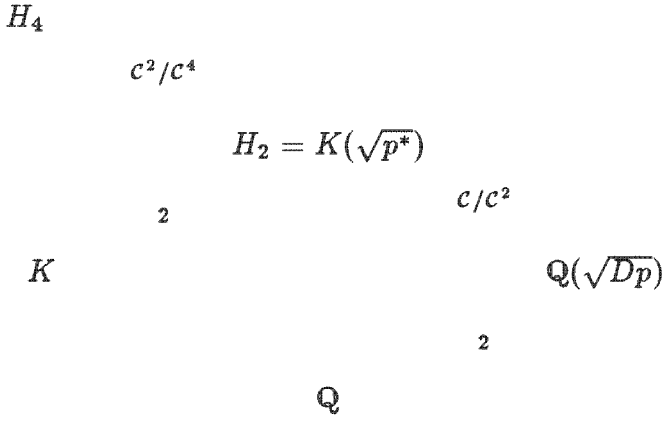
*If $p_1, p_2 \nmid 2D$ are rational primes that are congruent to $a$ mod 4 and satisfy $[p_1, M/\mathbb{Q}] = [p_2, M/\mathbb{Q}]$, then there is an isomorphism*

$$C(Dp_1)/C(Dp_1)^8 \cong C(Dp_2)/C(Dp_2)^8.$$

We remark that condition (c) in theorem 8.3 is equivalent to the requirement that the local conductors of $M/K$ at primes over 2 divide 4 in case $D$ is odd.

It should be noted that theorem 2.9 is a direct consequence of 10.4.

**Proof of 10.4.** let $p \equiv a \bmod 4$ be a prime number, and denote the subfield of $R_{Dp}$ that is invariant under $C^s = C(Dp)^s$ by $H_s$. The following diagram of fields illustrates the situation.




Extend the generator $\sigma$ of $\mathrm{Gal}(\mathbb{Q}(\sqrt{Dp})/\mathbb{Q})$ to $R_{Dp}$ such that it is the identity on $K$. Then (9.4) gives us

$$\mathrm{Gal}(H_4/K) \cong C(Dp)^2/C(Dp)^4 \times \langle\sigma\rangle,$$

so $\mathrm{Gal}(H_4/K)$ is an elementary abelian 2-group. Define the 'non-fundamental part' $f$ of $Dp$ by 10.1. The conductor of $R_{Dp}/\mathbb{Q}(\sqrt{Dp})$ then divides $(f)\cdot\infty$. We claim that the conductor of $H_4/K$ divides $(fp)\cdot\infty$. For the $p$-part of the conductor, this is clear from the diagram as $H_4/K(\sqrt{p^*})$ is unramified at primes over $p$. For the finite non-$p$-part of the conductor, it follows from lemma 8.2, with $M = K(\sqrt{p^*})$ and $L = H_4$. For the infinite part of the conductor, there is nothing to prove.

We can now apply theorem 8.1 for the extension $K/k = K_D^a/\mathbb{Q}$ with parameters $m = 2$, $\mathfrak{d} = (f)\cdot\infty$ and $S$ the set of primes dividing $D\cdot\infty$. In this case $K_m = K_2 = K$ and the governing field for $(\mathfrak{d}, m, S)$-equivalence furnished by theorem 8.1 is the field that is claimed to govern the 8-rank in 10.4. Thus, let $p_1$ and $p_2$ be two primes that do not divide $2D$ and are congruent to $a$ modulo 4, and suppose that the Frobenius classes of $p_1$ and $p_2$ in $\mathrm{Gal}(M/K)$ coincide. Then these primes are $(D, 2, S)$-equivalent in the sense of 7.4. If

we write $L(p)$ for the maximal abelian extension of $K$ that has exponent 2 and conductor dividing $(fp)\cdot\infty$, this means that there exists an isomorphism

$$g:\ \mathrm{Gal}(L(p_1)/\mathbb{Q})\xrightarrow{\sim}\mathrm{Gal}(L(p_2)/\mathbb{Q})$$

that respects the projections onto $\mathrm{Gal}(K/\mathbb{Q})$ such that the following is satisfied:

(a) the $g$-image of the inertia group of any prime above $p_1$ is the inertia group of a prime above $p_2$.

(b) for each rational prime $q$ dividing $D$ and $q=\infty$, there is an isomorphism of $\mathbb{Q}_q$-algebras

$$L(p_1)\otimes_{\mathbb{Q}}\mathbb{Q}_q\cong L(p_2)\otimes_{\mathbb{Q}}\mathbb{Q}_q$$

such that the group actions of $\mathrm{Gal}(L(p_1)/\mathbb{Q})$ on $L(p_2)\otimes\mathbb{Q}_q$ via this isomorphism and via $g$ coincide. Here the $q$-adic field $\mathbb{Q}_q$ for $q=\infty$ is the field of real numbers.

We have to prove that the conditions above imply that there is an isomorphism

$$C(Dp_1)/C(Dp_1)^8\ \cong\ C(Dp_2)/C(Dp_2)^8.$$

We first prove that $g$ induces an isomorphism

$$\mathrm{Gal}(L(p_1)/\mathbb{Q}(\sqrt{Dp_1}))\xrightarrow{\sim}\mathrm{Gal}(L(p_2)/\mathbb{Q}(\sqrt{Dp_2})).$$

Let $E\subset L(p_2)$ be the quadratic field for which $\mathrm{Gal}(L(p_2)/E)$ is the $g$-image of the Galois group $\mathrm{Gal}(L(p_1)/\mathbb{Q}(\sqrt{Dp_1}))$. Then $E/\mathbb{Q}$ is ramified at $p_2$ by 6.5(a) and locally isomorphic to $\mathbb{Q}(\sqrt{Dp_1})/\mathbb{Q}$ at the primes in $D\cdot\infty$ by 6.5(b). This implies that the local conductors of $\mathbb{Q}(\sqrt{Dp_1})/\mathbb{Q}$ and $E/\mathbb{Q}$ are equal at the primes in $D\cdot\infty$. As $E/\mathbb{Q}$ is unramified outside $Dp_2$ and infinity, its conductor equals the conductor of the extension $\mathbb{Q}(\sqrt{Dp_2})/\mathbb{Q}$. It follows that $E=\mathbb{Q}(\sqrt{Dp_2})$, since quadratic fields are uniquely determined by their conductor over $\mathbb{Q}$.

Denote the maximal abelian extension $F$ of $\mathbb{Q}(\sqrt{Dp_i})$ inside $L(p_i)$ that is dihedral over $\mathbb{Q}$ with group

$$\mathrm{Gal}(F/\mathbb{Q})\ \cong\ \mathrm{Gal}(F/\mathbb{Q}(\sqrt{Dp_i}))\rtimes\mathrm{Gal}(\mathbb{Q}(\sqrt{Dp_i})/\mathbb{Q})$$

by $F(Dp_i)$. Then we have isomorphisms

$$\mathrm{Gal}(F(Dp_1)/\mathbb{Q}(\sqrt{Dp_1}))\xrightarrow{\sim}\mathrm{Gal}(F(Dp_2)/\mathbb{Q}(\sqrt{Dp_2})).$$

The field $F(Dp_i)$ is abelian of exponent dividing 4 over $\mathbb{Q}(\sqrt{Dp_i})$ and dihedral over $\mathbb{Q}$, but it need not be equal to $H_4(Dp_i)$ since we only know that its conductor over $H_2(Dp_i)$—and not $\mathbb{Q}(\sqrt{Dp_i})$—divides $(f)\cdot\infty$. The extension $H_4(Dp_i)/\mathbb{Q}(\sqrt{Dp_i})$ is the maximal

subextension of $F(Dp_i)/\mathbb{Q}(\sqrt{Dp_i})$ that is of conductor dividing $(f)\cdot\infty$. It follows from the existence of the local isomorphisms at primes dividing $f$ (condition (b)) that the extensions $H_4(Dp_i)/\mathbb{Q}(\sqrt{Dp_i})$ for $i=1$ and $i=2$ correspond. We conclude that we have an isomorphism

$$\mathrm{Gal}(H_4(Dp_1)/\mathbb{Q}(\sqrt{Dp_1}))\xrightarrow{\sim}\mathrm{Gal}(H_4(Dp_2)/\mathbb{Q}(\sqrt{Dp_2}))$$

that is compatible with the local isomorphisms $H_4(Dp_1)\otimes_{\mathbb{Q}}\mathbb{Q}_q\xrightarrow{\sim}H_4(Dp_2)\otimes_{\mathbb{Q}}\mathbb{Q}_q$ for each rational prime $q$ in $D\cdot\infty$. From these local isomorphisms we obtain for each $q\mid D\cdot\infty$ an isomorphism between the subgroups

$$\mathbb{Q}(\sqrt{Dp_i})^*_{(q)}=\left(\mathbb{Q}(\sqrt{Dp_i})\otimes_{\mathbb{Q}}\mathbb{Q}_q\right)^*\subset\ J_i=J_{\mathbb{Q}(\sqrt{Dp_i})}$$

for $i=1$ and $i=2$. Note that this isomorphism respects the action of the group $\mathfrak{G}=\mathfrak{G}_i=\mathrm{Gal}(\mathbb{Q}(\sqrt{Dp_i})/\mathbb{Q})$ under the obvious identification $\mathfrak{G}_1=\mathfrak{G}_2$. Combining the isomorphisms for the various $q$, we have a commutative diagram of $\mathfrak{G}$-homomorphisms

$$\begin{array}{ccc}\prod\limits_{q\mid D}\mathbb{Q}(\sqrt{Dp_1})^*_{(q)} & \xrightarrow{\oplus_{q\mid D}\chi_q} & \prod\limits_{q\mid D}\left(\mathbb{Q}(\sqrt{Dp_1})^*_{(q)}/\mathcal{O}^*_{Dp_1,q}\right)\\ \downarrow\wr & & \downarrow\wr\\ \prod\limits_{q\mid D}\mathbb{Q}(\sqrt{Dp_2})^*_{(q)} & \xrightarrow{\oplus_{q\mid D}\chi_q} & \prod\limits_{q\mid D}\left(\mathbb{Q}(\sqrt{Dp_2})^*_{(q)}/\mathcal{O}^*_{Dp_2,q}\right).\end{array}$$

Taking inverse images of elements that are mapped to $\mathfrak{G}$-invariant ideals, we obtain an isomorphism

$$\prod_{q\mid D}\chi_q^{-1}\left(\left(\mathbb{Q}(\sqrt{Dp_1})^*_{(q)}/\mathcal{O}^*_{Dp_1,q}\right)^{\mathfrak{G}}\right)\xrightarrow{\sim}\prod_{q\mid D}\chi_q^{-1}\left(\left(\mathbb{Q}(\sqrt{Dp_2})^*_{(q)}/\mathcal{O}^*_{Dp_2,q}\right)^{\mathfrak{G}}\right).$$

Combining this with the isomorphism at the infinite primes, we have an isomorphism $H_1\xrightarrow{\sim}H_2$, with $H_i$ the subgroup defined in lemma 9.8(c) for $p=p_i$ and $\Delta=Dp_i$ that maps onto $C(Dp_i)_2$.

By the canonicity of the local Artin map, the local isomorphisms at the primes over $D\cdot\infty$ give rise to a commutative diagram

$$\begin{array}{ccccc}\prod\limits_{q\mid D\cdot\infty}\mathbb{Q}(\sqrt{Dp_1})^*_{(q)} & \longrightarrow & \mathrm{Gal}(H_4(Dp_1)\,/\,\mathbb{Q}(\sqrt{Dp_1})) & \xrightarrow{\sim} & C(Dp_1)\,/\,C(Dp_1)^4\\ \downarrow\wr & & \downarrow\wr & & \downarrow\wr\\ \prod\limits_{q\mid D\cdot\infty}\mathbb{Q}(\sqrt{Dp_2})^*_{(q)} & \longrightarrow & \mathrm{Gal}(H_4(Dp_2)\,/\,\mathbb{Q}(\sqrt{Dp_2})) & \xrightarrow{\sim} & C(Dp_2)\,/\,C(Dp_2)^4.\end{array}$$

Pasting all information together yields a commutative diagram

$$\begin{array}{ccccc} H_1 & \longrightarrow & C(Dp_1)_2 & \longrightarrow & C(Dp_1) \,/\, C(Dp_1)^4 \\ \downarrow\wr & & & & \downarrow\wr \\ H_2 & \longrightarrow & C(Dp_2)_2 & \longrightarrow & C(Dp_2) \,/\, C(Dp_2)^4. \end{array}$$

The homomorphism $H_i \to C(Dp_i)_2$ is surjective, so the right vertical arrow induces an isomorphism between the images of $C(Dp_i)_2$ in $C(Dp_i)/C(Dp_i)^4$ for $i = 1$ and $i = 2$. This implies that $C(Dp_1)$ and $C(Dp_2)$ have equal 8-ranks, since the 8-rank is given by

$$\begin{aligned} r_8 &= \dim_{\mathbf{F}_2}[\ker(C(Dp_i)_2 \longrightarrow C(Dp_i)/C(Dp_i)^4)] \\ &= r_2 - \dim_{\mathbf{F}_2}[\mathrm{im}(C(Dp_i)_2 \longrightarrow C(Dp_i)/C(Dp_i)^4)] \end{aligned}$$

and we know the 2-ranks of $C(Dp_1)$ and $C(Dp_2)$ to be equal. This finishes the proof of theorem 10.4. □

From the proof of 10.4 we obtain the following corollary.

**10.5 Corollary.** *In the situation of 10.4 let $p_1$ and $p_2$ be rational primes congruent to $a$ mod 4 that have the same Frobenius class in $\mathrm{Gal}(M/\mathbb{Q})$. Suppose that the 8-ranks of $C(Dp_1)$ and $C(Dp_2)$ equal zero. Then there is a commutative diagram*

$$\begin{array}{ccc} H_1 & \longrightarrow & C(Dp_1)_2 \\ \downarrow\wr & & \downarrow\wr \\ H_2 & \longrightarrow & C(Dp_2)_2 \end{array}$$

*where $H_i$ is the subgroup $H$ from* 9.8(c) *for $p = p_i$ and $\Delta = Dp_i$.*

**Proof.** The fact that the 8-ranks are zero implies that the canonical maps $C(Dp_i)_2 \longrightarrow C(Dp_i)/C(Dp_i)^4$ are injective, so the isomorphism between the images from the proof of 10.4 induces the required isomorphism. □

Since our theorem 8.1 can prove the existence of governing fields for 8-ranks, it is not too surprising that there also is a choice of parameters that gives governing fields for 4-ranks.

**10.6 Theorem.** *Let $D \not\equiv 2 \bmod 4$ be a non-zero integer, and let $M$ be the field*

$$\mathbb{Q}(\sqrt{-1}, \sqrt{q} : q \text{ is a prime divisor of } D).$$

*If $p_1, p_2 \nmid 2D$ are two rational primes that have the same Artin symbol in $M/\mathbb{Q}$ and satisfy $Dp_i \equiv 0, 1 \bmod 4$, $i = 1, 2$, then $C(Dp_1)/C(Dp_1)^4 \cong C(Dp_2)/C(Dp_2)^4$.*

**Proof.** Apply 8.1 for $K = k = \mathbb{Q}$ with $m = 2$, $\mathfrak{d} = (D) \cdot \infty$ and $S$ the set of primes dividing $(D) \cdot \infty$. The field $M$ defined above is the maximal abelian extension of $\mathbb{Q}$ that is of exponent 2 and unramified outside $2D \cdot \infty$ and can locally be obtained from $\mathbb{Q}_2$ by adjoining square roots of units if $D$ is odd, so it governs $(\mathfrak{d}, m, S)$-equivalence on $\mathbb{Q}$. It follows from (9.5) and the definition of $L(p)$, for $p \nmid 2D$ a rational prime satisfying $Dp \equiv 0, 1 \bmod 4$, that

$$H_2(p) \subset L(p) \subset H_2(p)(\zeta_8),$$

with $H_2(p) = G_{Dp}$ the genus field of discriminant $Dp$. If $p_1$ and $p_2$ are equivalent, then one argues along the lines of the proof of theorem 10.4 to conclude that there is a commutative diagram

$$\begin{array}{ccccc} H_1 & \longrightarrow & C(Dp_1)_2 & \longrightarrow & C(Dp_1) \,/\, C(Dp_1)^2 \\ \downarrow \wr & & & & \downarrow \wr \\ H_2 & \longrightarrow & C(Dp_2)_2 & \longrightarrow & C(Dp_2) \,/\, C(Dp_2)^2. \end{array}$$

It follows as in the proof of 10.4 that $C(Dp_1)$ and $C(Dp_2)$ are isomorphic modulo 4-th powers. □

As a consequence of 10.4, we give the following extension of the theorem.

**10.7 Theorem.** *Let $D$, $a$, $M$ be as in* 10.4, *and let $p_1, p_2 \nmid 2D$ be rational primes that are congruent to $a$* mod 4 *and satisfy $[p_1, M/\mathbb{Q}] = [p_2, M/\mathbb{Q}]$. If $C(Dp_1)$ has* 8*-rank zero, the following holds.*

(a) *If $Dp_1$ is fundamental and $d_{Dp_i}$ is defined as in* 7.3(*b*), *then*

$$d_{Dp_2} = \begin{cases} d_{Dp_1} & \text{if } p_1 \nmid d_{Dp_1}; \\ d_{Dp_1} \cdot p_2/p_1 & \text{if } p_1 \mid d_{Dp_1}. \end{cases}$$

(b) *If $\mathfrak{d}_{Dp_i}$ is defined as in* 7.5 *and $\mathfrak{p}_i \in \mathcal{I}_{Dp_i}$ is the unique prime ideal over $p_i$, then there is an isomorphism $\phi : \oplus_{q|D} \mathcal{I}_{Dp_1,q} \xrightarrow{\sim} \oplus_{q|D} \mathcal{I}_{Dp_2,q} \subset \mathcal{I}_{Dp_2}$ induced by local isomorphisms $\mathbb{Q}(\sqrt{Dp_1})_{(q)} \xrightarrow{\sim} \mathbb{Q}(\sqrt{Dp_2})_{(q)}$ such that*

$$\mathfrak{d}_{Dp_2} = \begin{cases} \phi(\mathfrak{d}_{Dp_1}) & \text{if } \mathfrak{p}_1 \nmid \mathfrak{d}_{Dp_1}; \\ \phi(\mathfrak{d}_{Dp_1}\mathfrak{p}_1^{-1}) \cdot \mathfrak{p}_2 & \text{if } \mathfrak{p}_1 \mid \mathfrak{d}_{Dp_1}. \end{cases}$$

**Proof.** Since $\mathfrak{d}_{Dp_i}$ and $d_{Dp_i}$ are quantities that describe the non-trivial relation between the generators of $C(Dp_i)$ from 9.9(b), it suffices for both (a) and (b) to prove that there is a commutative diagram

$$\begin{array}{ccc} \prod_{q|Dp_1} (\mathbb{Q}(\sqrt{Dp_1})^*_{(q)} / \mathcal{O}^*_{Dp_1,q})^{\mathfrak{G}} & \xrightarrow{h} & \prod_{q|Dp_2} (\mathbb{Q}(\sqrt{Dp_2})^*_{(q)} / \mathcal{O}^*_{Dp_2,q})^{\mathfrak{G}} \\ \downarrow \text{can} & & \downarrow \text{can} \\ C(Dp_1)_2 & \longrightarrow & C(Dp_2)_2, \end{array}$$

where $\mathfrak{G} = \mathfrak{G}_i = \mathrm{Gal}(\mathbb{Q}(\sqrt{Dp_i})/\mathbb{Q})$ under the obvious identification $\mathfrak{G}_1 = \mathfrak{G}_2$ and the vertical maps are those from (9.10). Here $h$ is induced by $\mathfrak{G}$-isomorphisms

$$\mathbb{Q}(\sqrt{Dp_1})_{(q)} \xrightarrow{\sim} \mathbb{Q}(\sqrt{Dp_2})_{(q)}$$

for each rational prime $q \mid D$ and an isomorphism

$$(\mathbb{Q}(\sqrt{Dp_1})^*_{(p_1)}/\mathcal{O}^*_{Dp_1,p_1})^{\mathfrak{G}} \xrightarrow{\sim} (\mathbb{Q}(\sqrt{Dp_2})^*_{(p_2)}/\mathcal{O}^*_{Dp_2,p_2})^{\mathfrak{G}}$$

mapping $\sqrt{Dp_1}$ mod $\mathcal{O}^*_{Dp_1,p_1}$ to $\sqrt{Dp_2}$ mod $\mathcal{O}^*_{Dp_2,p_2}$.

It follows from 10.5 that the local isomorphisms at $q \mid D$ exist and that the diagram above is commutative for the components at $q \mid D$. The groups $(\mathbb{Q}(\sqrt{Dp_i})^*_{(p_i)}/\mathcal{O}^*_{Dp_i,p_i})^{\mathfrak{G}}$ are infinite cyclic, generated by the class of $\sqrt{Dp_i}$. Correspondence of the images of $(\prod_{q|D} 1) \times \sqrt{Dp_i}$ under $\mathcal{C}(Dp_1) \xrightarrow{\sim} \mathcal{C}(Dp_2)$ follows from 10.5 if one realizes that this image in $\mathcal{C}(Dp_i)$ equals that of $\prod_{q|D\cdot\infty} \sqrt{Dp_i}^{-1} \times \prod_{q\nmid D\cdot\infty} 1 \in J_{\mathbb{Q}(\sqrt{Dp_i})}$ in $\mathcal{C}(Dp_i)$ by (7.1). This proves 10.7. □

**10.8 Example.** We consider the 8-rank of the class group of $\mathbb{Q}(\sqrt{-21p})$, for $p \equiv 3 \bmod 4$ a variable prime. This is the case that was treated in detail in theorem 2.10. We have $K = K^-_{21} = \mathbb{Q}(\sqrt{-3}, \sqrt{-7})$ by 10.3. Our governing field $M$ is the maximal exponent 2 extension of $K$ that is unramified outside $(2 \cdot 3 \cdot 7)$, and has completions at primes over 2 that can be obtained from the 2-adic completion $\mathbb{Q}_2(\sqrt{-3}, \sqrt{-7}) = \mathbb{Q}_2(\sqrt{-3})$ of $K$ by adjoining square roots of local units.

We know already that $K$ has class number one, and that its fundamental unit is $\epsilon = (\sqrt{-3} + \sqrt{-7})/2$. We write $\eta = -\epsilon^2 = (5 + \sqrt{21})/2$. The unit group of $\mathcal{O}_K$ is $\mathcal{O}^*_K = \zeta_6 \times \langle\epsilon\rangle$. The field $M$ is obtained from $K$ by adjoining the square roots of all units in $K$ and the square roots of a set of generators of primes over 3 and 7. The primes over 3 and 7 in $K$ are $\mathfrak{P}_3 = (\eta - 1)$, $\mathfrak{P}_7 = (\epsilon - 1)$ and $\mathfrak{P}'_7 = (\epsilon + 1)$. We find

$$M = K(\sqrt{-1}, \sqrt{\epsilon}, \sqrt{\eta - 1}, \sqrt{\epsilon - 1}, \sqrt{\epsilon + 1}).$$

Theorem 2.9 of chapter I shows that the smallest governing field for the 8-rank of $\mathbb{Q}(\sqrt{-21p})$ is the field

$$M' = \mathbb{Q}\Big(\sqrt{-1}, \sqrt{3}, \sqrt{7}, \sqrt{2 - \sqrt{-3}}, \sqrt{2(7 + \sqrt{21})}, \sqrt{-3 + 2\sqrt{-3}}\Big).$$

The field $M'$ is contained in $M$ as it is obtained from $K$ by taking square roots of elements that are divisible by primes over 3 and 7 only. Thus, we have found a quadratic extension of $M'$ as a governing field for the 8-rank of $\mathbb{Q}(\sqrt{-21p})$. This example shows that that our theorem does not necessarily give the *minimal* governing field for the 8-rank of $\mathcal{C}(Dp)$.

## References


1. P. Barrucand, H. Cohn, *Primes of type $x^2 + 32y^2$, class number and residuacity*, J. reine angew. Math. **238**, 67–70 (1969).
2. Z.I. Borevich, I.R. Shafarevich, *Number Theory*, Academic Press, London-New York, 1966, reprint 1987.
3. E. Brown, C. J. Parry, *Class numbers of imaginary quadratic number fields having exactly three discriminantal divisors*, J. reine angew. Math. **260**, 31–34 (1973).
4. E. Brown, *The power of 2 dividing the class number of a binary quadratic discriminant*, J. Number Theory **5**, 413–419 (1973).
5. E. Brown, *Class numbers of real quadratic number fields*, Trans. Amer. Math. Soc. **190**, 99–107 (1974).
6. G. Bruckner, *Charakterisierung der galoisschen Zahlkörper, deren zerlegte Primzahlen durch binäre quadratische Formen gegeben sind*, Math. Nachr. **32**, 317–326 (1966).
7. J.W.S. Cassels, A. Fröhlich, *Algebraic Number Theory*, Academic Press, London-New York, 1967, reprint 1987.
8. C. Chevalley, *Deux théorèmes d'arithmétique*, J. Math. Soc. Japan **3**, 36–44 (1951).
9. H. Cohn, J.C. Lagarias, *On the existence of fields governing the 2-invariants of the class group of $\mathbb{Q}(\sqrt{dp})$ as $p$ varies*, Math. Comp. **41**, 711–730 (1983).
10. G. Cornell, *The Structure of the Ray Class Group*, preprint, University of Connecticut, Storrs, 1986.
11. A. Greaves and R.W.K. Odoni, *Weil-numbers and CM-fields*, J. reine angew. Math. **391**, 198–212 (1988).
12. F. Halter-Koch, *Geschlechtertheorie der Ringklassenkörper*, J. reine angew. Math. **250**, 107–108 (1971).
13. H. Hasse, *Über die Teilbarkeit durch $2^3$ der Klassenzahl imaginärquadratischer Zahlkörper mit genau zwei verschiedenen Diskriminantenprimteilern*, J. reine angew. Math. **241**, 1–6 (1970).
14. H. Hasse, *Über die Teilbarkeit durch $2^3$ der Klassenzahl der quadratischen Zahlkörper mit genau zwei verschiedenen Diskriminantenprimteilern*, Math. Nachr. **46**, 61–70 (1970).
15. P.J. Hilton, U. Stammbach, *A Course in Homological Algebra*, Springer GTM 4, 1970.
16. P. Kaplan, *Divisibilité par 8 du nombre des classes des corps quadratiques dont le 2-groupe des classes est cyclique, et réciprocité biquadratique*, J. Math. Soc. Japan **25**, 596–608 (1973).
17. P. Kaplan, *Sur le 2-groupe des classes d'idéaux des corps quadratiques*, J. reine angew. Math. **283/284**, 313–363 (1976).
18. G. Karpilovsky, *Units of classical rings*, Oxford University Press, 1988.

19. M. Kneser, *Lineare Abhängigkeit von Wurzeln*, Acta Arith. **26**, 307–308 (1974).
20. H. Koch, W. Zink, *Über die 2-Komponente der Klassengruppe quadratischer Zahlkörper mit zwei Diskriminantenteilern*, Math. Nachr. **54**, 309–333 (1972).
21. S. Lang, *Algebraic number theory*, Addison-Wesley, Reading, 1970.
22. H.W. Lenstra, Jr, *On Artin's conjecture and Euclid's algorithm in global fields*, Inventiones math. **42**, 201–224 (1977).
23. H.W. Lenstra, Jr., *On the calculation of regulators and class numbers in quadratic fields*, pp. 123–150 in: J. Armitage (ed.), *Journées Arithmétiques* 1980, London Math. Soc. Lecture Note Series **56**, Cambridge University Press, Cambridge.
24. S. Mac Lane, *Homology*, Springer Grundlehren 114, Berlin-New York 1963.
25. P. Morton, *Density results for the 2-classgroups of imaginary quadratic fields*, J. reine angew. Math. **332**, 156–187 (1982).
26. P. Morton, *Density results for the 2-classgroups and fundamental units of real quadratic fields*, Studia Scientiarum Math. Hungarica **17**, 21–43 (1982).
27. P. Morton, *The quadratic number fields with cyclic 2-class groups*, Pac. J. Math. **108**, 165–175 (1983).
28. P. Morton, *Governing fields for the 2-classgroup of* $\mathbb{Q}(\sqrt{-q_1q_2p})$ *and a related reciprocity law*, submitted to Acta Arith.
29. L. Rédei, H. Reichardt, *Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppen eines beliebigen quadratischen Zahlkörpers*, J. reine angew. Math. **170**, 69–74 (1934).
30. L. Rédei, *Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper*, J. reine angew. Math. **171**, 55–60 (1935).
31. L. Rédei, *Über die Grundeinheit und die durch 8 teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper*, J. reine angew. Math. **171**, 131–148 (1935).
32. L. Rédei, *Ein neues zahlentheoretisches Symbol mit Anwendungen auf die Theorie der quadratischen Zahlkörper*, J. reine angew. Math. **180**, 1–43 (1939).
33. A. Schinzel, *Abelian binomials, power residues and exponential congruences*, Acta Arith. **32**, 245–274 (1977).
34. J-P. Serre, *Corps Locaux*, Hermann, Paris, 1968 (translation: *Local Fields*, Springer, Berlin-New York, 1979).
35. P. Stevenhagen, *Class groups and governing fields*, Thesis, UC Berkeley, 1988.
36. E. Van Tieghem, *Radikalen van multiplikatieve groepen in de algebraïsche getaltheorie*, Thesis, Katholieke Universiteit Leuven, 1975.
37. W.C. Waterhouse, *Pieces of eight in class groups of quadratic fields*, J. Number Theory **5**, 95–97 (1973).

*Peter STEVENHAGEN*
*Department of Mathematics*
*University of California*
*Berkeley, CA 94720*

*Adresse à partir de Mai 1990 :*

*Université de Franche-Comté Besançon*
*Faculté des Sciences*
*Laboratoire de Mathématiques*
*U.A. CNRS 741*
*25030 Besançon Cedex*