Procyclic Galois Extensions of Algebraic Number Fields

David Brink

Ph.D. thesis

Defence:
February 23, 2006

Thesis advisor:
Christian U. Jensen, Københavns Universitet, Denmark

Evaluating committee:
Ian Kiming, Københavns Universitet, Denmark
Niels Lauritzen, Aarhus Universitet, Denmark
Noriko Yui, Queen's University, Canada

Matematisk Afdeling · Københavns Universitet · 2006

David Brink
Matematisk Afdeling
Universitetsparken 5
2100 København Ø
Denmark
E-mail: brink@math.ku.dk

Contents

Preface

The present booklet constitutes my Ph.-D. thesis in mathematics. It was written in the period 2003–2005 under the supervision of Christian U. Jensen whom it is my pleasure to thank warmly for his interest and support over the years.

The thesis consists of 5 chapters. Chapter 1 is an introduction to the theory of procyclic Galois extensions. Chapters 2 and 3 are extended versions of my papers [3] and [4]. Chapters 4 and 5 are based on two papers still in preparation. For the benefit of the busy reader, I have included a thorough abstract to the entire thesis.

Abstract

Denote by $\mathbb{Z}_p$ the additive group of p-adic integers. The main theme of this thesis is the existence and properties of Galois extensions of algebraic number fields with Galois group $\mathbb{Z}_p$, in short $\mathbb{Z}_p$-extensions. We shall however also consider some non-abelian pro-p-groups as Galois groups (in particular in Chapter 5). The thesis is divided into 5 chapters.

Chapter 1. In this introductory chapter, results of Iwasawa and Shafarevich are summarised, note in particular Theorems 1, 3, and 6. The connection between $\mathbb{Z}_p$-extensions and Leopoldt's Conjecture is discussed. The notion of p-rationality is defined, and the classification of 2-rational imaginary quadratic fields is given (Theorem 10), apparently for the first time (correctly).

Chapter 2. Consider an imaginary quadratic number field K and an odd prime p. The following question is investigated: *if the p-class group of K is non-trivial and cyclic, is the p-Hilbert class field of K (or part of it) then embeddable in a $\mathbb{Z}_p$-extension of K?* It is shown that the answer is always *yes* when K is p-rational (Lemma 12), and two criteria for p-rationality are given (Theorem 13 of which only part (b) is new). Some examples are given indicating that "most" K are p-rational. When K is not p-rational, an effective algoritm is given that determines $\mathbb{Z}_p$-embeddability (Theorem 15). Numerical examples show that all five cases of that theorem occur.

Chapter 3. Consider an imaginary quadratic number field K and an odd prime p. The (well-known) fact that K has a unique $\mathbb{Z}_p$-extension which is prodihedral over $\mathbb{Q}$ is shown (Proposition 18). We call this extension the *anti-cyclotomic* p-extension of K.

We give laws for the decomposition of prime ideals in the anti-cyclotomic extension (Theorems 22 and 24). The laws involve representation of some rational prime power q^h by certain quadratic forms of the same discriminant d_K as K. Using Gauss' theory of composition of forms, we show that it suffices instead to represent q by some form (Section 3.3). The whole story becomes particularly simple when each genus of forms of discriminant d_K consists of a single class

(Theorem 28). This happens for 65 values of d_K closely connected to Euler's *numeri idonei* or *convenient numbers*

The decomposition laws also depend on how many steps of the anti-cyclotomic extension are unramified. This dependence may be turned around, meaning that if we know how certain primes decompose, then we can compute the number of unramified steps (Examples 25–27). In particular, we can answer whether the p-Hilbert class field of K is contained in the anti-cyclotomic extension and thus is $\mathbb{Z}_p$-embeddable.

In section 3.5 we show how to find explicit polynomials whose roots generate the first step of the anti-cyclotomic extension. When K is not p-rational this involves using the decomposition laws to identify the right polynomial f among a finite number of candidates (Examples 31 and 32). When this is done, one obtains nice laws for the splitting of f modulo q. For instance we show that $X^5 + 5X^2 + 3$ splits into linear factor modulo a prime number $q \neq 3, 5$ if and only if q is of the form $x^2 + 5xy + 100y^2$ or $3x^2 + 15xy + 50y^2$.

Chapter 4. Consider an imaginary quadratic number field K with Hilbert class field K_H. The ring class field $N = N(2^\infty)$ over K of conductor 2^∞ is the maximal 2-ramified (i.e. unramified outside 2) abelian extension of K which is generalised dihedral over $\mathbb{Q}$.

We determine the structure of the Galois group $\mathrm{Gal}(N/K_H)$ (Lemma 33) and, in some cases, $\mathrm{Gal}(N/K)$ (Corollaries 39, 44, 49).

We give a law for the decomposition of prime ideals in the anti-cyclotomic 2-extension of K (Theorem 34) similar to that from Chapter 3 (but more complicated). Again, this law involves representation of rational prime powers by quadratic forms.

In Sections 4.5–4.8, quadratic forms are discussed. For example, we show the new result (Lemma 36) that a prime number congruent to 1 modulo 16 is representable by both or none of the forms $X^2 + 32Y^2$ and $X^2 + 64Y^2$, whereas a prime number congruent to 9 modulo 16 is representable by one, but not both of these forms. New proofs of two formulae of Hasse regarding the order of cyclic 2-class groups are given. The key ingredient in these proofs are two new explicit expressions ((4.10) and (4.12)) for a form representing a class of order 4 in the form class group.

The first step of the anti-cyclotomic 2-extension K_{anti}/K is of the form $K(\sqrt{a})$ with an $a \in \mathbb{Z}$. As a $\mathbb{Z}_2$-extension, K_{anti}/K is unramified outside 2. However, the lower steps might be unramified also at 2. Let ν denote the number of unramified steps. When the 2-class group of K is cyclic (possibly trivial), we give algorithms to compute both ν and a (Theorems 37, 42, 47). In most cases we can even give explicit expressions for ν (Theorems 38, 43, 48) and a (Theorems 41, 46, 50 of which 41 and 46 are not new). The proofs of these results involve the class number formulae of Hasse.

When the 2-class field of K is non-trivial and cyclic, one can ask if it can be embedded into a $\mathbb{Z}_2$-extension of K. We answer this question completely (Theorem 51) using many of our previous results. For any (odd or even) prime p, it is conjectured that there exist imaginary quadratic fields with $\mathbb{Z}_p$-embeddable p-class field of arbitrarily high degree,

Put $K = \mathbb{Q}(\sqrt{-l})$ and $K' = \mathbb{Q}(\sqrt{-2l})$ with a prime $l \equiv 1 \pmod 8$. There are some quite surprising interrelations between these two fields. Let h and h' be the class numbers of K and K', respectively. We show $8 \mid h \;\Leftrightarrow\; 8 \mid h'$ for $l \equiv 1 \pmod{16}$, and $8 \mid h \;\Leftrightarrow\; 8 \nmid h'$ for $l \equiv 9 \pmod{16}$ (Theorem 52). We also give results on interrelations between the anti-cyclotomic 2-extensions of K and K' (Theorems 54, 55). Finally, a conjecture for primes $l \equiv 1 \pmod{16}$ is put forth that would allow a certain assumption in Theorems 54 and 55 to be omitted. This conjecture has been verified by the author for all primes up to 14 millions.

In the last section, many numerical examples are given showing that the results of the previous sections are best possible.

Chapter 5. The pro-2-group $\mathfrak{H} = \langle a, b \mid ba = a^{-1}b^{-1},\ ba^{-1} = ab^{-1}\rangle$ is described as a fibre product of two copies of the 2-adic prodihedral group $\mathbb{D}_2$. The *socle* of a $\mathfrak{H}$-extension $M/\mathbb{Q}$ is defined as its unique biquadratic subfield. It is investigated which biquadratic extensions of $\mathbb{Q}$ appear as socle of a $\mathfrak{H}$-extension. This is for example the case for $\mathbb{Q}(\sqrt{-1}, \sqrt{2})$ (Example 58). If the socle of a $\mathfrak{H}$-extension $M/\mathbb{Q}$ is of the type $\mathbb{Q}(\sqrt{-l}, \sqrt{2})$ with an odd prime l, it is shown than M contains a square root of either $\sqrt{2}+2$ or $\sqrt{2}-2$ (Lemma 59). The determination of the right square root is not trivial, and some partial results in this direction are given (Theorems 60 and 61).

The pro-2-group $\mathfrak{G} = \langle a, b \mid ab^2 = b^2a,\ a^2b = ba^2\rangle$ is described as a fibre product of $\mathbb{Z}_2 \times \mathbb{Z}_2$ with $\mathbb{D}_2$. $\mathfrak{G}$ is not realisable as Galois group over $\mathbb{Q}$. Some results on the number $\nu(\mathfrak{G}, K)$ of $\mathfrak{G}$-extensions of imaginary quadratic fields of type $K = \mathbb{Q}(\sqrt{-l})$ or $K = \mathbb{Q}(\sqrt{-2l})$ with l an odd prime are given, for example it is shown that always $\nu(\mathfrak{G}, K) \le 3$ (Theorem 63). Further, it is shown that the free pro-2-group of rank 2 is realisable over K in some cases ($l \equiv 3, 5 \pmod 8$), but not in others ($l = 353$, for example).

Chapter 1

Iwasawa's theory of $\mathbb{Z}_p$-extensions

1.1 Introduction and notation

Let p be a fixed prime number. Denote by $\mathbb{Z}_p$ the additive group of p-adic integers. We have

$$\mathbb{Z}_p \cong \varprojlim \mathbb{Z}/p^n,$$

i.e. $\mathbb{Z}_p$ is the infinite procyclic pro-p-group.

We shall consider Galois extensions of algebraic number fields with Galois group $\mathbb{Z}_p$, in short $\mathbb{Z}_p$-extensions.

In this chapter, an overview of important results is given. In particular we emphasise Theorem 1 and Theorem 3 which are due to Iwasawa [18], Theorem 6 (and its Corollary 7) due to Shafarevich [26] , and the definition of the *anti-cyclotomic* extension at the end of section 1.6.

In all of this chapter 1, we use the following notation:

p :	a prime number
$\mathbb{Z}_p$:	the additive group of p-adic integers
ζ :	a primitive p'th root of unity
K :	an algebraic number field
$\mathcal{O}$:	the ring of integral elements in K
$\mathscr{E}$:	the group of units $\mathcal{O}$
r_1, r_2 :	the number of real and complex primes of K, respectively
$U_\mathfrak{p}$:	the group of local units at $\mathfrak{p}$ (note $U_\mathfrak{p} = K_\mathfrak{p}^*$ for $\mathfrak{p}$ infinite)
K_H :	the Hilbert class field of K
K_∞ :	the maximal abelian p-extension of K unramified outside p
$K_{\mathbb{Z}_p}$:	the composite of all $\mathbb{Z}_p$-extensions of K

1.2 Ramification in $\mathbb{Z}_p$-extensions

An algebraic extension L/K is called **unramified outside** p if all primes $\mathfrak{p}$ of K with $\mathfrak{p} \nmid p$ (including the infinite ones) are unramified. More generally, for a (usually finite) set S of primes of K, it is said that L/K is **unramified outside** S if all primes $\mathfrak{p} \notin S$ are unramified. We shall later see that being unramified outside a finite set of primes is a rather strict condition.

Theorem 1. *Any $\mathbb{Z}_p$-extension L of the algebraic number field K is unramified outside p.*

Proof. Let $\mathfrak{p}$ be a prime of K with $\mathfrak{p} \nmid p$ and assume indirectly that $\mathfrak{p}$ ramifies in L. Consider a localisation $L_{\mathfrak{p}}/K_{\mathfrak{p}}$. This means the following: Pick some prime $\mathfrak{P}$ of L extending $\mathfrak{p}$. Let $L_n \subset L$ be the subextension of degree p^n over K and denote by $L_{n,\mathfrak{p}}$ the completion of L_n with respect to the restriction of $\mathfrak{P}$ to L_n. Then we have the tower

$$K_{\mathfrak{p}} \subsetneqq L_{1,\mathfrak{p}} \subsetneqq L_{2,\mathfrak{p}} \subsetneqq \dots$$

and $L_{\mathfrak{p}}$ is defined as the union of the $L_{n,\mathfrak{p}}$.

We may assume that $L_{\mathfrak{p}}/K_{\mathfrak{p}}$ is a totally ramified $\mathbb{Z}_p$-extension. By the below valuation-theoretic lemma, each $L_{n,\mathfrak{p}}/K_{\mathfrak{p}}$ is a radical extension. Hence $K_{\mathfrak{p}}$ contains a primitive p^n'th root of unity for all n, a contradiction. □

Lemma 2. *Let F be a field with a complete and discrete valuation. Assume E/F is a totally and tamely ramified extension of finite degree n. Then there exists a uniformising element $\Pi \in E$ with $\Pi^n \in F$. In particular E/F is a radical extension.*

Proof. Let Π and π be uniformising elements for E and F, respectively. Write $\Pi^n = u\pi$ with some unit $u \in E$. Since F and E have the same residue field, we may pick a unit $u' \in F$ with $u' \equiv u \pmod{\Pi}$. Put $u^* := u/u'$ and $\pi^* := u'\pi$. Then $\Pi^n = u^*\pi^*$ where $\pi^* \in F$, and the unit $u^* \in E$ satisfies $u^* \equiv 1 \pmod{\Pi}$. By Hensel's Lemma, u^* is an n'th power: $u^* = v^n$. The uniformising element $\Pi^* := \Pi/v$ then satisfies $(\Pi^*)^n = \pi^*$. Now replace Π with Π^*. □

1.3 Rank and essential rank of pro-p-groups

Let X be a pro-p-group. The **Frattini subgroup** $\Phi(X)$ of X is the closed subgroup generated by the commutators and the p'th powers. The quotient $X/\Phi(X)$ is an elementary abelian p-group. The **rank** of X is defined as the dimension of $X/\Phi(X)$ as vectorspace over $\mathbb{F}_p$. By Burnside's Basis Theorem[1], this rank equals the cardinality of any minimal generating subset of X.

Now let X be an *abelian* pro-p-group. We may view X as a (compact) $\mathbb{Z}_p$-module. Iwasawa defines the **essential rank** of X as the dimension over the p-adic numbers $\mathbb{Q}_p$ of the tensor product

$$X \otimes_{\mathbb{Z}_p} \mathbb{Q}_p.$$

If X has finite rank, the Elementary Divisor Theorem gives

$$X \cong (\mathbb{Z}_p)^a \times T$$

where $a < \infty$ is the essential rank of X, and T is a finite p-group.

Let us finally note that if

$$1 \to X \to Y \to Z \to 1$$

is an exact sequence of abelian pro-p-groups, then exactness is conserved by tensoring with $\mathbb{Q}_p$, and hence

$$\text{ess.rank}(Y) = \text{ess.rank}(X) + \text{ess.rank}(Z).$$

In particular, $\text{ess.rank}(X) = \text{ess.rank}(Y)$ if Z is finite.

The reason we introduce the above concepts is this: We shall take as X the Galois group $\text{Gal}(K_\infty/K)$. It will then be a key point of this chapter to show that $\text{rank}(X)$ is finite and to give an expression for this rank as well as for $\text{ess.rank}(X)$. We can interpret the essential rank as the maximal number of linearly disjoint $\mathbb{Z}_p$-extensions of K.

1.4 Leopoldt's conjecture

Consider the algebraic number field K and the rational prime p. For any prime $\mathfrak{p}$ of K dividing p, denote by $U_\mathfrak{p}$ the group of local units at $\mathfrak{p}$, i.e. the group of units in the ring of integers $\mathcal{O}_\mathfrak{p}$ of the completion $K_\mathfrak{p}$. Further, consider the *higher unit groups*

$$U_\mathfrak{p}^{(n)} = \{x \in U_\mathfrak{p} \mid x \equiv 1 \pmod{\mathfrak{p}^n}\}$$

for $n \geq 1$.

[1] Burnside's Basis Theorem is well known for finite p-groups, see for instance [17]. It can be extended to pro-p-groups without too much trouble. Note incidentally that the cyclic group of order 6 shows that the assumption that X is a p-group can not be omitted.

For sufficiently large n, the $\mathfrak{p}$-adic logarithm is an isomorphism

$$\log_{\mathfrak{p}} : U_{\mathfrak{p}}^{(n)} \to (\mathfrak{p}^n, +).$$

Hence $U_{\mathfrak{p}}^{(n)}$ is a free $\mathbb{Z}_p$-module of rank $[K_{\mathfrak{p}} : \mathbb{Q}_p]$. It follows that $U_{\mathfrak{p}}^{(1)}$ is a $\mathbb{Z}_p$-module of rank $[K_{\mathfrak{p}} : \mathbb{Q}_p]$. Hence the direct product

$$U^{(1)} := \prod_{\mathfrak{p}|p} U_{\mathfrak{p}}^{(1)}$$

is a $\mathbb{Z}_p$-module of rank

$$\sum_{\mathfrak{p}|p} [K_{\mathfrak{p}} : \mathbb{Q}_p] = [K : \mathbb{Q}].$$

Let $\mathscr{E}$ be the group of global units of K and put

$$\mathscr{E}_1 = \{\epsilon \in \mathscr{E} \mid \forall \mathfrak{p} \mid p : \epsilon \equiv 1 \pmod{\mathfrak{p}}\}.$$

The abelian group $\mathscr{E}_1$ is a subgroup of $\mathscr{E}$ of finite index and hence has the same rank which is

$$\operatorname{rank}(\mathscr{E}_1) = \operatorname{rank}(\mathscr{E}) = r_1 + r_2 - 1$$

by Dirichlet's unit theorem (r_1 and r_2 have the usual meaning). We may consider $\mathscr{E}_1$ as a subgroup of $U^{(1)}$ via the embedding

$$\mathscr{E}_1 \hookrightarrow U^{(1)}, \ \epsilon \mapsto (\epsilon, \ldots, \epsilon).$$

The closure $\overline{\mathscr{E}}_1$ of $\mathscr{E}_1$ with respect to the topology of $U^{(1)}$ is a (compact) $\mathbb{Z}_p$-module.

One could think that the $\mathbb{Z}_p$-rank of $\overline{\mathscr{E}}_1$ equals the $\mathbb{Z}$-rank of $\mathscr{E}_1$. This might also very well be true, however only the inequality

$$\mathbb{Z}_p\text{-rank}(\overline{\mathscr{E}}_1) \leq r_1 + r_2 - 1$$

is clear. We have the

Leopoldt Conjecture for the field K and the prime p: The $\mathbb{Z}_p$-rank of $\overline{\mathscr{E}}_1$ is $r_1 + r_2 - 1$.

This conjecture was formulated by Leopoldt [21] in 1962 for totally real fields.

If $K = \mathbb{Q}$ or K is imaginary quadratic, then $r_1 + r_2 - 1 = 0$ and hence the Leopoldt Conjecture is trivially true. Further, it was shown by Brumer [6] that the Leopoldt Conjecture is true if K is abelian over $\mathbb{Q}$ or over an imaginary quadratic field. In the general case, however, neither proof nor counter-example is known.

1.5 The maximal number of linearly disjoint $\mathbb{Z}_p$-extensions

Let K_∞ be the maximal abelian p-extension of K which is unramified outside p. By Theorem 1, any $\mathbb{Z}_p$-extension of K is contained in K_∞. Write

$$[K:\mathbb{Q}] = r_1 + 2r_2$$

where r_1 and $2r_2$ are the numbers of real and complex embeddings of K, respectively.

THEOREM 3. *The rank of the abelian pro-p-group Gal(K_∞/K) is finite, and the essential rank a satisfies*

$$r_2 + 1 \leq a \leq [K:\mathbb{Q}].$$

Equality $a = r_2 + 1$ holds if and only if the Leopoldt Conjecture for the field K and the prime p is true.

We have

$$\mathit{Gal}(K_\infty/K) \cong (\mathbb{Z}_p)^a \times T$$

with a finite p-group T.

Proof. We start by summarising some results from class field theory. Let J be K's idèle group. For any abelian extension L/K, the *global norm symbol*

$$(\ \ ,L/K) : J \to \mathrm{Gal}(L/K)$$

is a continuous, surjective homomorphism. The kernel N is called the *normgroup* of L. The mapping $L \mapsto N$ gives a 1-1 corresponding between the abelian extensions L/K and the closed subgroups $N \subseteqq J$ containing the principal idèles K^* and with J/N totally disconnected. Moreover, a prime $\mathfrak{p}$ of K is unramified in L/K iff the normgroup N contains the group $U_\mathfrak{p}$ of local units at $\mathfrak{p}$.

Put

$$U' = \prod_{\mathfrak{p}|p} U_\mathfrak{p} \ \ , \ \ U'' = \prod_{\mathfrak{p}\nmid p} U_\mathfrak{p} \ \ , \ \ U = U' \times U''.$$

U is an open subgroup of J. The normgroup of the maximal abelian extension of K unramified outside p is

$$H = \overline{U''K^*}.$$

So $\mathrm{Gal}(K_\infty/K)$ is isomorphic to the p-part of J/H. The normgroup corresponding to K's Hilbert class field is $H' = UK^*$. Clearly

$$H \subset H' \subset J,$$

and H' has finite index in J (because J/H' is isomorphic to K's class group). Evidently $U'H = H'$, so

$$H'/H \cong U'/(U' \cap H).$$

Let $U^{(1)}$ be as in section 1.4. It is a subgroup of U' of finite index. So $U^{(1)}/(U^{(1)} \cap H)$ has finite index in $U'/(U' \cap H)$.

Recall we have an embedding

$$\psi : \mathscr{E}_1 \hookrightarrow U^{(1)}.$$

This embedding does not commute with the standard embedding $K^* \hookrightarrow J$, so we cannot omit the ψ here.

We claim

$$\psi(\overline{\mathscr{E}}_1) = U^{(1)} \cap H.$$

For an $\varepsilon \in \mathscr{E}_1$, we have

$$\psi(\varepsilon) = \varepsilon \cdot \frac{\psi(\varepsilon)}{\varepsilon} \in K^*U''$$

and hence $\overline{\mathscr{E}}_1 \subseteqq \overline{K^*U''} = H$. Proving the other inclusion is somewhat technical and we omit the details. The reader is referred to [27], page 266.

Write the rank of $\overline{\mathscr{E}}_1$ (as a $\mathbb{Z}_p$-module) as $r_1+r_2-1-\delta$ with a $\delta \geq 0$. Then $\delta = 0$ iff the Leopoldt Conjecture for K and p holds. Hence $U^{(1)}/(U^{(1)} \cap H) = U^{(1)}/\overline{\mathscr{E}}_1$ has $\mathbb{Z}_p$-rank

$$[K : \mathbb{Q}] - (r_1 + r_2 - 1 - \delta) = r_2 + 1 + \delta$$

by section 1.4. This module is isomorphic to a submodule of J/H of finite index. It follows that the p-part of J/H has finite rank and that its essential rank is $r_2 + 1 + \delta$. The claims follow by section 1.3. □

The composite $K_{\mathbb{Z}_p}$ of all $\mathbb{Z}_p$-extensions of K (inside a fixed algebraic closure) is called the **maximal $\mathbb{Z}_p$-power extension** of K. By Theorem 3, $\mathrm{Gal}(K_{\mathbb{Z}_p}/K)$ is a free $\mathbb{Z}_p$-module of rank a. Therefore, $a = a(K)$ is the *maximal number of linearly disjoint $\mathbb{Z}_p$-extensions* of K. No number field K is known for which $a(K)$ depends on the prime p (hence the notation); in fact no K is known for which $a(K) \neq r_2 + 1$ since that would constitute a counter-example to the Leopoldt Conjecture.

For an arbitrary (abstract) field k, it still holds that $\mathrm{Gal}(k_{\mathbb{Z}_p}/k)$ is a free $\mathbb{Z}_p$-module, but its rank is in general no longer equal to the essential rank of $\mathrm{Gal}(k_\infty/k)$ (see [12]). The rank of $\mathrm{Gal}(k_{\mathbb{Z}_p}/k)$ is called the **Iwasawa number** of k with respect to p. For number fields, we henceforth use the term *Iwasawa number* instead of the equivalent *essential rank*.

From Theorem 3 follows immediately $a(\mathbb{Q}) = 1$, i.e. there is a unique $\mathbb{Z}_p$-extension of $\mathbb{Q}$ for any p. We can describe this extension explicitly. Adjoint to $\mathbb{Q}$ all roots of unity of p-power order. By class field theory, this is the maximal abelian extension of $\mathbb{Q}$ unramified outside $\{p, \infty\}$. Its Galois group over $\mathbb{Q}$ is isomorphic to $\mathbb{Z}_p \times \mathbb{Z}/(p-1)$ for $p > 2$ and to $\mathbb{Z}_2 \times \mathbb{Z}/2$ for $p = 2$. Hence it has a unique subfield $\mathbb{Q}_{\text{cycl}}$ with Galois group $\mathbb{Z}_p$ over $\mathbb{Q}$. We call $\mathbb{Q}_{\text{cycl}}$ the **cyclotomic** $\mathbb{Z}_p$-extension of $\mathbb{Q}$. In the simplest case $p = 2$, one finds

$$\mathbb{Q} \subset \mathbb{Q}\left(\sqrt{2}\right) \subset \mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right) \subset \cdots \subset \mathbb{Q}_{\text{cycl}}.$$

For any number field K, the composite $K_{\text{cycl}} = K\mathbb{Q}_{\text{cycl}}$ is a $\mathbb{Z}_p$-extension of K called the cyclotomic extension of K.

From Theorem 3 also follows $a(K) = 2$ for an imaginary quadratic field K. Hence K has maximally 2 linearly disjoint $\mathbb{Z}_p$-extensions. One such, of course, is K_{cycl}. We shall have more to say on finding a "complementary" $\mathbb{Z}_p$-extension of K.

In chapter 2, we shall concern ourselves with the determination of the torsion T from Theorem 3 in case K is imaginary quadratic. A first step is to compute the rank of $\text{Gal}(K_\infty/K)$. This is done in section 1.8 using a theorem of Shafarevich. To formulate and prove this result, we first need to introduce the concept of *hyperprimary elements* in section 1.7.

1.6 The dihedral Iwasawa number

For a prime p, define the **p-adic prodihedral group** $\mathbb{D}_p$ as the natural projective limit of the dihedral groups of order $2p^n$, $n \geq 1$:

$$\mathbb{D}_p = \varprojlim D_{p^n}.$$

$\mathbb{D}_p$ contains the procyclic group $\mathbb{Z}_p$ as unique abelian subgroup of index 2. Any element $\tau \in \mathbb{D}_p \backslash \mathbb{Z}_p$ has order 2 and inverts $\mathbb{Z}_p$ by conjugation. So we may write $\mathbb{D}_p$ as the semidirect product

$$\mathbb{D}_p = \mathbb{Z}_p \rtimes \mathbb{Z}/2.$$

If a field extension M/K has $\text{Gal}(M/K) \cong \mathbb{D}_p$, we denote the subfield corresponding to the subgroup $\mathbb{Z}_p$ as the **quadratic base** of the $\mathbb{D}_p$-extension.

Now let L/K be a quadratic extension of number fields and consider the maximal $\mathbb{Z}_p$-power extension $L_{\mathbb{Z}_p}$ for some prime p. Let $a(K)$ and $a(L)$ be the Iwasawa numbers of K and L with respect to p. Define L^+ and L^- as the maximal subextensions of $L_{\mathbb{Z}_p}/L$, normal over K, such that $\mathrm{Gal}(L/K)$ operates trivially on $\mathrm{Gal}(L^+/L)$ and by inversion on $\mathrm{Gal}(L^-/L)$, respectively. Then $L_{\mathbb{Z}_p}$ is the composite of $L^+ = K_{\mathbb{Z}_p}L$ and L^- and hence

$$\mathrm{Gal}(L^+/L) \cong \mathbb{Z}_p^{a(K)} \quad , \quad \mathrm{Gal}(L^-/L) \cong \mathbb{Z}_p^{a(L)-a(K)}$$

(see section 3 of [12] for details on this).

We call $a(L/K) := a(L) - a(K)$ the **dihedral Iwasawa number** of K (with respect to p). It is the maximal number of linearly disjoint (over L) $\mathbb{D}_l$-extensions with quadratic base L/K.

Clearly, L^+ and L^- are linearly disjoint over L for $p > 2$, but it is not always the case for $p = 2$. This will cause us some trouble.

Now consider an imaginary quadratic field K. It has dihedral Iwasawa number

$$a(K/\mathbb{Q}) = a(K) - a(\mathbb{Q}) = 2 - 1 = 1.$$

Hence there exists a unique $\mathbb{D}_p$-extension with quadratic base $K/\mathbb{Q}$ for every prime p. We call it the **anti-cyclotomic** $\mathbb{Z}_p$-extension of K and denote it K_{anti}. As noted previously, K_{cycl} and K_{anti} are linearly disjoint over K when $p > 2$. For $p = 2$, however, the intersection could be $K(\sqrt{2})$ which is always the first step of the cyclotomic 2-extension of K.

1.7 Hyperprimary elements

Consider a finite set S of primes of K. We shall mainly be interested in the case $S = \{\mathfrak{p} \mid \mathfrak{p} \text{ divides } p\}$, but for the moment S is arbitrary. Define the set of **hyperprimary** elements

$$V := \{x \in K^* \mid (x) = \mathfrak{a}^p \text{ for an ideal } \mathfrak{a} \subseteqq \mathcal{O}\}$$

and the set of S-**hyperprimary** elements

$$V_S := V \cap \bigcap_{\mathfrak{p} \in S} K_{\mathfrak{p}}^p.$$

Evidently one has $V = V_\emptyset$ and the inclusions

$$K^{*p} \subseteqq V_S \subseteqq V \subseteqq K^*.$$

The quotient V_S/K^{*p} is a vectorspace over $\mathbb{F}_p$, the dimension of which is denoted $\sigma(S)$. First we compute $\sigma(\emptyset)$:

Lemma 4. *Let $\mathscr{E} = \mathcal{O}^*$ be the group of units in K and let $\mathscr{C}$ be the class group of K. Then*

$$\dim(V/K^{*p}) = \mathrm{rank}_p(\mathscr{E}) + \mathrm{rank}_p(\mathscr{C}).$$

Proof. For a hyperprimary $x \in V$, the ideal $\mathfrak{a}$ with $(x) = \mathfrak{a}^p$ is unique. Therefore

$$V \longrightarrow \mathscr{C} \ , \ x \mapsto [\mathfrak{a}]$$

is a well-defined homomorphism. The image is $\{[\mathfrak{a}] \in \mathscr{C} \mid [\mathfrak{a}]^p = 1\}$, and the kernel is $\mathscr{E} \cdot K^{*p}$. The lemma follows. □

Remark 5. Assume that K contains a primitive p'th root of unity and that S contains all primes dividing p. Then there is the following characterisation of S-hyperprimary elements:

$$x \in V_S \ \Leftrightarrow \ \begin{cases} \text{In the extension } K(\sqrt[p]{x})/K, \text{ every finite} \\ \text{prime (i.e. every prime ideal) is unramified,} \\ \text{and moreover, every } \mathfrak{p} \in S \text{ splits.} \end{cases}$$

In this case, $K(\sqrt[p]{V_S})$ is the maximal elementary abelian p-extension of K in which all prime ideals are unramified and all $\mathfrak{p} \in S$ split. Kummer theory then gives

$$V_S/K^{*p} \cong \mathrm{Gal}(K(\sqrt[p]{V_S})/K).$$

A reference to hyperprimary elements is [16].

1.8 A theorem of Shafarevich

Let S be a finite set of primes of the number field K. Define K_S as the maximal elementary abelian p-extension of K which is unramified outside S, and let $d(S)$ be the dimension of $\mathrm{Gal}(K_S/K)$ over $\mathbb{F}_p$. In other words, $d(S)$ is the maximal number of linearly disjoint $\mathbb{Z}/p$-extensions of K unramified outside S. The following theorem of Shafarevich links this number to the dimension $\sigma(S)$ of V_S/K^{*p} (see section 1.7).

Theorem 6. *Let $t(S)$ be the number of non-complex primes $\mathfrak{p} \in S$ such that the completion $K_\mathfrak{p}$ contains a primitive p'th root of unity ζ. Put $\delta = 1$ if $\zeta \in K$, else $\delta = 0$. Further, let*

$$\lambda(S) = \sum_{\mathfrak{p} \in S, \ \mathfrak{p} | p} [K_\mathfrak{p} : \mathbb{Q}_p]$$

and $r = r_1 + r_2 - 1$. *Then one has the equality*

$$d(S) = \sigma(S) + t(S) - \delta + \lambda(S) - r \ .$$

In particular, K_S *is a finite extension of* K.

Proof. The proof is somwhat similar to that of Theorem 3 whose notation we reuse. The definition of K_S gives that its normgroup is the open group

$$N_S = U_S J^p K^*$$

with $U_S = \prod_{\mathfrak{p} \notin S} U_{\mathfrak{p}}$. So we have to compute the dimension of

$$J/N_S \cong \mathrm{Gal}(K_S/K).$$

Consider the following sequence of vectorspaces over $\mathbb{F}_p$:

$$1 \longrightarrow V_S/K^{*p} \xrightarrow{f_4} V/K^{*p} \xrightarrow{f_3} U_\emptyset/U_S U^p \xrightarrow{f_2} J/N_S \xrightarrow{f_1} J/N_\emptyset \longrightarrow 1.$$

Here f_1, f_2 and f_4 are defined the natural way. For an $x \in V$, the principal idèle (x) is the product of a $u \in U_\emptyset$ and a $y^p \in J^p$. The idèle u is unique modulo U^p. Therefore $f_3 : x \mapsto u$ gives a well-defined homomorphism.

With a little work, it is seen that the above sequence is exact. We show below that all dimensions are finite. Thus

$$\dim(V_S/K^{*p}) - \dim(V/K^{*p}) + \dim(U_\emptyset/U_S U^p) - \dim(J/N_S) + \dim(J/N_\emptyset) = 0. \quad (*)$$

The dimension of V_S/K^{*p} is $\sigma(S)$ by definition. The dimensionen of J/N_S is $d(S)$ by definition. We have

$$U_\emptyset/U_S U^p \cong \prod_{\mathfrak{p} \in S} U_{\mathfrak{p}}/U_{\mathfrak{p}}^p \quad , \quad \dim(U_\emptyset/U_S U^p) = \sum_{\mathfrak{p} \in S} \dim(U_{\mathfrak{p}}/U_{\mathfrak{p}}^p).$$

By the determination of powers in valued fields (use Hensel's lemma or see [16], for instance), $U/U_S U^p$ has dimension $t(S) + \lambda(S)$. Note that $K_\emptyset$ is the maximal unramified elementary abelian p-extension of K. Hence $\dim(J/N_\emptyset)$ equals the p-rank of K's class group $\mathscr{C}$. By Dirichlet's unit theorem, the p-rank of K's group of units $\mathscr{E}$ is $r + \delta$. Lemma 4 now gives that V/K^{*p} has dimension $r + \delta + \dim(J/N_\emptyset)$. Putting everything into $(*)$ gives the claim. □

It is an important, but straightforward observation that $d(S)$ equals the rank of the Galois group over K of the *maximal* p*-extension unramified outside* S (see definition of rank in section 1.3). The same goes for the maximal *abelian* p-extension of K unramified outside S. In particular we get for

$S = \{\mathfrak{p} \mid \mathfrak{p} \text{ divides } p\}$:

Corollary 7. *The rank of the pro-p-group Gal(K_∞/K) is $\sigma(S)+t(S)-\delta+r_2+1$.* □

This rank can be computed explicitly in some simple cases:

Corollary 8. *Assume $p = 2$ and that $K = \mathbb{Q}(\sqrt{-\Delta})$ is imaginary quadratic with a square-free $\Delta \in \mathbb{N}$. Then the rank of the pro-2-group Gal(K_∞/K) is*

$$\begin{cases} r+2 & \textit{if all } p_i \equiv \pm 1 \pmod 8 \\ r+1 & \textit{otherwise} \end{cases}$$

where r is the number of odd primes $p_1, \ldots, p_r$ dividing Δ.

Proof. Clearly $r_2 = \delta = 1$. Let S be the set of primes of K dividing 2. So $t(S)$ is the cardinality of S, i.e. $t(S) = 2$ when $\Delta \equiv -1 \pmod 8$ so that 2 splits in K, else $t(S) = 1$. To compute $\sigma(S)$, let E/K be the maximal unramified abelian 2-extension in which all primes $\mathfrak{p} \in S$ split. So $\sigma(S)$ is the 2-rank of Gal(E/K). The genus field F of K contains E. Let μ be the number of primes dividing K's discriminant d_K. So μ equals $r+1$ or r according to whether d_K is even or odd. Define $p_i^* := \pm p_i$ such that $p_i^* \equiv 1 \pmod 4$. Genus theory gives $F = K(\sqrt{p_1^*}, \ldots, \sqrt{p_r^*})$. The 2-rank of Gal$(F/K)$ is $\mu - 1$. The degree of F/E is 1 or 2 since this extension is cyclic (Gal(F/E) is the decomposition group of an unramified extension). Now note for a $\mathfrak{p} \in S$:

$$\begin{aligned} \mathfrak{p} \text{ splits in } K(\sqrt{p_i^*})/K \quad &\Leftrightarrow \quad p_i^* \text{ is a square in } K_\mathfrak{p} = \mathbb{Q}_2(\sqrt{-\Delta}) \\ &\Leftrightarrow \quad p_i^* \text{ or } -\Delta p_i^* \text{ is a square in } \mathbb{Q}_2 \\ &\Leftrightarrow \quad p_i^* \text{ or } -\Delta p_i^* \text{ is } \equiv 1 \pmod 8 \end{aligned}$$

It follows that $\sigma(S) = \mu - 1$ if all $p_i \equiv \pm 1 \pmod 8$ or $-\Delta \equiv 5 \pmod 8$, else $\sigma(S) = \mu - 2$. Putting everything into Corollary 7 gives the claim. □

1.9 The notion of p-rationality

The situation is particularly simple when

$$\mathrm{Gal}(K_\infty/K) \cong (\mathbb{Z}_p)^{r_2+1}.$$

In this case K is called **p-rational.** This notion was introduced in [19].

Theorem 9. *The following conditions are equivalent:*

(a) The field K is p-rational.

(b) Gal(K_∞/K) has rank $r_2 + 1$.

(c) Gal(K_∞/K) is torsion-free, and the Leopoldt Conjecture for K and p holds.

(d) One has $V_S = K^{*p}$ where V_S denotes the set of S-hyperprimary elements in K for $S = \{\mathfrak{p} \mid \mathfrak{p}$ divides $p\}$. Further, if K contains a primitive p'th root of unity ζ, then K has only one prime $\mathfrak{p}$ dividing p. If K does not contain ζ, then neither do the completions $K_\mathfrak{p}$ with $\mathfrak{p} \mid p$.

Proof. The equivalence of (a), (b), and (c) follows immediately from Theorem 3. The equivalence of (b) and (d) follows from Corollary 7. □

Classifying the p-rational fields is not trivial. We show here one result in that direction and return to the question in section 2.2.

Theorem 10. *(a) $\mathbb{Q}$ is p-rational for all primes p.*

(b) The 2-rational imaginary quadratic number fields are exactly $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-l})$, and $\mathbb{Q}(\sqrt{-2l})$ for primes $l \equiv 3, 5$ (mod 8).

Proof. (a) Let $\mathbb{Q}(\zeta_{p^\infty})$ denote the field obtained by adjoining to $\mathbb{Q}$ all roots of unity of p-power order. Then the maximal abelian extension of $\mathbb{Q}$ unramified outside p is the maximal real subfield of $\mathbb{Q}(\zeta_{p^\infty})$. This is a $\mathbb{Z}_2$-extension for $p = 2$ and a $\mathbb{Z}_p \times \mathbb{Z}/((p-1)/2)$-extension for $p > 2$. The claim follows. (One also sees that $\mathbb{Q}$ is 2-rational by noting that $\mathbb{Q}(\sqrt{2})$ is the only quadratic extension of $\mathbb{Q}$ which is unramified outside 2.)

(b) For an imaginary quadratic field K we have $r_1 = 1$, so p-rationality means that $\mathrm{Gal}(K_\infty/K)$ has rank 2. The claim now follows from Corollary 8. □

Note that the classification of the 2-rational imaginary quadratic fields in [19] (Corollaire 1.3) is not correct.

1.10 Prime decomposition in ring class fields

One of the central results in class field theory is the law on decomposition of prime ideals in abelian extensions L/K of algebraic number fields. We consider here the case where K is imaginary quadratic and $L/\mathbb{Q}$ is a generalised dihedral extension:

$$\mathrm{Gal}(L/\mathbb{Q}) \cong \mathrm{Gal}(L/K) \rtimes \mathbb{Z}/2.$$

Then L is contained in a ring class field $N(f)$ over K with suitable conductor f due to a theorem of Bruckner (see [5]).

The *ring class group* over K of conductor f is the group $I_K(f)$ of fractional K-ideals prime to f modulo the subgroup $P_K(f)$ generated by the principal ideals (α) with integral $\alpha \equiv a \pmod{f}$ for some $a \in \mathbb{Z}$ prime to f. By class field theory, there is a canonical isomorphism (the *Artin symbol*)

$$I_K(f)/P_K(f) \to \mathrm{Gal}(N(f)/K).$$

To the field L corresponds a subgroup of $\mathrm{Gal}(N(f)/K)$ which again by the Artin symbol corresponds to a subgroup H' of $I_K(f)$. For a prime ideal $\mathfrak{p}$ of K prime to f, we now have the following decomposition law: $\mathfrak{p}$ *splits in L if and only if* $\mathfrak{p} \in H'$ (see [22], Theorem 7.3).

Now consider the group $\mathscr{C}$ of classes of forms of discriminant $d_K f^2$ where d_K is the discriminant of K. There is a canonical isomorphism between the ring class group $I_K(f)/P_K(f)$ and the form class group $\mathscr{C}$ (see [8], Theorem 7.7 and 7.22). Let H be the subgroup of $\mathscr{C}$ corresponding to H' under this isomorphism. Then a prime number p is representable by some form (class) $f \in H$ if and only if p is the norm of an ideal $\mathfrak{p} \in H'$ ([8], Theorem 7.7). There follows:

PROPOSITION 11. *Consider an imaginary quadratic field K with discriminant d_K. Let L be an abelian extension of K contained in K's ring class field $N(f)$ of conductor f. Denote by $\mathscr{C}$ the form class group of discriminant $d_K f^2$. Let H be the subgroup of $\mathscr{C}$ corresponding to L under the canonical isomorphism Gal($N(f)/K$) $\cong \mathscr{C}$. Let p be a prime number dividing neither d_K nor f. Then p splits totally in the generalised dihedral extension $L/\mathbb{Q}$ if and only if p is representable by a form in H.* □

REMARK. Antoniadis [1] gives another criterion for the splitting of primes in ring class fields: For each character ψ on $\mathrm{Gal}(N(f)/K)$ with $\psi^2 \neq 1$, he considers the L-series

$$L(\psi, s) = \sum_{n=1}^{\infty} a_\psi(n) n^{-s}$$

where ψ is viewed as a character on the absolute Galois group of K. This L-series coincides with the Artin L-series

$$L(\mathrm{Ind}_K^{\mathbb{Q}}(\psi), s)$$

coming from a dihedral type Galois representation over $\mathbb{Q}$. Antoniadis then shows that a prime $p \nmid f$ splits in $N(f)$ if and only if the p'th coefficient satifies $a_\psi(p) = 2$

for all ψ (Satz 2). A main result in Antoniadis' article is the explicit determination of all the coefficients $a_\psi(n)$ (page 204) from which Proposition 11 can be deduced.

Chapter 2

On $\mathbb{Z}_p$-embeddability of cyclic p-class fields

2.1 Introduction

Let p be an odd prime and consider an imaginary quadratic number field K. As shown by Iwasawa (Theorem 1), any $\mathbb{Z}_p$-extension of K is unramified outside p. The lower steps of a such extension might well be unramified also at p. In this chapter the following question is investigated: *if the p-class group of K is non-trivial and cyclic, is the p-Hilbert class field of K (or part of it) then embeddable in a $\mathbb{Z}_p$-extension of K?* In doing so, we are led to study the torsion subgroup of the Galois group over K of the maximal abelian p-extension of K which is unramified outside p. First fix some notation:

p :	an odd prime number
ζ :	a primitive p'th root of unity
Δ :	a square-free natural number
K :	the imaginary quadratic number field $\mathbb{Q}(\sqrt{-\Delta})$
$\mathcal{O}$:	the ring of integral elements in K
K_0 :	the p-Hilbert class field of K
K_e :	the p-part of K's ray class field with conductor p^e, $e \geqq 0$
K_∞ :	the union $\bigcup_{e=0}^{\infty} K_e$
T :	the torsion subgroup of $\mathrm{Gal}(K_\infty/K)$
K_{cycl} :	the cyclotomic $\mathbb{Z}_p$-extension of K
K_{anti} :	the anti-cyclotomic $\mathbb{Z}_p$-extension of K
I :	the group of fractional ideals of K prime to p
P :	the group of principal fractional ideals of K prime to p
P_e :	the ray modulo p^e, $e \geq 0$

Note that the ray class field with conductor 1 is exactly the Hilbert class field so that the notation is consistent. We have the tower

$$K \subsetneqq K_0 \subsetneqq K_1 \subsetneqq K_2 \subsetneqq \cdots \subset K_\infty$$

and note that the union K_∞ is the maximal abelian p-extension of K which is unramified outside p. Thus, by Iwasawa's result, any $\mathbb{Z}_p$-extension of K is contained in K_∞. It is well known that K_∞ is the composite of three fields K_{cycl}, K_{anti}, and K^T which are linearly disjoint over K (see chapter 1). The cyclotomic extension K_{cycl} is the unique $\mathbb{Z}_p$-extension of K which is abelian over $\mathbb{Q}$. The anti-cyclotomic extension K_{anti} is the unique $\mathbb{Z}_p$-extension of K which is pro-dihedral over $\mathbb{Q}$. Finally, K^T is a finite extension of K with $\text{Gal}(K^T/K) \cong T$ and dihedral over $\mathbb{Q}$ (but not unique with these properties). As we shall see, we may usually for K^T take K_0 or a subfield of K_0. From the above discussion follows the isomorphism

$$\text{Gal}(K_\infty/K) \cong \mathbb{Z}_p \times \mathbb{Z}_p \times T$$

which will be important in the following. It may also be noted that the composite $K_{\text{anti}}K^T$ is the maximal abelian p-extension of K which is unramified outside p and dihedral over $\mathbb{Q}$, and hence equals the union of all p-ring class fields over K with conductor a power of p.

2.2 Criteria for p-rationality

The concept of p-rationality has an obvious connection to the question of $\mathbb{Z}_p$-embeddability:

Lemma 12. *Let $p > 2$ and assume that the imaginary quadratic field K is p-rational. Then the p-Hilbert class field K_0 of K is cyclic (possibly trivial) and embeddable into an $\mathbb{Z}_p$-extension of K.*

Proof. Since K_0 is dihedral over $\mathbb{Q}$, it is contained in $K_{\text{anti}}K^T$. So if K is p-rational and the torsion T thus trivial, it will follow that K_0 is contained in K_{anti}. □

We remark that the situation is more difficult for $p = 2$. Here a cyclic 2-class field can be $\mathbb{Z}_2$-embeddable even though it is not contained in K_{anti}. We return to this problem in section 4.12.

What we need now are criteria for p-rationality.

Theorem 13. *(a) $\mathbb{Q}(\sqrt{-3})$ is 3-rational. Let $K = \mathbb{Q}(\sqrt{-\Delta})$ with a square-free*

$\Delta \in \mathbb{N}$. *Then K is 3-rational if $\Delta \not\equiv 3 \pmod 9$ and the class number of $\mathbb{Q}(\sqrt{3\Delta})$ is not divisible by 3.*

(b) Assume $p \geq 5$ and let K be as above. Then K is p-rational if it has the same p-class number as $K(\zeta)$ where ζ is a primitive p'th root of unity.

Proof. (a) We use condition (d) of Theorem 9.

$K = \mathbb{Q}(\sqrt{-3})$ contains a primitive third root of unity ζ, and 3 ramifies in K. If K had a non-trivial hyperprimary element $x \in V_S \backslash K^{*3}$ where S is the set of primes dividing 3, then $K(\sqrt[3]{x})/K$ would be an unramified $\mathbb{Z}/3$-extension. Since K has class number 1, this is impossible. Thus K is 3-rational.

Now let $K = \mathbb{Q}(\sqrt{-\Delta})$ with $\Delta \neq 3$. Then K does not contain ζ. We have the biimplication

$$\zeta \in K_{\mathfrak{p}} = \mathbb{Q}_3(\sqrt{-\Delta}) \ \Leftrightarrow \ \Delta \equiv 3 \ (\mathrm{mod}\ 9) \ .$$

Let K_0 be the 3-Hilbert class field of K. By a theorem of Kubota (see [20]), the p-class number of $K(\sqrt{-3})$ is the product of the p-class numbers of K, $\mathbb{Q}(\sqrt{-3})$, and $\mathbb{Q}(\sqrt{3\Delta})$ for an odd prime p. It then follows from the assumption and the fact that $\mathbb{Q}(\sqrt{-3})$ has trivial class number that $K(\sqrt{-3})$ has the same 3-class number as K. Hence $K_0(\sqrt{-3})$ is the 3-Hilbert class field of $K(\sqrt{-3})$. Clearly $K_0(\sqrt{-3})/K$ is abelian. Assume for a contradiction that K has a non-trivial hyperprimary element $x \in V_S \backslash K^{*3}$. Then $K(\sqrt{-3}, \sqrt[3]{x})/K(\sqrt{-3})$ is an unramified $\mathbb{Z}/3$-extension (see Remark 5). Therefore $\sqrt[3]{x}$ is contained in the 3-Hilbert class field $K_0(\sqrt{-3})$. But $K(\sqrt[3]{x})$ is not normal over K, a contradiction. Hence K is 3-rational.

(b) In the case $p \geq 5$ neither K nor $K_{\mathfrak{p}} = \mathbb{Q}_p(\sqrt{-\Delta})$ contain ζ. The same argument as above shows $V_S = K^{*p}$ where S now is the set of primes dividing p. □

Remarks. (a) We shall later see that K is p-rational for $p \geq 5$ when its class number is not divisible by p.

(b) Note that part (b) of Theorem 10 generalises the similar part of [19], Corollaire 1.3.

(c) The proof of Theorem 10 shows that it suffices to assume in part (b) that the p-class groups of K and $K(\zeta)$ have the same ranks. However this seems to happen only when the p-class numbers are also identical.

(d) Theorem 10 never applies when p is an *irregular* prime, i.e. when the class number of $\mathbb{Q}(\zeta)$ is divisible by p.

The below table shows all values of $\Delta < 200$ for which the 3-part h of the class number of $K = \mathbb{Q}(\sqrt{-\Delta})$ is divisible by 3. An asterix means that $\Delta \equiv 3 \pmod 9$. h' is the 3-part of the class number of $\mathbb{Q}(\sqrt{3\Delta})$.

Δ	23	26	29	31	38	53	59	61	83	87	89	106	107
h	3	3	3	3	3	3	3	3	3	3	3	3	3
h'	1	1	1	1	1	1	1	1	1	1	1	1	3

Δ	109	110	118	129^*	139	157	170	174^*	182	186	199
h	3	3	3	3	3	3	3	3	3	3	9
h'	1	1	1	1	1	1	1	1	1	1	1

We see that for $\Delta = 23$, 26, 29, 31, 38 etc., K_0/K is cyclic of degree 3 and $\mathbb{Z}_3$-embeddable. We shall deal with the remaining cases $\Delta = 107, 129, 174$ in the next section.

Below is the equivalent table for $p = 5$. Here H is the 5-part of the class number of $K(\zeta)$ (with ζ a primitive fifth root of unity):

Δ	47	74	79	86	103	119	122	127	131	143	159	166	179	181	194	197
h	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
H	5	5	5	5	5	5	5	25	5	5	5	125	5	5	5	5

We see similarly that the 5-class field K_0/K is cyclic of degree 5 and $\mathbb{Z}_5$-embeddable for $\Delta = 47$, 74, 79 etc. We return to the remaining cases $\Delta = 127$, 166 in the next section.

Finally a table for $p = 7$:

Δ	71	101	134	149	151	173
h	7	7	7	7	7	7
H	7	7	7^3	7^3	7	7

2.3 Algorithm to determine $\mathbb{Z}_p$-embeddability

We shall now see how the cases where Theorem 10 does not apply can be dealt with. Recall that the **ray group** modulo p^e is the subgroup P_e of P generated by the principal ideals (α) with integral $\alpha \equiv 1 \pmod{p^e}$. The **ray class group** modulo p^e is the quotient I/P_e. It is a central result in class field theory that there is an isomorphism, the **Artin symbol**, from the p-part of I/P_e to $\mathrm{Gal}(K_e/K)$. It maps the p-part of P/P_e onto $\mathrm{Gal}(K_e/K_0)$.

Lemma 14. *(I) With notation as above, we have for $p > 3$,*

$$Gal(K_e/K_0) \cong \begin{cases} \mathbb{Z}/p^{e-1} \times \mathbb{Z}/p^{e-1} & \text{if } p \nmid \Delta \ , \\ \mathbb{Z}/p^{e-1} \times \mathbb{Z}/p^{e} & \text{if } p \mid \Delta \ . \end{cases}$$

Taking the inverse limit gives Gal$(K_\infty/K_0) \cong \mathbb{Z}_p \times \mathbb{Z}_p$. *In particular,* $T = 0$ *if* $K_0 = K$.

(II) For $p = 3$, *the above remains valid when* $\Delta \not\equiv 3$ *(mod* 9*). Assume* $\Delta \equiv 3$ *(mod* 9*) and* $\Delta \neq 3$. *Then*

$$\mathit{Gal}(K_e/K_0) \cong \mathbb{Z}/3^{e-1} \times \mathbb{Z}/3^{e-1} \times \mathbb{Z}/3 \ .$$

Taking the inverse limit gives Gal$(K_\infty/K_0) \cong \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}/3$. *In particular,* $T \cong \mathbb{Z}/3$ *if* $K_0 = K$.

Proof. There is a natural exact sequence

$$1 \longrightarrow \mathcal{O}^* \longrightarrow (\mathcal{O}/p^e)^* \longrightarrow P/P_e \longrightarrow 1 \ .$$

The exclusion of the case $p = \Delta = 3$ ensures that $\mathcal{O}^*$ has trivial p-part. Hence $\mathrm{Gal}(K_e/K_0)$ is isomorphic to the p-part of $(\mathcal{O}/p^e)^*$ by the Artin symbol. So we compute the structure of $(\mathcal{O}/p^e)^*$.

To begin with, note that each coset of $\mathcal{O}/p^e$ has a unique representative of the form $a + b\sqrt{-\Delta}$ with $a, b = 0, 1, \ldots, p^e - 1$.

The order of $(\mathcal{O}/p^e)^*$, i.e. the norm of the ideal $p^e\mathcal{O}$, depends on the prime ideal decomposition of p in K. More precisely, the order of the p-part is

$$|p\text{-part of } (\mathcal{O}/p^e)^*| = \begin{cases} p^{2e-2} & \text{if } p \nmid \Delta \ , \\ p^{2e-1} & \text{if } p \mid \Delta \ . \end{cases}$$

We note the following two facts:

(∗) Let $x \in \mathcal{O}$ and write $(1 + x)^p = 1 + x'$. If $p^i || x$ for some $i \geqq 1$ (meaning that $p^i | x$, but $p^{i+1} \nmid x$), then $p^{i+1} || x'$.

(∗∗) Let a and b be integers with $a \equiv 1 \pmod p$ and $p^i || b$ for some $i \geqq 1$. Write $(a + b\sqrt{-\Delta})^p = a' + b'\sqrt{-\Delta}$. Then $a' \equiv 1 \pmod p$ and $p^{i+1} || b'$.

It follows from (∗) that the cyclic subgroups $U := \langle 1 + p \rangle$ and $V := \langle 1 + p\sqrt{-\Delta} \rangle$ of $(\mathcal{O}/p^e)^*$ both have order p^{e-1}. It follows from (∗∗) that they have trivial intersection. So for $p \nmid \Delta$,

$$(p\text{-part of } (\mathcal{O}/p^e)^*) = U \times V \cong \mathbb{Z}/p^{e-1} \times \mathbb{Z}/p^{e-1} \ .$$

Assume $p \mid \Delta$. Then $U \times V$ has index p in the p-part of $(\mathcal{O}/p^e)^*$. If $p > 3$, or $p = 3$ and $\Delta \not\equiv 3 \pmod 9$, the same argument shows

$$(p\text{-part of } (\mathcal{O}/p^e)^*) = U \times V' \cong \mathbb{Z}/p^{e-1} \times \mathbb{Z}/p^e$$

for $V' := \langle 1+\sqrt{-\Delta}\rangle$. In case $p=3$ and $\Delta \equiv 3 \pmod 9$, the 3-part of $(\mathcal{O}/9)^*$ is $\langle 4\rangle \times \langle 1+3\sqrt{-\Delta}\rangle \times \langle 1+\sqrt{-\Delta}\rangle \cong (\mathbb{Z}/3)^3$, and therefore

$$(\text{3-part of } (\mathcal{O}/3^e)^*) = U \times V \times (\text{group of order 3}) \cong \mathbb{Z}/p^{e-1} \times \mathbb{Z}/p^{e-1} \times \mathbb{Z}/3\ .$$

This finishes the proof of the lemma. □

The question of $\mathbb{Z}_p$-embeddability in the case where the p-class field is cyclic of degree p can now be answered.

THEOREM 15. *Assume K_0/K is cyclic of degree p. Pick a prime $\mathfrak{q} \nmid p$ of K of order p in the class group, and write $\mathfrak{q}^p = (\alpha)$ with $\alpha \in \mathcal{O}$.*

I. Suppose $p > 3$.

- *(a) If α is not a p'th power in $(\mathcal{O}/p^2)^*$, then K_0/K is $\mathbb{Z}_p$-embeddable (in fact K_0 is contained in K_{anti}), and $T = 0$.*
- *(b) If α is a p'th power in $(\mathcal{O}/p^2)^*$, then K_0/K is not embeddable in $\mathbb{Z}/p^2$-extension unramified outside p, and $T \cong \mathbb{Z}/p$.*

II. Now suppose $p = 3$. If $\Delta \not\equiv 3 \pmod 9$, all the above remains valid. Assume $\Delta \equiv 3 \pmod 9$, and write $\alpha \equiv a + b\sqrt{-\Delta} \pmod 9$ with $a, b \in \mathbb{Z}$.

- *(c) If $(a,b) \equiv (\pm 1, 0)$ modulo 3, but not modulo 9, then K_0/K is $\mathbb{Z}_3$-embeddable (in fact K_0 is contained in K_{anti}), and $T \cong \mathbb{Z}/3$.*
- *(d) If $(a,b) \not\equiv (\pm 1, 0)$ modulo 3, then K_0/K is embeddable in a $\mathbb{Z}/9$-extension unramified outside 3, but not in a $\mathbb{Z}/27$-extension unramified outside 3, and $T \cong \mathbb{Z}/9$.*
- *(e) If $(a,b) \equiv (\pm 1, 0)$ modulo 9, then K_0/K is not embeddable in a $\mathbb{Z}/9$-extension unramified outside 3, and $T \cong \mathbb{Z}/3 \times \mathbb{Z}/3$.*

Proof. I. Assume $p > 3$. By Lemma 14, $\mathrm{Gal}(K_\infty/K_0) \cong \mathbb{Z}_p \times \mathbb{Z}_p$. Since $\mathrm{Gal}(K_0/K) \cong \mathbb{Z}/p$, there are two possibilities for T: 0 or $\mathbb{Z}/p$.

(a) If $T = 0$, i.e. $\mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p \times \mathbb{Z}_p$, then K_0 is contained in $K_{\text{cycl}}K_{\text{anti}}$. Since K_0 is dihedral over $\mathbb{Q}$, it is in fact contained in K_{anti}. Both I/P_2 and P/P_2 have p-rank 2. Therefore, $\mathfrak{q}^p = (\alpha)$ is *not* a p'th power in P/P_2. So α is not a p'th power in $(\mathcal{O}/p^2\mathcal{O})^*$.

(b) If $T \cong \mathbb{Z}/p$, i.e. $\mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}/p$, then K_0 is linearly disjoint from $K_{\text{cycl}}K_{\text{anti}}$. So we may for K^T take K_0. Hence no $\mathbb{Z}/p^2$-extension of K inside K_∞ contains K_0. Now the p-part of P/P_2 is a direct summand in the p-part of I/P_2. Therefore, $\mathfrak{q}^p = (\alpha)$ *is* a p'th power in P/P_2. So α is a p'th power in $(\mathcal{O}/p^2\mathcal{O})^*$.

II. Now assume $p = 3$. If $\Delta \not\equiv 3 \pmod 9$, everything goes like above. Henceforth assume $\Delta \equiv 3 \pmod 9$. Then $(\mathcal{O}/9)^* \cong \mathbb{Z}/2 \times \mathbb{Z}/3 \times \mathbb{Z}/3 \times \mathbb{Z}/3$ (see the proof of Lemma 14), so that $\alpha = a + b\sqrt{-\Delta}$ is a cube in $(\mathcal{O}/9)^*$ iff $(a, b) \equiv (\pm 1, 0)$ modulo 9. Further, $(\mathcal{O}/3)^* \cong \mathbb{Z}/2 \times \mathbb{Z}/3$, so that α is a cube in $(\mathcal{O}/3)^*$ iff $(a, b) \equiv (\pm 1, 0)$ modulo 3. By Lemma 14, $\mathrm{Gal}(K_\infty/K_0) \cong \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}/3$. Since $\mathrm{Gal}(K_0/K) \cong \mathbb{Z}/3$, there are three possibilities for T: $\mathbb{Z}/3$, $\mathbb{Z}/9$, or $\mathbb{Z}/3 \times \mathbb{Z}/3$.

(c) If $T \cong \mathbb{Z}/3$, i.e. $\mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}/3$, then K_0 is contained in $K_{\mathrm{cycl}}K_{\mathrm{anti}}$ and therefore also in K_{anti}. Both I/P_2 and P/P_2 have 3-rank 3. Therefore, $\mathfrak{q}^3 = (\alpha)$ is *not* a cube in P/P_2. So α is not a cube in $(\mathcal{O}/9)^*$. On the other hand, the 3-part of P/P_1 is a direct summand in the 3-part of I/P_1. Therefore, $\mathfrak{q}^3 = (\alpha)$ *is* a cube in P/P_1. So α is a cube in $(\mathcal{O}/3)^*$. This shows the claims about a and b.

The cases (d) where $T \cong \mathbb{Z}/9$ and (e) where $T \cong \mathbb{Z}/3 \times \mathbb{Z}/3$ are treated in a similar manner, so their proofs are omitted. □

The same arguments give a description of the torsion subgroup T in the general case where K_0/K is not necessarily cyclic: If $p > 3$, or $p = 3$ and $\Delta \not\equiv 3 \pmod 9$, then $K_\infty = K_{\mathrm{cycl}}K_{\mathrm{anti}}K_0$, and therefore $T \cong \mathrm{Gal}(K_0/K_0 \cap K_{\mathrm{anti}})$, i.e. T is isomorphic to a subgroup of $\mathrm{Gal}(K_0/K)$ with cyclic quotient. If $p = 3$ and $\Delta \equiv 3 \pmod 9$, then K_∞ has degree 3 over $K_{\mathrm{cycl}}K_{\mathrm{anti}}K_0$, and therefore T has a subgroup of index 3 which is isomorphic to $\mathrm{Gal}(K_0/K_0 \cap K_{\mathrm{anti}})$.

The following examples answer the questions regarding $\mathbb{Z}_p$-embeddability from the previous section and show that all cases of Theorem 15 occur.

Examples. (i) Let $p = 5$ and $\Delta = 127$. The class number of K is 5. The prime number 2 is divisible by a non-principal prime ideal $\mathfrak{q}$ of K. Further, $\mathfrak{q}^5 = (\alpha)$ with $\alpha = (1 + \sqrt{-127})/2$ since $2^5 = \alpha\bar{\alpha}$. Since α is not a fifth power in $(\mathcal{O}/25)^*$, we are in case (a).

(ii) Let $p = 5$ and $\Delta = 166$. The class number of K is 10. Here 7 is divisible by a non-principal prime ideal $\mathfrak{q}$ such that $\mathfrak{q}^5 = (\alpha)$ is principal, $\alpha = (129 + \sqrt{-166})/2$. Modulo 25 we have $\alpha \equiv \alpha^5$ and conclude that we are in case (b).

(iii) Let $p = 3$ and $\Delta = 107$. The class number of K is 3. Here 11 is divisible by a non-principal prime ideal $\mathfrak{q}$ such that $\mathfrak{q}^3 = (\alpha)$ is principal, $\alpha = (9+7\sqrt{-107})/2$. Modulo 9 we have $\alpha \equiv \alpha^3$ and conclude that we are in case (b).

(iv) Let $p = 3$ and $\Delta = 237$. The class number of K is 12. Here 13 is divisible by a non-principal prime ideal $\mathfrak{q}$ such that $\mathfrak{q}^3 = (\alpha)$ is principal, $\alpha = 8+3\sqrt{-237}$. We are in case (c).

(v) Let $p = 3$ and $\Delta = 129$. The class number of K is 12. Here 13 is divisible by a non-principal prime ideal $\mathfrak{q}$ such that $\mathfrak{q}^3 = (\alpha)$ is principal, $\alpha = 41+2\sqrt{-129}$.

We are in case (d).

(vi) Let $p = 3$ and $\Delta = 3387$. The class number of K is 12. Here the prime 43 is divisible by a non-principal prime ideal $\mathfrak{q}$ such that $\mathfrak{q}^3 = (\alpha)$ is principal, $\alpha = (209 + 9\sqrt{-3387})/2 \equiv 1 \pmod{9}$. We are in case (e).

As is the case for the ideal class group, there is numerical evidence that the torsion subgroup T "prefers" having small rank, so that case (e) occurs quite rarely. More precisely, there are 260 values of $\Delta < 10,000$ with $\Delta \equiv 3 \pmod{9}$ such that the class number of K is divisible by 3, and for these values, case (c) occurs 55 times, case (d) occurs 199 times, whereas case (e) occurs only 6 times.

Finally a criterion for $\mathbb{Z}_p$-embeddability of a cyclic p-class field (or part of it) of arbitrary degree is given.

THEOREM 16. *Assume K_0/K is cyclic of degree $p^n > 1$, and let F/K be some subextension*

(I) Suppose $p > 3$. Then F/K is $\mathbb{Z}_p$-embeddable if it is embeddable in a $\mathbb{Z}/p^{n+1}$-extension unramified outside p.

(II) Suppose $p = 3$. If $\Delta \not\equiv 3 \pmod{9}$, the above holds. Assume $\Delta \equiv 3 \pmod{9}$. Then F/K is $\mathbb{Z}_3$-embeddable if it is embeddable in a $\mathbb{Z}/3^{n+2}$-extension unramified outside 3.

Proof. Only (I) is proved since the proof of (II) is very similar. Put $F' := K_0 \cap K_{\mathrm{cycl}}K_{\mathrm{anti}} = K_0 \cap K_{\mathrm{anti}}$, and let p^i be the degree of F'/K. It is the maximal $\mathbb{Z}_p$-embeddable subextension of K_0/K. Then $T \cong \mathbb{Z}/p^{n-i}$. Assume F/K is not $\mathbb{Z}_p$-embeddable, i.e. that F is a proper extension of F'. Assume that F/K is embedded in a cyclic extension L/K inside K_∞. Then $F' = L \cap K_{\mathrm{cycl}}K_{\mathrm{anti}}$. Therefore $[L : F'] = [K_{\mathrm{cycl}}K_{\mathrm{anti}}L : K_{\mathrm{cycl}}K_{\mathrm{anti}}] \leqq p^{n-i}$ and we conclude that $[L : K] \leqq p^n$. □

Chapter 3

Prime decomposition in the anti-cyclotomic extension

3.1 Introduction

Let l be an odd prime number, and denote by $\mathbb{Z}_l$ the infinite pro-cyclic l-group $\varprojlim \mathbb{Z}/l^n$. Consider an imaginary quadratic number field K. As is well known, K has a unique $\mathbb{Z}_l$-extension which is pro-dihedral over $\mathbb{Q}$. We call it the *anti-cyclotomic* $\mathbb{Z}_l$-extension of K (for reasons later to be clear).

The purpose of this chapter is to study the decomposition of primes $\mathfrak{p}$ of K in the anti-cyclotomic extension. Since this extension is pro-cyclic, the decomposition type of $\mathfrak{p}$ is completely determined by the number of *steps* of the anti-cyclotomic extension in which $\mathfrak{p}$ is unramified, and the number of steps in which $\mathfrak{p}$ splits totally. By the *n'th step* of a $\mathbb{Z}_l$-extension we understand the subextension of degree l^n over the ground field.

Such decomposition laws are given in section 3.3 (Theorem 22 and Theorem 24). The laws involve representations of primes p or prime powers p^h by certain quadratic forms of the same discriminant d_K as K. Using Gauss' theory of composition of forms, it always suffices to represent p by some form. The whole story becomes particularly simple when each genus of forms of discriminant d_K consists of a single class. This happens for 65 values of d_K closely connected to Euler's *numeri idonei* or *convenient numbers.*

As we shall see, the decomposition laws also depend on how many steps of the anti-cyclotomic extension are unramified. This dependence may be turned around, meaning that if we know how certain primes decompose, then we can compute the number of unramified steps. In particular, we can answer whether the Hilbert class field of K is contained in the anti-cyclotomic extension and thus is $\mathbb{Z}_l$-embeddable.

In section 3.5 we show how to find explicit polynomials whose roots generate the first step of the anti-cyclotomic extension. When K is not l-rational (to be defined in section 3.2), this involves using the decomposition laws to identify the right polynomial f among a finite number of candidates. When this is done, one obtains nice laws for the splitting of f modulo p. For instance we show that $X^5 + 5X^2 + 3$ splits into linear factor modulo a prime number $p \neq 3, 5$ if and only if p is of the form $x^2 + 5xy + 100y^2$ (for example $p = 379, 439, 571, 631$) or $3x^2 + 15xy + 50y^2$ (for example $p = 137, 173, 233, 317$).

Throughout the article we use the following notation:

l :	an odd prime number
Δ :	a square-free natural number
K :	the imaginary quadratic number field $\mathbb{Q}(\sqrt{-\Delta})$
d_K :	the discriminant of K
h, μ, u :	we write the class number of K as $h = l^\mu u$ with $l \nmid u$
$\mathcal{O}$:	the ring of integral elements in K
$\mathfrak{p}$:	a prime of K, i.e. a prime ideal in $\mathcal{O}$
p :	the rational prime divisible by $\mathfrak{p}$
K_H :	the Hilbert class field of K
$K_{\max}$:	the maximal abelian extension of K unramified outside l
$K_{\text{anti}}^{(n)}$:	the n'th step of the anti-cyclotomic extension K_{anti}
ν :	the non-negative integer defined by $K_{\text{anti}} \cap K_H = K_{\text{anti}}^{(\nu)}$
$(\cdot/\cdot)$:	the Legendre or Kronecker symbol

3.2 The cyclotomic and the anti-cyclotomic extension

In Iwasawa [18] it is shown that any $\mathbb{Z}_l$-extension of K is unramified outside l. This result motivates the study of the maximal abelian extension $K_{\max}$ of K which is unramified outside l. If K^f denotes the ray class field over K of conductor f, then $K_{\max}$ is the union of the tower

$$K \subseteq K^1 \subseteq K^l \subseteq K^{l^2} \subseteq \ldots$$

Here, K^1 is the Hilbert class field of K which we also denote K_H.

Let τ denote complex conjugation. Clearly, $K_{\max}$ is normal over $\mathbb{Q}$, so τ operates on $\text{Gal}(K_{\max}/K)$ by conjugation.

Main Lemma 17. *We may write Gal$(K_{\max}/K) = U \times W \times T \times T'$ such that*

(i) *U is isomorphic to $\mathbb{Z}_l$, and τ operates trivially on U,*
(ii) *W is isomorphic to $\mathbb{Z}_l$, and τ operates by inversion on W,*
(iii) *T is a finite l-group, and τ operates by inversion on T,*
(iv) *T' is finite of order prime to l.*

Further, we may write Gal$(K_{\max}/K_H) = U \times V \times T^* \times S'$ where

(v) *V is isomorphic to $\mathbb{Z}_l$, contained in $W \times T$, and has $|V : W \cap V| \leq |T|$,*
(vi) *T^* is trivial unless $l = 3$, $\Delta \equiv 3$ (mod 9), and $\Delta \neq 3$; in this* exceptional case, *T^* has order 3 and is contained in T,*
(vii) *S' is contained in T' (and thus finite of order prime to l).*

Consider a conductor $\mathfrak{m} = l^e$ with $e \geq 1$. Then Gal$(K_{\max}/K^{\mathfrak{m}}) = U^{\mathfrak{m}} \times V^{\mathfrak{m}}$ where

(iix) *$U^{\mathfrak{m}}$ is contained in U and has index $|U : U^{\mathfrak{m}}| = l^{e-1}$,*
(ix) *$V^{\mathfrak{m}}$ is contained in V. If $l \nmid \Delta$, then $|V : V^{\mathfrak{m}}| = l^{e-1}$. If $l \mid \Delta$, then $|V : V^{\mathfrak{m}}| = l^e$ unless $l = 3$ and $\Delta \equiv 3$ (mod 9); in this case, $|V : V^{\mathfrak{m}}| = 3^{e-1}$.*

The subgroups U, $W \times T$, T, T', V, T^*, S', $U^{\mathfrak{m}}$, and $V^{\mathfrak{m}}$ are unique with these properties.

A proof will be given at the end of the section. At this point, we only note that the uniqueness statement is seen as follows: U is the maximal subgroup of the l-part of Gal$(K_{\max}/K)$ on which τ operates trivially, $W \times T$ is the maximal subgroup of the l-part of Gal$(K_{\max}/K)$ on which τ operates by inversion, T is the l-torsion and T' is the non-l-part[1] (and the non-l-torsion) of Gal$(K_{\max}/K)$, V equals Gal$(K_{\max}/K_K) \cap (W \times T)$, T^* is the l-torsion, and S' is the non-l-part of Gal$(K_{\max}/K_H)$. Note that W is not unique if T is non-trivial.

Proposition 18. *(a) K has a unique $\mathbb{Z}_l$-extension which is pro-cyclic over $\mathbb{Q}$. It is called the* **cyclotomic** *extension and is denoted K_{cycl}. Adjoin to $\mathbb{Q}$ all roots of unity of l-power-order, and let $\mathbb{Q}_{\text{cycl}}$ be the l-part of this extension. Then K_{cycl} is the composite of K and $\mathbb{Q}_{\text{cycl}}$.*

(b) K has a unique $\mathbb{Z}_l$-extension which is pro-dihedral over $\mathbb{Q}$. It is called the **anti-cyclotomic** *extension and is denoted K_{anti}.*

(c) K_{cycl} and K_{anti} are the only absolutely normal $\mathbb{Z}_l$-extensions of K. They are linearly disjoint over K, and any $\mathbb{Z}_l$-extension of K is contained in the composite $K_{\text{cycl}}K_{\text{anti}}$. The l-part of the Hilbert class field K_H (or any other part of it) is embeddable in a $\mathbb{Z}_l$-extension of K iff it is contained in K_{anti}.

(d) The Galois group of the maximal abelian l-extension of K which is un-

[1] The l-part of an abelian pro-finite group is its Sylow-l-subgroup, the "non-l-part" is the product of the l'-parts for $l' \neq l$. The l-part of an abelian field extension is the fixed field of the non-l-part of the Galois group, and vice versa.

ramified outside l is isomorphic to $\mathbb{Z}_l \times \mathbb{Z}_l \times T$ where T is a finite l-group. If T is trivial, the l-part of K_H is cyclic and $\mathbb{Z}_l$-embeddable.

Proof. Everything follows from the theorem: K_{cycl} is the fixed field of $W \times T \times T'$, and K_{anti} is the fixed field of $U \times T \times T'$. Any $\mathbb{Z}_l$-extension of K is contained in the fixed field of the torsion $T \times T'$, i.e. in $K_{\mathrm{cycl}}K_{\mathrm{anti}}$. K_{cycl} and K_{anti} are the only absolutely normal $\mathbb{Z}_l$-extensions of K since U and W are the only τ-invariant subgroups of $U \times W$ with quotient $\mathbb{Z}_l$. Since K_H is generalised dihedral over $\mathbb{Q}$, the maximal $\mathbb{Z}_l$-embeddable subfield of it is $K_H \cap K_{\mathrm{anti}}$. If T is trivial, the l-part of K_H is contained in K_{anti}. It is clear that $\mathbb{Q}_{\mathrm{cycl}}$ is a $\mathbb{Z}_l$-extension of $\mathbb{Q}$. Hence $K\mathbb{Q}_{\mathrm{cycl}}$ is a $\mathbb{Z}_l$-extension of K and a $(\mathbb{Z}_l \times \mathbb{Z}/2)$-extension of $\mathbb{Q}$. The uniqueness of K_{cycl} implies $K_{\mathrm{cycl}} = K\mathbb{Q}_{\mathrm{cycl}}$. □

The situation is particularly simple when the torsion T is trivial. If this is the case, K is called **l-rational**. This notion was introduced in [19]. Some criteria for l-rationality are given there and in [3].

LEMMA 19. *(a) Let X be an infinite abelian pro-l-group, and assume V and T^* are subgroups of X of which V is pro-cyclic with finite index, and T^* is finite. Then we may write $X = W \times T$ with W pro-cyclic, T finite containing T^*, and $|V : V \cap W| \leq |T|$.*

(b) Let X be an abelian pro-l-group with a subgroup V. Assume τ is an automorphism of order 2 on X that operates by inversion both on V and on X/V. Then τ operates by inversion on X.

(c) Let X be an abelian pro-l-group with a subgroup U. Assume τ is an automorphism on X that operates trivially on U and by inversion on X/U. Then $X = U \times V$ where $V = \{x \in X \mid x^\tau = x^{-1}\}$.

Proof. (a) Assume $V \times T^*$ to have index l in X; the general case will then follow by induction. Pick an $x \in X \backslash (V \times T^*)$ and write $x^l = vt$ with $v \in V$ and $t \in T^*$. If v is an l'th power in V, then $X = V \times T$ with a T containing T^*. If v^l is not an l'th power in V, then $X = W \times T^*$ where W is the pro-cyclic group generated by x; from $x^{l \cdot |T^*|} = v^{|T^*|}$ follows $|V : W \cap V| \leq |T^*|$.

(b) Let $x \in X$. Then $x^\tau = x^{-1}v$ for some $v \in V$. Hence $x = x^{\tau\tau} = x^{-\tau}v^\tau = xv^{-2}$ and therefore $v^2 = e$, $v = e$ (since X has no elements of order 2), and $x^\tau = x^{-1}$.

(c) Let $x \in X$. Then $x^\tau = x^{-1}u$ for a $u \in U$. Every element in X is a square, so there is a $u_0 \in U$ with $u_0^2 = u^{-1}$. Put $v = xu_0$. Then $v^\tau = x^\tau u_0 = x^{-1}uu_0 = v^{-1}$, i.e. $v \in V$. Hence $x = u_0^{-1}v \in U \times V$. □

LEMMA 20. *Let $e \geq 1$. The group of units in the ring $\mathcal{O}/l^e$ may be written $(\mathcal{O}/l^e)^* = U \times V \times S'$ such that the following hold:*

(a) Complex conjugation τ operates trivially on U which is isomorphic to $\mathbb{Z}/l^{e-1}$.

(b) Complex conjugation τ operates by inversion on V, and

$$V \cong \begin{cases} \mathbb{Z}/l^{e-1} & \text{if } l \nmid \Delta, \\ \mathbb{Z}/l^{e} & \text{if } l \mid \Delta, \text{ unless } l = 3 \text{ and } \Delta \equiv 3 \ (\text{mod } 9), \\ \mathbb{Z}/3^{e-1} \times \mathbb{Z}/3 & \text{if } l = 3 \text{ and } \Delta \equiv 3 \ (\text{mod } 9). \end{cases}$$

(c) S' is the non-l-part of $(\mathcal{O}/l^e)^*$ and has order

$$|S'| = \begin{cases} (l-1)^2 & \text{if } (-\Delta/l) = 1, \\ l^2 - 1 & \text{if } (-\Delta/l) = -1, \\ l - 1 & \text{if } (-\Delta/l) = 0. \end{cases}$$

There is a subgroup S'' of S' of order $l-1$ such that $(\mathbb{Z}/l^e)^* = U \times S''$.

Proof. To begin with, note that each coset of $\mathcal{O}/l^e$ has a unique representative of the form $a + b\sqrt{-\Delta}$ with $a, b \in \{0, 1, \dots, l^e - 1\}$.

The order of $(\mathcal{O}/l^e)^*$ depends on the decomposition of l in K as follows:

$$|(\mathcal{O}/l^e)^*| = \begin{cases} (l-1)^2 l^{2e-2} & \text{if } l \text{ splits,} \\ (l^2-1) l^{2e-2} & \text{if } l \text{ is inert,} \\ (l-1) l^{2e-1} & \text{if } l \text{ ramifies.} \end{cases}$$

This gives the order of S'.

The subgroups $U := \langle 1+l \rangle$ and $V' := \langle 1+l\sqrt{-\Delta} \rangle$ of $(\mathcal{O}/l^e)^*$ are both $\cong \mathbb{Z}/l^{e-1}$ and have trivial intersection. Clearly, τ operates trivially on U and by inversion on $(U \times V')/U$. So by Lemma 20 (c), $U \times V' = U \times V$ for a group $V \cong \mathbb{Z}/l^{e-1}$ on which τ operates by inversion. This shows (a) and (b) when $l \nmid \Delta$.

When $l \mid \Delta$ the same arguments work for $V' := \langle 1 + \sqrt{-\Delta} \rangle$ unless $l = 3$ and $\Delta \equiv 3$ (mod 9). In the *exceptional case* $l = 3$ and $\Delta \equiv 3$ (mod 9), however, the 3-part of $(\mathcal{O}/9)^*$ is $\langle 1+3 \rangle \times \langle 1 + 3\sqrt{-\Delta} \rangle \times \langle 1 + \sqrt{-\Delta} \rangle \cong (\mathbb{Z}/3)^3$, showing $V \cong \mathbb{Z}/3^{e-1} \times \mathbb{Z}/3$. This finishes the proof of (b).

To see the last part of (c), note $U = \{u \in (\mathbb{Z}/l^e)^* \mid u \equiv 1 \ (\text{mod } l^e)\}$. □

Proof of Main Lemma. Consider conductors $\mathfrak{m} = l^e$ with $e \geq 1$. Let $J_K^{\mathfrak{m}}$ be the group of fractional ideals prime to $\mathfrak{m}$ (i.e. prime to l) and let $P_K^{\mathfrak{m}}$ be the subgroup generated by the principal ideals (α) with integral $\alpha \equiv 1 \pmod{\mathfrak{m}}$. By class field theory, the *Artin symbol* is a surjective homomorphism

$$\left(\frac{K^{\mathfrak{m}}/K}{\quad}\right) : J_K^{\mathfrak{m}} \to \mathrm{Gal}(K^{\mathfrak{m}}/K)$$

with kernel $P_K^{\mathfrak{m}}$. It maps the group P_K of principal ideals prime to l onto $\mathrm{Gal}(K^{\mathfrak{m}}/K_H)$ and behaves nicely when e varies. Moreover, the Artin symbol satifies

$$\left(\frac{K^{\mathfrak{m}}/K}{\tau(\mathfrak{p})}\right) = \tau \left(\frac{K^{\mathfrak{m}}/K}{\mathfrak{p}}\right) \tau \ .$$

Assume for simplicity $\Delta \neq 1, 3$. We then have the natural exact sequence

$$1 \to \{\pm 1\} \to (\mathcal{O}/l^e)^* \to P_K/P_K^{\mathfrak{m}} \to 1$$

where an $\alpha \in (\mathcal{O}/l^e)^*$ is sent to the principal ideal (α). The Artin symbol thus induces an isomorphism

$$\varprojlim \, (\mathcal{O}/l^e)^*/\{\pm 1\} \xrightarrow{\cong} \mathrm{Gal}(K_{\max}/K_H) \ .$$

Conclude from Lemma 20 that $\mathrm{Gal}(K_{\max}/K_H) = U \times V \times T^* \times S'$ with U, V, and T^* as in the theorem, and S' finite of order

$$|S'| = \begin{cases} (l-1)^2/2 & \text{if } (-\Delta/l) = 1, \\ (l^2-1)/2 & \text{if } (-\Delta/l) = -1, \\ (l-1)/2 & \text{if } (-\Delta/l) = 0. \end{cases}$$

From Lemma 20 also follows $\mathrm{Gal}(K_{\max}/K^{\mathfrak{m}}) = U^{\mathfrak{m}} \times V^{\mathfrak{m}}$ with $U^{\mathfrak{m}}$ and $V^{\mathfrak{m}}$ as in the theorem.

The rest is group theory: Write $\mathrm{Gal}(K_{\max}/K) = X \times T'$ with l-part X and non-l-part T'. Then X contains $U \times V \times T^*$, and T' contains S' with index $|T' : S'| = u$. It is well known that K_H is a generalised dihedral extension of $\mathbb{Q}$, so that τ operates by inversion on $X/(U \times V \times T^*)$. It follows from Lemma 19 (b) that τ operates by inversion on X/U. By Lemma 19 (c), $X = U \times Y$ where $Y = \{x \in X \mid x^\tau = x^{-1}\}$. Clearly, Y contains $V \times T^*$ with finite index $|Y : V \times T^*| = l^\mu$. By Lemma 19 (a), $Y = W \times T$ with $W \cong \mathbb{Z}_l$, T finite containing T^*, and $|V : W \cap V| \leq |V|$.

In the case $\Delta = l = 3$, the occurence of a factor of order 3 in $\mathcal{O}^*$ causes T^* to vanish. So in this situation, we are *not* in the “exceptional case”. □

3.3 Prime decomposition laws

Consider a prime ideal $\mathfrak{p}$ of K, and let p the rational prime it divides. Our main objective is to give a law for the decomposition or factorisation of $\mathfrak{p}$ in K_{anti}. For the sake of completeness, we start with the cyclotomic extension in which the law has the simplest form possible.

PROPOSITION 21. *If $p = l$, then $\mathfrak{p}$ is totally ramified in K_{cycl}. If $p \neq l$, then $\mathfrak{p}$ is unramified in K_{cycl}, and $\mathfrak{p}$ splits totally in the n'th step of K_{cycl} iff $p \equiv \pm 1 \pmod{l^{n+1}}$.*

Proof. This is an immediate consequence of Proposition 1 (a) and the law on decomposition of prime numbers in cyclotomic fields. □

Now we turn to the anti-cyclotomic extension. Recall that K_{anti}/K is unramified outside l by Iwasawa's result. Define $\nu \geq 0$ such that $K_{\text{anti}} \cap K_H = K_{\text{anti}}^{(\nu)}$. Then any prime $\mathfrak{P}$ of $K_{\text{anti}}^{(\nu)}$ dividing l ramifies totally in K_{anti}.

Class field theory gives that $\mathfrak{p}$ splits totally in any ring class field $N^{\mathfrak{m}}$ of conductor $\mathfrak{m}$ prime to l if p is inert in $K/\mathbb{Q}$, and that $\mathfrak{p}$ splits totally in a subfield of $N^{\mathfrak{m}}$ over which $N^{\mathfrak{m}}$ has degree 2 if p ramifies in $K/\mathbb{Q}$. In particular, $\mathfrak{p}$ splits totally in K_{anti} if p is different from l and non-split in K. So the remaining problem is the case where $p \neq l$ splits in K. We treat first the easier situation where K is l-rational (as defined in section 3.2).

THEOREM 22. *Assume K is l-rational, and consider a prime $p \nmid d_K l$ and an integer $n \geq 0$. Write the class number of K as $h = l^{\mu} u$ with $l \nmid u$. For $n \leq \mu$, p splits in $K_{\text{anti}}^{(n)}$ iff p is representable by a quadratic form of discriminant d_K whose order in the form class group is not divisible by $l^{\mu-n+1}$. For $n > \mu$, p splits in $K_{\text{anti}}^{(n)}$ iff p is representable by a quadratic form of discriminant*

$$\begin{cases} d_K \cdot l^{2(n-\mu+1)} & \textit{if } l \nmid \Delta \textit{ or } \Delta = l = 3 \\ d_K \cdot l^{2(n-\mu)} & \textit{otherwise} \end{cases}$$

whose order in the form class group is prime to l.

Proof. First some general observations (see also section 1.10). Consider a ring class field $N^{\mathfrak{m}}$ of K with arbitrary conductor $\mathfrak{m}$. The Galois group $\text{Gal}(N^{\mathfrak{m}}/K)$ is isomorphic to the ring class group of conductor $\mathfrak{m}$ via the Artin isomorphism. This ring class group is again isomorphic to the form class group $\mathscr{C}$ of discriminant $-d_K f^2$. Now let L be any field with $K \subsetneqq L \subsetneqq N^{\mathfrak{m}}$. By the main theorem of Galois theory and the above isomorphisms, there corresponds to L some subgroup H of $\mathscr{C}$. For a prime number p dividing neither d_K nor f, class field theory gives that

p splits totally in L iff p is representable by a quadratic form f whose equivalence class $[f]$ belongs to H.

Assume $n \leq \mu$ and let N be the ring class field of K with conductor $f = 1$ (which equals the Hilbert class field). The l-part of N/K is $K_{\text{anti}}^{(\mu)}$ since K is l-rational. The subgroup H of the form class group $\mathscr{C}$ of discriminant d_K corresponding to $L := K_{\text{anti}}^{(n)}$ consists of the classes of forms of order not divisible by $l^{\mu-n+1}$. This proves the first claim.

Now assume $n > \mu$. We only prove the case $l \nmid \Delta$. Let N be the ring class field of K with conductor $f = l^{n-\mu+1}$. By the Main Lemma, the l-part of N/K is $K_{\text{anti}}^{(n)}$ since K is l-rational. The subgroup H of the form class group $\mathscr{C}$ of discriminant $d_K f^2$ corresponding to $L := K_{\text{anti}}^{(n)}$ consists of the classes of forms of order prime to l. This proves the second claim. □

Antoniadis [1] gives a prime decomposition law for ring class fields and their subfields involving coefficients of L-series.

Example 23. (a) Let $l = 3$ and $\Delta = 3$. We seek the primes $p \neq 3$ that split in $K_{\text{anti}}^{(1)}$. The form class group of discriminant $-3 \cdot 3^4 = -243$ has order 3. So p splits iff it is representable by the principal form $x^2 + xy + 61y^2$.

(b) Let $l = 7$ and $\Delta = 1$. The form class group of discriminant $-4 \cdot 7^4 = -9604$ is cyclic of order 28. So a prime $p \neq 2, 7$ splits in $K_{\text{anti}}^{(1)}$ iff it is representable by either the principal form $x^2 + 2401y^2$, or the form $2x^2 + 2xy + 1201y^2$ of order 2, or the form $41x^2 + 20xy + 61y^2$ of order 4 (the other form of order 4 is $41x^2 - 20xy + 61y^2$ which represents the same numbers).

When K is not l-rational, the l-part of the the ring class fields of l-power conductor is not contained in K_{anti}, and the problem lies in identifying the intersection.

Theorem 24. *Assume that p is different from l and splits in K. We may then write*

$$p^h = \begin{cases} a^2 + \Delta b^2 & \text{if } \Delta \not\equiv 3 \ (\textit{mod } 4), \\ a^2 + ab + ((\Delta+1)/4)b^2 & \text{if } \Delta \equiv 3 \ (\textit{mod } 4), \end{cases} \tag{3.1}$$

with relatively prime $a, b \in \mathbb{Z}$. Put $\omega := \sqrt{-\Delta}$ if $\Delta \not\equiv 3$ (mod 4), otherwise $\omega := (1 + \sqrt{-\Delta})/2$. Let $n \geq 0$ be an integer.

(a) Suppose l splits in K. Write $(a + b\omega)^{l-1} = a^* + b^*\omega$. Then $\mathfrak{p}$ splits totally in $K_{\text{anti}}^{(n)}$ iff $b^* \equiv 0$ (mod $l^{n+1+\mu-\nu}$).

(b) *Suppose l is inert in K. Write $(a+b\omega)^{l+1} = a^* + b^*\omega$. Then the conclusion of (a) holds.*

(c) *Suppose l is ramified in K and we are not in the exceptional case (d). Then $\mathfrak{p}$ splits totally in $K_{\text{anti}}^{(n)}$ iff $b \equiv 0$ (mod $l^{n+\mu-\nu}$).*

(d) *Suppose $l = 3$ and $\Delta \equiv 3$ (mod 9). Write $(a + b\omega)^3 = a^* + b^*\omega$. Then $\mathfrak{p}$ splits totally in $K_{\text{anti}}^{(n)}$ iff $b^* \equiv 0$ (mod $3^{n+2+\mu-\nu}$).*

Proof. Write $(p) = \mathfrak{p}\mathfrak{q}$ with conjugate prime ideals $\mathfrak{p}, \mathfrak{q}$ of K. By definition of h, $\mathfrak{p}^h$ and $\mathfrak{q}^h$ are principal, i.e. $\mathfrak{p}^h = (a+b\omega)$ and $\mathfrak{q}^h = (a+b\bar{\omega})$ for some $a, b \in \mathbb{Z}$. When $\Delta \not\equiv 3$ (mod 4), we have $(p^h) = \mathfrak{p}^h\mathfrak{q}^h = (a + b\sqrt{-\Delta})(a - b\sqrt{-\Delta}) = (a^2 + \Delta b^2)$ and consequently $p^h = a^2 + \Delta b^2$. The representation of p^h in case $\Delta \equiv 3$ (mod 4) is seen similarly. If a and b were not relatively prime, then $\mathfrak{p}^h = (a + b\omega)$ and $\mathfrak{q}^h = (a + b\bar{\omega})$ would not be relatively prime either, a contradiction.

Now assume a representation

$$p^h = (u + v\omega)(u + v\bar{\omega})$$

is given with relatively prime $u, v \in \mathbb{Z}$. Then $\mathfrak{p}^h\mathfrak{q}^h = (p^h) = (u + v\omega)(u + v\bar{\omega})$. If $(u + v\omega)$ and $(u + v\bar{\omega})$ were not relatively prime, then one of these ideals would be divisible by $\mathfrak{p}\mathfrak{q} = (p)$ which is not the case since u and v are relatively prime. Hence the ideal $(u + v\omega)$ equals either $\mathfrak{p}^h$ or $\mathfrak{q}^h$, say $(u + v\omega) = \mathfrak{p}^h = (a + b\omega)$.

The remainder of the proof relies on Main Lemma 17 whose notation we adopt. The different cases are now treated separately.

(a) Assume l splits in K. It follows immediately from the definition of ν that $\text{Gal}(K_{\max}/K_{\text{anti}}^{(\nu)}) = U \times V \times T \times T'$. Hence $l^\nu = |W \times T : V \times T|$ and $|T| = l^{\mu-\nu}$ since $|W \times T : V| = l^\mu$.

Consider the conductor $\mathfrak{m} = l^e$ with $e = n + 1 + \mu - \nu$. By Main Lemma 17 (v) and (ix), $V^\mathfrak{m}$ is contained in W and hence

$$\text{Gal}(K^\mathfrak{m}/K) = \bar{U} \times \bar{W} \times T \times T'$$

where $\bar{U} = U/U^\mathfrak{m}$ is cyclic of order $l^{e-1} = l^{n+\mu-\nu}$, $\bar{W} = W/V^\mathfrak{m}$ is cyclic of order $l^{e-1+\nu} = l^{n+\mu}$, and T' has order prime to l. The fixed field of $\bar{U} \times T \times T'$ is $K_{\text{anti}}^{(n+\mu)}$ It follows from Lemma 20 that he image of $(\mathbb{Z}/l^e)^*$ under the Artin symbol

$$\left(\frac{K^\mathfrak{m}/K}{}\right) : (\mathcal{O}/l^e)^* \to \text{Gal}(K^\mathfrak{m}/K)$$

is $\bar{U} \times S''$ where S'' is a subgroup of T' with index $u(l-1)$.

Let W_0 be the subgroup of $\bar{W}$ of order l^μ. Then $K_{\text{anti}}^{(n)}$ is the fixed field of $\bar{U} \times W_0 \times T \times T'$. Now class field theory yields (see Neukirch [22]),

$$\begin{aligned}
\mathfrak{p} \text{ splits in } K_{\text{anti}}^{(n)} \quad &\Leftrightarrow \quad \left(\frac{K^{\mathfrak{m}}/K}{\mathfrak{p}}\right) \in \bar{U} \times W_0 \times T \times T' \\
&\Leftrightarrow \quad \left(\frac{K^{\mathfrak{m}}/K}{\mathfrak{p}^{h(l-1)}}\right) \in \bar{U} \times S'' \\
&\Leftrightarrow \quad b^* \equiv 0 \pmod{l^e}
\end{aligned}$$

if we write $\mathfrak{p}^{h(l-1)} = (a^* + b^*\omega)$.

(b) If l is inert in K, everything goes the same way except that T' has now order $u(l^2-1)/2$.

(c) Suppose l ramifies in K and we are not in the exceptional case. Then T' has order $u(l-1)/2$, and everything goes as above using the conductor $\mathfrak{m} = l^e$ with $e = n + \mu - \nu$.

(d) Suppose we are in the exceptional case. Then $|T| = 3^{\mu-\nu+1}$ and $|T'| = u(l-1)/2$. Using the conductor $\mathfrak{m} = l^e$ with $e = n+2+\mu-\nu$, the same arguments hold if we write $\mathfrak{p}^{3h} = (a^* + b^*\omega)$. □

Remark. Everything goes the same way if one uses the exponent of K's class group instead of h.

When the l-Hilbert class field of K is non-trivial, the decomposition law depends on how much of it is contained in K_{anti}, expressed by the number ν. Since all primes trivially split in in the zero'th step $K_{\text{anti}}^{(0)} = K$, but not all primes split in $K_{\text{anti}}^{(1)}$, we can give the following description of ν (here stated in the case where l splits in K, the other cases are similar): *Let p run through all primes $\neq l$ that split in K, and compute b^* as in Theorem 24 (a). Then ν is the minimal integer such that $l^{1+\mu-\nu}$ divides all the b^*.* We illustrate this principle by three examples.

Example 25. Let $l = 5$ and $K = \mathbb{Q}(\sqrt{-599})$. The class group of K is cyclic of order 25. Thus $\mu = 2$ and $\nu = 0, 1$, or 2. The prime $p = 2$ splits in K since $(-599/2) = 1$. We therefore write $2^{25} = a^2 + ab + 150b^2$ with $a = 5737$ and $b = 49$ and find $b^* = 37079430566955$ (Theorem 24 (a)). Since b^* is divisible by 5, but not by 25, we conclude $\nu = 2$. In other words: *the entire Hilbert class field K_H of K is contained in K_{anti}.*

Example 26. Let $l = 5$ and $K = \mathbb{Q}(\sqrt{-479})$. Again, the class group of K is cyclic of order 25, so $\mu = 2$ and $\nu = 0, 1$, or 2. Further, $p = 2$ again splits in K. Writing $2^{25} = a^2 + ab + 120b^2$ with $a = -56$ and $b = 529$ gives

$b^* = -14765386940175$ which is divisible by 25, but not by 125. This shows $\nu \geq 1$, so K_H contains at least $K_{\text{anti}}^{(1)}$. Now class field theory gives a simple decomposition law for $K_{\text{anti}}^{(1)}$: *a prime ideal* $\mathfrak{p}$ *of* K *splits in* $K_{\text{anti}}^{(1)}$ *iff it has order 1 or 5 in the ideal class group.* Since 2^5 is not of the form $a^2 + ab + 120b^2$, a prime $\mathfrak{p}$ of K dividing 2 has order 25 in the class group, so it does not split in $K_{\text{anti}}^{(1)}$. If ν were equal to 2, Theorem 24 (a) would contradict this. Hence ν equals 1, and we conclude: K_{anti} *contains the subfield of* K_H *of degree 5 over* K*, but not the entire* K_H*.*

Example 27. Let $l = 5$ and $K = \mathbb{Q}(\sqrt{-2887})$. The class group of K is cyclic of order 25. Writing $2^{25} = a^2 + ab + 722b^2$ with $a = 4771$ and $b = 119$ gives $b^* = -503658527236874547125$ which is divisible by 125. The same arguments as in Example 26 show that $p = 2$ is inert in H_K. This implies $\nu = 0$ and therefore: K_H *and* K_{anti} *are linearly disjoint over* K*.*

Finding a primitive representation of p^h by the principal binary quadratic form of discriminant d_K requires some thought when h is large. Since p is assumed to split in K, p is representable by some primitive form of discriminant d_K. For $\Delta = -599$, for example, the class group of $K = \mathbb{Q}(\sqrt{-599})$ is cyclic of order 25, and there are 25 reduced forms of discriminant -599. One of these is $2x^2 + xy + 75y^2$, representing $p = 2$, 103, 211 etc. What we need now is some way of getting a representation of p^{25} by the form $a^2 + ab + 150b^2$ from the representation of p by $2x^2 + xy + 75y^2$. The classical theory of composition of forms as developed by Lagrange, Legendre, and Gauss solves this problem. Indeed, Gauss writes in *Disquisitiones Arithmeticae* (1801), paragraph 244:

> *Si per formam aliquam f repraesentari potest numerus a, per formam f' numerus a', atque forma F in ff' est transformabilis: nullo negotio perspicitur, productum aa' per formam F repraesentabile fore.*
>
> If the number a can be represented by some form f, the number a' by the form f', and the form F is transformable into ff' (i.e. F is equivalent to ff'): the product aa' is with no difficulty seen to be representable by the form F.

Working this out explicitly in our example gives the identity

$$(2x^2 + xy + 75y^2)^{25} = a^2 + ab + 150b^2$$

with the formidable expressions

$$\begin{aligned}
a &= 5737x^{25} - 91875x^{24}y- \\
&65092500x^{23}y^2 + 67447500x^{22}y^3+ \\
&103112996250x^{21}y^4 + 158110895250x^{20}y^5- \\
&53870804872500x^{19}y^6 - 126755146072500x^{18}y^7+ \\
&12194776755129375x^{17}y^8 + 31718890562926875x^{16}y^9- \\
&1356699586464321000x^{15}y^{10} - 3520204400465145000x^{14}y^{11}+ \\
&78886011398262967500x^{13}y^{12} + 193451948219481577500x^{12}y^{13}- \\
&2452713817135817565000x^{11}y^{14} - 5459267179075675053000x^{10}y^{15}+ \\
&40449997738560715944375x^9y^{16} + 78446421200576378131875x^8y^{17}- \\
&339479206707433788682500x^7y^{18} - 544224194572452405742500x^6y^{19}+ \\
&1325418345983101131704250x^5y^{20} + 1615531276650390507251250x^4y^{21}- \\
&2004786679367985817042500x^3y^{22} - 1567484258719010395702500x^2y^{23}+ \\
&751856639324745597343125xy^{24} + 210972665126371211409675y^{25},
\end{aligned}$$

$$\begin{aligned}
b &= 49x^{25} + 72325x^{24}y- \\
&117300x^{23}y^2 - 249970900x^{22}y^3- \\
&501939350x^{21}y^4 + 215483219490x^{20}y^5+ \\
&622656857900x^{19}y^6 - 72265343734100x^{18}y^7- \\
&223898051032425x^{17}y^8 + 11305829887202675x^{16}y^9+ \\
&34419776360103640x^{15}y^{10} - 901554415980148200x^{14}y^{11}- \\
&2579359309593087700x^{13}y^{12} + 38153326044334939900x^{12}y^{13}+ \\
&99259403255921364600x^{11}y^{14} - 862933285089295273480x^{10}y^{15}- \\
&1975687645051553227025x^9y^{16} + 10184376201223013660475x^8y^{17}+ \\
&19695732755955420398300x^7y^{18} - 58907482043693383631300x^6y^{19}- \\
&90469751492421868406070x^5y^{20} + 147017689820318959916450x^4y^{21}+ \\
&160231724224609951560700x^3y^{22} - 120297062291959295574900x^2y^{23}- \\
&70324221708790403803225xy^{24} + 13630648352319103870798y^{25}
\end{aligned}$$

and shows the not evident fact that a and b are relatively prime when $2x^2+xy+75y^2$ is prime. This formula gives the expression for 2^{25} in Example 25, but also for instance

$$103^{25} = a^2 + ab + 150b^2$$

with

$$\begin{aligned}
a &= 140436428063910768266648713, \\
b &= -33528624548147312802520 2,
\end{aligned}$$

by writing $103 = 2x^2 + xy + 75y^2$ with $x = 4$ and $y = -1$ and inserting these values in the expressions for a and b above.

3.4 Discriminants with one class per genus

Given a negative discriminant D, i.e. a negative integer $D \equiv 0, 1 \pmod 4$, one may consider the property that each genus of primitive, positive definite quadratic forms of discriminant D consists of a single class. Dickson [9] is the first to give a list of 101 such D, and it is now known that there exists at most one more (see [8] and the references therein). Of these, 65 are of the form $D = -4n$, and these n are the *convenient numbers* or *numeri idonei* studied by Euler. It is a strange coincidence that there are also 65 numbers in Dickson's list that are fundamental discriminants.

D	$h(D)$	D	$h(D)$	D	$h(D)$	D	$h(D)$	D	$h(D)$
−4	1	−64	2	−192	4	−480	8	−1248	8
−8	1	−72	2	**−228**	4	**−520**	4	**−1320**	8
−12	1	**−84**	4	**−232**	2	**−532**	4	**−1380**	8
−16	1	**−88**	2	−240	4	**−660**	8	**−1428**	8
−20	2	−96	4	**−280**	4	−672	8	**−1540**	8
−24	2	−100	2	−288	4	**−708**	4	−1632	8
−28	1	−112	2	**−312**	4	**−760**	4	**−1848**	8
−32	2	**−120**	4	**−340**	4	**−840**	8	−2080	8
−36	2	**−132**	4	−352	4	−928	4	−3040	8
−40	2	**−148**	2	**−372**	4	−960	8	−3360	16
−48	2	−160	4	**−408**	4	**−1012**	4	−5280	16
−52	2	**−168**	4	**−420**	8	**−1092**	8	**−5460**	16
−60	2	−180	4	−448	4	−1120	8	−7392	16

Table 1: Negative discriminants $D \equiv 0 \pmod 4$ with one class per genus. Fundamental discriminants are bold.

D	$h(D)$	D	$h(D)$	D	$h(D)$	D	$h(D)$	D	$h(D)$
−3	1	**−51**	2	**−163**	1	**−435**	4	**−1435**	4
−7	1	**−67**	1	**−187**	2	**−483**	4	**−1995**	8
−11	1	−75	2	**−195**	4	**−555**	4	**−3003**	8
−15	2	**−91**	2	**−235**	2	**−595**	4	**−3315**	8
−19	1	−99	2	**−267**	2	**−627**	4		
−27	1	**−115**	2	−315	4	**−715**	4		
−35	2	**−123**	2	**−403**	2	**−795**	4		
−43	1	−147	2	**−427**	2	**−1155**	8		

Table 2: Negative discriminants $D \equiv 1 \pmod 4$ with one class per genus. Fundamental discriminants are bold.

As we shall now see, the anti-cyclotomic decomposition law takes a more elegant form when d_K is one of the 65 fundamental discriminants in Dickson's list.

THEOREM 28. *Assume that each genus of primitive, positive forms of discriminant d_K consists of a single class, and that l divides Δ. If $l = 3$, assume further $\Delta \not\equiv 3 \pmod 9$. Consider a prime number p with $(d_K/p) = 1$.*

(a) Assume Δ is even. We may then write

$$p = dx^2 + (\Delta/d)y^2 \tag{3.2}$$

with some positive d dividing Δ/l.

(b) Assume $\Delta \equiv 1 \pmod 4$. We may then write either $p = dx^2 + (\Delta/d)y^2$ as above or

$$p = 2dx^2 + 2dxy + \frac{\Delta/d + d}{2}y^2 \tag{3.3}$$

with some positive d dividing Δ/l.

(c) Assume $\Delta \equiv 3 \pmod 4$. We may then write

$$p = dx^2 + dxy + \frac{\Delta/d + d}{4}y^2 \tag{3.4}$$

with some positive d dividing Δ/l.

(d) A prime $\mathfrak{p}$ of K dividing p splits totally in $K_{\text{anti}}^{(n)}$ iff l^n divides y.

Proof. It is well known that a prime p splitting in K is representable by a (unique) primitive, positive quadratic form of discriminant d_K. The assumption that each genus consists of a single class implies that K's class group has exponent at most 2, an observation due to Gauss. The list of reduced forms of order ≤ 2 is also well known, see [8].

To show (d), we must find a primitive representation of p^2 (the case $h = 1$ is trivial and can be excluded) by the principal form of discriminant d_K in order to use Theorem 24. Squaring (3.2) gives the identity or "duplication formula"

$$p^2 = (dx^2 - (\Delta/d)y^2)^2 + \Delta(2xy)^2\ .$$

Primitivity is evident. Since l divides Δ/d, but not p, it follows from (3.2) that l does not divide x either. Hence the maximal power of l dividing $2xy$ equals the maximal power of l dividing y.

Squaring (3.3) gives

$$p^2 = \left(\frac{d(2x+y)^2 - (\Delta/d)y^2}{2}\right)^2 + \Delta\Big((2x+y)y\Big)^2\ .$$

Again, primitivity is clear. If we put $a = d(2x + y)$ and $b = y$, then

$$2dp = a^2 + \Delta b^2 \ . \tag{3.5}$$

By (3.5), l does not divide a and consequently not $2x + y = a/d$ either. Hence the maximal power of l dividing $(2x+y)y$ equals the maximal power of l dividing y.

Squaring (3.4) gives

$$\begin{aligned} p^2 \ = \ & \left(dx^2 + (d-1)xy - \frac{\Delta/d - d + 2}{4}y^2\right)^2 + \\ & \left(dx^2 + (d-1)xy - \frac{\Delta/d - d + 2}{4}y^2\right)\Big((2x+y)y\Big) + \frac{\Delta + 1}{4}\Big((2x+y)y\Big)^2 \ . \end{aligned}$$

Note that $\Delta/d + d$ is divisible by 4 since $\Delta \equiv 3 \pmod 4$. If we put $a = (d(2x + y) - y)/2$ and $b = y$, then

$$dp = a^2 + ab + \left(\frac{\Delta + 1}{4}\right) b^2 \ . \tag{3.6}$$

Multiplication with 4 gives

$$4dp = (2a + b)^2 + \Delta b^2 \ . \tag{3.7}$$

From (3.7) follows $p \nmid (2a + b)b$ and hence $p \nmid (2x + y)y$. This gives primitivity. Also by (3.7), l does not divide $2a + b$ and consequently not $2x + y = (2a + b)/d$ either. Hence the maximal power of l dividing $(2x + y)y$ equals the maximal power of l dividing y. □

Example 29. (a) Let $K = \mathbb{Q}(\sqrt{-10})$ and $l = 5$. Consider prime numbers p with $(-10/p) = 1$. Then a prime $\mathfrak{p}$ of K dividing p splits in the first step of K_{anti} iff p is of the form $x^2 + 250y^2$ or $2x^2 + 125y^2$.

(b) Let $K = \mathbb{Q}(\sqrt{-5})$ and $l = 5$. Consider prime numbers p with $(-5/p) = 1$. Then a prime $\mathfrak{p}$ of K dividing p splits in the first step of K_{anti} iff p is of the form $x^2 + 125y^2$ or $2x^2 + 10xy + 75y^2$.

(c) Let $K = \mathbb{Q}(\sqrt{-15})$ and $l = 5$. Consider prime numbers p with $(-15/p) = 1$. Then a prime $\mathfrak{p}$ of K dividing p splits in the first step of K_{anti} iff p is of the form $x^2 + 5xy + 100y^2$ or $3x^2 + 15xy + 50y^2$.

3.5 The first step of the anti-cyclotomic extension

In this section we address the problem of finding the first step $K_{\mathrm{anti}}^{(1)}$ of the anti-cyclotomic extension K_{anti}/K. By "finding" we understand displaying explicitly a polynomial f over $\mathbb{Q}$ of degree l having $K_{\text{anti}}^{(1)}$ as its splitting field. The decomposition laws from section 3.3 then dictate the factorisation of f modulo p. In some cases we will actually use this knowledge of the factorisation to identify f among a number of candidates.

To begin with, recall that $K_{\text{anti}}^{(1)}$ is a dihedral extension of $\mathbb{Q}$ of degree $2l$ having K as its quadratic subfield, and that $K_{\text{anti}}^{(1)}/K$ is unramified outside l. If K is l-rational, $K_{\text{anti}}^{(1)}$ is unique with these properties. We state without proof a lemma that allows us easily to determine if a given dihedral extension is unramified, or unramified outside l, over its quadratic subfield.

Lemma 30. *Consider a dihedral extension $M/\mathbb{Q}$ of degree $2l$ having K as its quadratic subfield. Let L be one of the l subfields of M of absolute degree l. Then the cyclic extension M/K is unramified iff the field discriminants satisfy $d_L = d_K^{(l-1)/2}$. Further, M/K is unramified outside l iff $d_L =$ (power of l)$\cdot d_K^{(l-1)/2}$.*

So when K is l-rational, we can find $K_{\text{anti}}^{(1)}$ by guessing a D_l-polynomial f whose splitting field contains K, and such that the discriminant condition of the lemma is satisfied. Some examples are given in the following table.

Δ	h	f (for $l=3$)	f (for $l=5$)
1	1	X^3-3X-4	$X^5+2500X+120000$
2	1	$X^3-3X-10$	$X^5+6875X+17500$
3	1	X^3-3	$X^5+10X^3-15X^2+10X-12$
5	2	X^3-3X-8	$X^5+20X+32$
6	2	X^3+3X-2	$X^5+15X^3-70X^2+60X-24$
7	1	X^3-3X-5	$X^5+15X^3-5X^2+35X-91$
10	2	$X^3-3X-22$	$X^5-5X+12$
11	1	X^3+6X-1	$X^5-15X^3-15X^2+110X+143$
13	2	$X^3+9X-36$	$X^5+25772500X-395460000$
14	4	$X^3-3X-26$	$X^5+10X^3-140X^2+585X-532$
15	2	X^3+3X-1	X^5+5X^2+3
17	4	$X^3+6X-28$	$X^5-35X^3-30X^2+1060X-2616$
19	1	X^3+6X-5	$X^5+35X^3-40X^2+160X-232$

Consider one of the polynomials f from the table, and let p be a prime not dividing the discriminant of f. If p is inert in K, then it splits in $K_{\text{anti}}^{(1)}$. It follows that f is the product of one linear and $(l-1)/2$ irreducible quadratic polynomials modulo p. If, on the other hand, p splits as $\mathfrak{p}\mathfrak{q}$ in K, then f is either irreducible modulo p, or f is the product of linear factors modulo p – and this happens according to whether $\mathfrak{p}$ is inert or splits in $K_{\text{anti}}^{(1)}$.

For example, the result mentioned in the introduction about the factorisation of the polynomial $X^5 + 5X^2 + 3$ modulo p follows immediately from the above table ($\Delta = 15$) and Example 29 (c).

When K is not l-rational, finding $K_{\text{anti}}^{(1)}$ is harder since it is no longer unique with the property of being dihedral over $\mathbb{Q}$ and unramified outside l over K. But this case can be dealt with by first finding all fields with that property, and then identifying $K_{\text{anti}}^{(1)}$ using our knowledge of which primes split in that field. This method always leads to a conclusive answer, for different Galois extensions have different sets of splitting primes by a theorem of Bauer (see [22], page 572). We illustrate by two examples.

Example 31. Let $l = 3$ and consider $K = \mathbb{Q}(\sqrt{-21})$. This field is not 3-rational, indeed it has (two linearly disjoint and hence) four $\mathbb{Z}/3$-extensions which are unramified outside 3 and dihedral over $\mathbb{Q}$ (see [3]). Using Lemma 30 and a computer, we easily find four polynomials $f_1, \ldots, f_4$ whose splitting fields are the above-mentioned four dihedral fields. The polynomials are shown in the below table together with all primes < 200 modulo which they split into linear factors. These prime lists are the “finger prints” of the polynomials, and we shall use them to uncover the culprit among our four suspects.

i	f_i	primes < 200 modulo which f_i splits
1	$X^3 - 3X + 16$	$17, 101, 107, 139, 179, 193$
2	$X^3 + 9X + 12$	$11, 19, 89, 103, 191$
3	$X^3 + 9X + 30$	$5, 71, 109, 199$
4	$X^3 + 18X + 12$	$23, 31, 37, 41, 173$

Now consider a prime p that splits in K, i.e. with $(-21/p) = 1$. The class group of K has exponent 2, so we may write

$$p^2 = a^2 + 21b^2$$

with relatively prime $a, b \in \mathbb{N}$. This is shown in the table below for all $p < 200$. We have

$$(a + b\sqrt{-21})^3 = (a^3 - 63ab^2) + (3a^2b - 21b^3)\sqrt{-21} \; .$$

Therefore, by Theorem 24 (d), p splits in $K_{\text{anti}}^{(1)}$ iff $b^* = 3a^2b - 21b^3$ is divisible by

27. The primes for which this is the case are typed in bold in the table.

p	a	b	b^*
5	2	1	-9
11	10	1	279
17	10	3	333
19	5	4	-1044
23	2	5	-2565
31	25	4	6156
37	5	8	-10152
41	34	5	14715
71	50	11	54549
89	86	5	108315
101	74	15	175545
103	47	20	-35460
107	82	15	231705
109	59	20	40860
139	85	24	229896
173	170	7	599697
179	10	39	-1233999
191	170	19	1503261
193	185	12	1195812
199	185	16	1556784

Comparing the bold primes with the ones in the previous table reveals f_4 as the wanted polynomial.

Let us note additionally that p splits in the 3-part of K's ray class field of conductor 3 iff b is divisible by 3. The table shows that this is the case for the primes $17, 101, 107$ etc., i.e. the primes modulo which the polynomial f_1 splits. So this ray class field is the splitting field of f_1. Finally, all four polynomials f_i split modulo p iff b is divisible by 9.

Example 32. We now aim at finding the first step of the anti-cyclotomic extension of $K = \mathbb{Q}(\sqrt{-107})$ for $l = 3$. Again, there are four $\mathbb{Z}/3$-extensions of K which are unramified outside 3 and dihedral over $\mathbb{Q}$ (see [3]), and we find four candidate polynomials:

i	f_i	primes < 200 modulo which f_i splits
1	$X^3 - X + 4$	$29, 47, 83, 137$
2	$X^3 + 6X - 17$	$23, 37, 47, 61, 79, 101, 149$
3	$X^3 + 15X - 28$	$11, 19, 47, 151, 163, 197$
4	$X^3 + 18X - 45$	$13, 41, 47, 53, 89, 193, 199$

The class number of K is 3, and since f_1 generates a cubic field with discriminant -107, the splitting field of f_1 is the Hilbert class field of K by Lemma 30. The anti-cyclotomic decomposition law depends on whether this class field is contained in K_{anti} (and thus equals $K_{\text{anti}}^{(1)}$) or not.

Let $p \neq 3$ be a prime that splits in K. Since K has class number 3, we write

$$p^3 = a^2 + ab + 27b^2$$

with relatively prime $a, b \in \mathbb{Z}$. This representation is shown in the table below for all $p < 200$. We are in case (a) of Theorem 24 and must compute

$$(a + b\omega)^2 = (a^2 - 27b^2) + (2ab + b^2)\omega \ .$$

Thus, p splits in $K_{\text{anti}}^{(1)}$ iff $b^* = 2ab + b^2$ is divisible by $3^{3-\nu}$.

p	a	b	b^*
11	1	7	63
13	1	9	99
19	64	9	1233
23	89	11	2079
29	107	20	4680
37	163	27	9531
41	118	43	11997
47	253	34	18360
53	341	29	20619
61	442	27	24597
79	523	81	91287
83	109	142	51120
89	694	79	115893
101	962	47	92637
137	163	304	191520
149	953	281	614547
151	1412	207	627417
163	1360	279	836721
193	1189	441	1243179
197	2690	83	453429
199	316	531	617553

Now if the Hilbert class field were contained in K_{anti}, that is if $\nu = 1$, then all the primes in the table would split in $K_{\text{anti}}^{(1)}$ since all the b^* are divisible by 9. Not only does this seem unlikely, it is also demonstrably false since none of the polynomials f_i splits modulo all these primes. Hence $\nu = 0$, and the Hilbert class field is not contained in K_{anti}. So the p that split in $K_{\text{anti}}^{(1)}$ are the ones for which 27 divides b^*. These primes (typed in bold in the table) are the ones in the second line of the previous table, thereby identifying f_2 as the polynomial whose splitting field is $K_{\text{anti}}^{(1)}$.

Chapter 4

The ring class field of conductor 2^∞ over imaginary quadratic number fields

4.1 Introduction

Consider an imaginary quadratic number field K with Hilbert class field K_H. The ring class field $N = N(2^\infty)$ over K of conductor 2^∞ is the maximal 2-ramified (i.e. unramified outside 2) abelian extension of K which is generalised dihedral over $\mathbb{Q}$.

We determine the structure of the Galois group $\mathrm{Gal}(N/K_H)$ and, in some cases, $\mathrm{Gal}(N/K)$.

N/K has a unique $\mathbb{Z}_2$-subextension which we call the **anti-cyclotomic** $\mathbb{Z}_2$-extension K_{anti}. We give a law for the decomposition of primes p in K_{anti}. This law involves a representation of a power of p by a binary quadratic form as well as the degree 2^ν of $K_{\text{anti}} \cap K_H$ over K. The exponent ν is the number of unramified steps of K_{anti}.

The first step of the anti-cyclotomic extension is of the form $K(\sqrt{a})$ with an $a \in \mathbb{Z}$. When the 2-class group of K is cyclic (possibly trivial), we give an algorithm to compute both ν and a. In most cases we can even give an explicit expression for ν and a. This involves some formulae of Hasse giving the 2-class number 2^μ of K. We give here alternative proofs of Hasse's results using quadratic forms rather than ideals. The key ingredient in the proofs presented here are two new explicit expressions (4.10 and 4.12) for a form representing a class of order 4.

When the 2-class field of K is non-trivial and cyclic, one can ask if it can be embedded into a $\mathbb{Z}_2$-extension of K. We answer this question completely.

Finally, some interrelations between the class groups and anti-cyclotomic extensions of the two fields $\mathbb{Q}(\sqrt{-l})$ and $\mathbb{Q}(\sqrt{-2l})$ are given, some of which are conjectural.

Throughout the article we use the following notation:

$\mathbb{Z}_2$:	the additive group of dyadic integers
Δ :	a square-free natural number
K :	the imaginary quadratic number field $\mathbb{Q}(\sqrt{-\Delta})$
$\mathcal{O}$:	the ring of integral elements in K
ω :	$\sqrt{-\Delta}$ if $\Delta \equiv 1, 2 \pmod 4$, otherwise $(1+\sqrt{-\Delta})/2$
d_K :	the discriminant of K
r :	the number of odd primes $l_1, \dots l_r$ dividing Δ
s :	the number of primes dividing d_K
h, μ, u :	we write the class number of K as $h = 2^\mu u$ with odd u
$N(f)$:	the ring class field over K of conductor f
K_H :	the Hilbert class field of K, i.e. $K_H = N(1)$
$K_{\text{anti}}^{(n)}$:	the n'th step of the anti-cyclotomic $\mathbb{Z}_2$-extension K_{anti}
ν :	the non-negative integer defined by $K_{\text{anti}} \cap K_H = K_{\text{anti}}^{(\nu)}$

4.2 The ring class field of conductor 2^∞ and the anti-cyclotomic extension

Let $N(2^\infty)$ denote the union of all $N(2^e)$, $e \geq 1$. We call it the ring class field of conductor 2^∞ over K. It is the maximal 2-ramified (i.e. unramified outside 2) abelian extension of K which is generalised dihedral over $\mathbb{Q}$.

LEMMA 33. *Let $e \geq 1$ if $\Delta \equiv 1, 2$ (mod 4), otherwise $e \geq 2$. For $\Delta \neq 1, 3$ we have*

$$Gal(N(2^e)/K_H) \cong \begin{cases} \mathbb{Z}/2^e & \text{if } \Delta \equiv 2 \ (mod\ 4), \\ \mathbb{Z}/2^{e-1} \times \mathbb{Z}/2 & \text{if } \Delta \equiv 1 \ (mod\ 4), \\ \mathbb{Z}/2^{e-2} \times \mathbb{Z}/2 & \text{if } \Delta \equiv 7 \ (mod\ 8), \\ \mathbb{Z}/2^{e-2} \times \mathbb{Z}/6 & \text{if } \Delta \equiv 3 \ (mod\ 8), \end{cases}$$

and further

$$Gal(N(2^\infty)/K_H) \cong \begin{cases} \mathbb{Z}_2 & \text{if } \Delta \equiv 2 \ (mod\ 4), \\ \mathbb{Z}_2 \times \mathbb{Z}/2 & \text{if } \Delta \equiv 1, 5, 7 \ (mod\ 8), \\ \mathbb{Z}_2 \times \mathbb{Z}/6 & \text{if } \Delta \equiv 3 \ (mod\ 8). \end{cases}$$

In addition,

$$\mathit{Gal}(N(2^e)/K_H) \cong \begin{cases} \mathbb{Z}/2^{e-1} & \textit{for } \Delta = 1, \\ \mathbb{Z}/2^{e-2} \times \mathbb{Z}/2 & \textit{for } \Delta = 3 \end{cases}$$

and

$$\mathit{Gal}(N(2^\infty)/K_H) \cong \begin{cases} \mathbb{Z}_2 & \textit{for } \Delta = 1, \\ \mathbb{Z}_2 \times \mathbb{Z}/2 & \textit{for } \Delta = 3. \end{cases}$$

Proof. Class field theory gives a surjective homomorphism (the "Artin symbol")

$$\left(\frac{N(f)/K}{}\right) : (\mathcal{O}/f)^* \longrightarrow \mathrm{Gal}(N(f)/K_H)$$

whose kernel is generated by $(\mathbb{Z}/f)^*$ and $\mathcal{O}^*$. One shows that $(\mathcal{O}/2^e)^*/(\mathbb{Z}/2^e)^*$ equals

$$\begin{cases} \langle 1+\sqrt{-\Delta}\rangle \cong \mathbb{Z}/2^e & \text{if } \Delta \equiv 2 \pmod 4, \\ \langle 1+2\sqrt{-\Delta}\rangle \times \langle\sqrt{-\Delta}\rangle \cong \mathbb{Z}/2^{e-1} \times \mathbb{Z}/2 & \text{if } \Delta \equiv 1 \pmod 4, \\ \langle 1+4\omega\rangle \times \langle\sqrt{-\Delta}\rangle \cong \mathbb{Z}/2^{e-2} \times \mathbb{Z}/2 & \text{if } \Delta \equiv 7 \pmod 8, \\ \langle 1+4\omega\rangle \times \langle\sqrt{-\Delta}\rangle \times \langle a\rangle \cong \mathbb{Z}/2^{e-2} \times \mathbb{Z}/2 \times \mathbb{Z}/3 & \text{if } \Delta \equiv 3 \pmod 8, \end{cases}$$

where in the last case a is some element of order 3. From this everything follows. The exceptions for $\Delta = 1, 3$ are due to the fact that $\mathcal{O}^*$ in these cases is greater than $\{\pm 1\}$. □

It follows from the lemma that we have an isomorphism

$$\mathrm{Gal}(N(2^\infty)/K) \cong \mathbb{Z}_2 \times T$$

with a finite abelian group T. Hence K has a unique $\mathbb{Z}_2$-extension which is dihedral over $\mathbb{Q}$. We call it the **anti-cyclotomic** $\mathbb{Z}_2$-extension of K and denote it K_{anti}. Its n'th step $K_{\text{anti}}^{(n)}$ is the subextension of degree 2^n over K.

Being a subfield of $N(2^\infty)$, the anti-cyclotomic extension is 2-ramified. However, its lower steps may well be unramified also at 2. The number of unramified steps of K_{anti} is expressed by the number ν defined by

$$K_{\text{anti}} \cap K_H = K_{\text{anti}}^{(\nu)}.$$

The order of T depends on ν. If $\Delta \neq 1, 3$, then

$$|T| = \begin{cases} 2^{\mu-\nu} \cdot u & \text{if } \Delta \equiv 2 \pmod 8, \\ 2^{\mu-\nu+1} \cdot u & \text{if } \Delta \equiv 1, 5, 7 \pmod 8, \\ 3 \cdot 2^{\mu-\nu+1} \cdot u & \text{if } \Delta \equiv 3 \pmod 8, \end{cases}$$

and in the two exceptional cases,

$$|T| = \begin{cases} 1 & \text{if } \Delta = 1, \\ 2 & \text{if } \Delta = 3. \end{cases}$$

We note *en passant* that $N(2^\infty)$ is obtained by adjoining $\sqrt{-1}$ to K_{anti} in the case $\Delta = 3$.

When the 2-Hilbert class field of K is (non-trivial) cyclic, one may ask if it can be embedded in a $\mathbb{Z}_2$-extension of K. This happens of course when it is contained in the anti-cyclotomic extension, i.e. when $\nu = \mu$. In contrast to the case of $\mathbb{Z}_p$-embeddability for odd p, however, this is not a necessary condition. As we shall see, a cyclic 2-Hilbert class field might also be $\mathbb{Z}_2$-embeddable when $\nu = \mu - 1$. In the following, we give various ways of determining ν and use this to give a complete answer to the question of $\mathbb{Z}_2$-embeddability in section 4.12.

4.3 The genus field and other elementary abelian extensions of K

Let $l_1, \ldots, l_r$ be the odd primes dividing Δ. The **genus field** K_{gen} of $K = \mathbb{Q}(\sqrt{-\Delta})$ is the maximal unramified elementary abelian 2-extension of K. It is an elementary abelian 2-extension of $\mathbb{Q}$ and is given explicitly as

$$K_{\text{gen}} = \begin{cases} K(\sqrt{l_1^*}, \ldots, \sqrt{l_r^*}) & \text{if } \Delta \equiv 1, 2 \pmod 4 \\ K(\sqrt{l_1^*}, \ldots, \sqrt{l_{r-1}^*}) & \text{if } \Delta \equiv 3 \pmod 4 \end{cases}$$

where l^* denotes $(-1)^{(l-1)/2}p$ for an odd prime l. Thus $\text{Gal}(K_{\text{gen}}/K)$ has 2-rank

$$s - 1 = \begin{cases} r & \text{if } \Delta \equiv 1, 2 \pmod 4, \\ r - 1 & \text{if } \Delta \equiv 3 \pmod 4, \end{cases}$$

where s denotes the number of primes dividing K's discriminant d_K.

We note that the imaginary quadratic fields with trivial 2-class group are $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-2})$, and $\mathbb{Q}(\sqrt{-l})$ with a prime $l \equiv 3 \pmod 4$.

The imaginary quadratic fields with non-trivial cyclic 2-class group are $\mathbb{Q}(\sqrt{-l})$ with a prime $l \equiv 1 \pmod 4$, $\mathbb{Q}(\sqrt{-2l})$ with a prime $l > 2$, and $\mathbb{Q}(\sqrt{-ll'})$ with two primes $l \equiv 1 \pmod 4$ and $l' \equiv 3 \pmod 4$. For these fields, the genus field is the first step of the 2-class field and explicitly given by

$$\begin{aligned}
\mathbb{Q}(\sqrt{-l})_{\text{gen}} &= \mathbb{Q}(\sqrt{-l},\sqrt{-1})\ , \\
\mathbb{Q}(\sqrt{-2l})_{\text{gen}} &= \begin{cases} \mathbb{Q}(\sqrt{-2l},\sqrt{-2}) & \text{if } l \equiv 1 \pmod 4, \\ \mathbb{Q}(\sqrt{-2l},\sqrt{2}) & \text{if } l \equiv 3 \pmod 4, \end{cases} \\
\mathbb{Q}(\sqrt{-ll'})_{\text{gen}} &= \mathbb{Q}(\sqrt{-ll'},\sqrt{l})\ .
\end{aligned}$$

Define K_{elem} as the *maximal 2-ramified extension of* K *which is an elementary abelian 2-extension of* $\mathbb{Q}$. It is the maximal elementary abelian 2-subextension of $N(2^\infty)/K$. A short consideration gives

$$K_{\text{elem}} = \begin{cases} K_{\text{gen}}(\sqrt{-1},\sqrt{2}) & \text{if } \Delta \equiv 3 \pmod 4 \\ K_{\text{gen}}(\sqrt{-1}) & \text{if } \Delta \equiv 2 \pmod 4 \quad (\sqrt{2} \text{ or } \sqrt{-2} \text{ is in } K_{\text{gen}}) \\ K_{\text{gen}}(\sqrt{2}) & \text{if } \Delta \equiv 1 \pmod 4 \quad (\sqrt{-1} \text{ is in } K_{\text{gen}}) \end{cases}$$

Thus $\mathrm{Gal}(K_{\text{elem}}/K)$, and therefore also $\mathrm{Gal}(N(2^\infty)/K)$, has 2-rank $r+1$.

4.4 Prime decomposition in the anti-cyclotomic extension

Consider a prime $\mathfrak{p}$ of K (i.e. a prime ideal in $\mathcal{O}$) dividing an odd rational prime p. In this section we investigate the prime decomposition of $\mathfrak{p}$ in the anti-cyclotomic $\mathbb{Z}_2$-extension of K.

If p is inert in K, then $\mathfrak{p}$ is a principal ideal prime to 2. It then follows that $\mathfrak{p}$ splits totally in $N(2^\infty)$ (see the *Primzerlegungsgesetz* (7.3) in [22]) and hence also in K_{anti}. Similarly, if p ramifies in K, then $\mathfrak{p}$ splits totally in a subextension of $N(2^\infty)/K$ over which $N(2^\infty)$ has degree 2; in particular $\mathfrak{p}$ splits totally in K_{anti}. So we are left with the case where p splits in K.

THEOREM 34. *Let p be an odd rational prime that splits in $K = \mathbb{Q}(\sqrt{-\Delta})$. Assume at first $\Delta \neq 1, 3$. If h denotes the class number of K, we may write*

$$\begin{cases} p^h = a^2 + \Delta b^2 & \textit{for } \Delta \equiv 2 \ (\textit{mod } 4), \\ p^{2h} = a^2 + \Delta b^2 & \textit{for } \Delta \equiv 1 \ (\textit{mod } 4), \\ p^{2h} = a^2 + ab + ((\Delta+1)/4)b^2 & \textit{for } \Delta \equiv 7 \ (\textit{mod } 8), \\ p^{6h} = a^2 + ab + ((\Delta+1)/4)b^2 & \textit{for } \Delta \equiv 3 \ (\textit{mod } 8), \end{cases} \tag{4.1}$$

with relatively prime $a, b \in \mathbb{Z}$. Then for an integer $n \geq 0$, p splits totally in $K^{(n)}_{\text{anti}}$ iff

$$v_2(b) \geq \begin{cases} n+\mu-\nu & \text{when } \Delta \equiv 2 \pmod 4 \\ n+\mu-\nu+2 & \text{when } \Delta \equiv 1 \pmod 4 \\ n+\mu-\nu+3 & \text{when } \Delta \equiv 3 \pmod 4 \end{cases}$$

where v_2 denotes the dyadic valuation.

Now assume $\Delta = 1$. An (odd) rational prime p that splits in $K = \mathbb{Q}(i)$ may be written

$$p = a^2 + 4b^2,$$

and then

$$p \text{ splits totally in } K^{(n)}_{\text{anti}} \Leftrightarrow v_2(b) \geq n.$$

Assume finally $\Delta = 3$. An (odd) rational prime p that splits in $K = \mathbb{Q}(\sqrt{-3})$ may be written

$$p = a^2 + ab + b^2 \quad \text{with odd } a, b,$$

and then

$$p \text{ splits totally in } K^{(n)}_{\text{anti}} \Leftrightarrow \begin{cases} v_2(a+b) \geq n+2 & \text{for } p \equiv 1 \pmod 4, \\ v_2(a-b) \geq n+2 & \text{for } p \equiv 3 \pmod 4. \end{cases}$$

Proof. First assume $\Delta \equiv 2 \pmod 4$. Write $(p) = \mathfrak{p}\mathfrak{q}$ with primes $\mathfrak{p}, \mathfrak{q}$ of K. Then $\mathfrak{p}^h$ is principal with generator $a + b\omega$.

Consider the ring class field $N = N(2^e)$ over K with $e = n + \mu - \nu$. By Lemma 33 we may write

$$\text{Gal}(N/K) = W \times T$$

such that W is cyclic of order $2^{e+\nu} = 2^{n+\mu}$, T has order $2^{\mu-\nu}u$, and $K^{(n+\mu)}_{\text{anti}}$ is the fixed field of T.

Let W_0 be the subgroup of W of order 2^μ. Then $K^{(n)}_{\text{anti}}$ is the fixed field of $W_0 \times T$. Now class field theory gives

$$\begin{aligned} p \text{ splits in } K^{(n)}_{\text{anti}} \quad &\Leftrightarrow \quad (N/K, \mathfrak{p}) \in W_0 \times T \\ &\Leftrightarrow \quad (N/K, \mathfrak{p})^h = 1 \\ &\Leftrightarrow \quad a + b\omega \in (\mathbb{Z}/2^e)^* \\ &\Leftrightarrow \quad b \equiv 0 \pmod{2^e}. \end{aligned}$$

This finishes the proof for $\Delta \equiv 2 \pmod 4$.

The other cases with $\Delta \neq 1, 3$ are proved similarly using the ring class fields $N(2^e)$ with $e = n + \mu - \nu + 2$ and $e = n + \mu - \nu + 3$.

Now assume $\Delta = 1$. Then $K_{\text{anti}}^{(n)}$ equals the ring class field $N(2^{n+1})$ over K and the claim follows.

Finally assume $\Delta = 3$. Then the ring class field $N = N(2^{n+2})$ over K is the composite of $K_{\text{anti}}^{(n)}$ with a quadratic extension of K. A prime p that splits in K may be written

$$p = a^2 + ab + b^2.$$

We may assume that b is odd. The identity

$$a^2 + ab + b^2 = (-b)^2 + (-b)(a + b) + (a + b)^2$$

shows that we may also assume that a is odd. We have the representation

$$p^2 = (2ab + b^2)^2 + (2ab + b^2)(a^2 - b^2) + (a^2 - b^2)^2.$$

Hence

$$p \text{ splits in } K_{\text{anti}}^{(n)} \ \Leftrightarrow\ v_2(a^2 - b^2) \geq n + 3$$

Both $a + b$ and $a - b$ are even. If $p \equiv 1 \pmod 4$, then $a + b$, but not $a - b$ is divisible by 4. If $p \equiv 3 \pmod 4$, then $a - b$, but not $a + b$ is divisible by 4. The claim follows. □

Remark 35. Theorem 34 can be formulated in a slightly different manner in some cases.

(a) Assume $\Delta \equiv 1 \pmod 4$, $\Delta \neq 1$. We may write

$$p^h = u^2 + \Delta v^2$$

and get $p^{2h} = (u^2 - \Delta v^2)^2 + \Delta(2uv)^2$. Either u or v is odd, so

$$p \text{ splits in } K_{\text{anti}}^{(n)} \ \Leftrightarrow\ u \text{ or } v \text{ is divisible by } 2^{n+\mu-\nu+1}.$$

The proof of Theorem 34 shows that v is odd iff the ring class field extension $N(2)/K$ is cyclic, and p is inert in its first step (which is then necessarily $K_{\text{gen}} = K(\sqrt{-1})$). Thus

$$v \text{ is odd } \Leftrightarrow\ \Delta \text{ is prime and } p \equiv 3 \pmod 4.$$

(b) Assume $\Delta \equiv 7 \pmod 8$. Then we can write

$$p^h = u^2 + uv + ((\Delta + 1)/4)v^2$$

with necessarily odd u and even v. Thus $p^{2h} = a^2 + ab + ((\Delta + 1)/4)b^2$ with $a = u^2 - ((\Delta + 1)/4)v^2$ and $b = 2v(u + v/2)$. Either $v/2$ or $u + v/2$ is odd, so

$$p \text{ splits in } K_{\text{anti}}^{(n)} \ \Leftrightarrow\ v/2 \text{ or } u + v/2 \text{ is divisible by } 2^{n+\mu-\nu+1}.$$

Computing modulo 8 shows that $v/2$ is odd iff $p^h \equiv 3, 7 \pmod 8$, i.e.

$$v/2 \text{ odd } \Leftrightarrow \Delta \text{ is prime and } p \equiv 3 \pmod 4.$$

(c) Assume $\Delta \equiv 3 \pmod 8$. We can write

$$p^h = u^2 + uv + ((\Delta + 1)/4)v^2$$

and get a representation $p^{6h} = a^2 + ab + ((\Delta + 1)/4)b^2$ with

$$b = v(2u + v)\left(u^2 + uv + \frac{1 - 3\Delta}{4}v^2\right)\left(3u^2 + 3uv + \frac{3 - \Delta}{4}v^2\right). \tag{4.2}$$

Computing modulo 4 shows that two of the four factors in (4.2) are odd, one is 2 modulo 4, and one is 0 modulo 4. So

$$p \text{ splits in } K_{\text{anti}}^{(n)} \Leftrightarrow \text{ one of the factors in (4.2) is divisible by } 2^{n+\mu-\nu+2}.$$

There does not seem to be a simple criterion showing which of the factors are odd.

4.5 The norm form of the eighth cyclotomic field

An odd prime number l can be written as $u^2 + v^2$ or $x^2 - 2y^2$ or $z^2 + 2w^2$ iff $l \equiv 1, 5 \pmod 8$ or $l \equiv 1, 7 \pmod 8$ or $l \equiv 1, 3 \pmod 8$, respectively. When $l \equiv 1 \pmod 8$ and all three representations are at hand, there are some relations between them that we summarise in the following lemma.

Lemma 36. *Consider a prime number $l \equiv 1 \pmod 8$. We can write*

$$l = u^2 + v^2 = x^2 - 2y^2 = z^2 + 2w^2 \tag{4.3}$$

with integers u, v, x, y, z, w satisfying

$$u \text{ odd}, \ 4 \mid v, \ x > 0 \text{ odd}, \ y \text{ even}, \ z \text{ odd}, \ w \text{ even}. \tag{4.4}$$

In this situation we have

$$8 \mid v \Leftrightarrow x \equiv 1, 3 \pmod 8 \Leftrightarrow z \equiv 1, 7 \pmod 8. \tag{4.5}$$

If $l \equiv 1 \pmod{16}$, there holds in addition

$$u \equiv 1, 7 \pmod 8\,; \ x \equiv 1, 7 \pmod 8 \Leftrightarrow 4 \mid y\,; \ z \equiv 1, 7 \pmod 8 \Leftrightarrow 4 \mid w. \tag{4.6}$$

If $l \equiv 9$ (mod 16), there holds in addition

$$u \equiv 3,5\ (mod\,8)\ ;\ \ x \equiv 1,7\ (mod\,8)\ \Leftrightarrow\ 4 \nmid y\ ;\ \ z \equiv 1,7\ (mod\,8)\ \Leftrightarrow\ 4 \nmid w. \quad (4.7)$$

In particular, a prime number congruent to 1 modulo 16 is representable by both or none of the forms X^2+32Y^2 and X^2+64Y^2, whereas a prime number congruent to 9 modulo 16 is representable by one, but not both of these forms.

Proof. Consider the eighth cyclotomic field $\mathbb{Q}(\xi) = \mathbb{Q}(i, \sqrt{2})$ where $\xi = (1+i)/\sqrt{2}$. Since l splits in $\mathbb{Q}(\xi)$ which is a PID, l is the norm of an integer in $\mathbb{Q}(\xi)$. This means that l is of the form

$$\begin{aligned} l &= N_{\mathbb{Q}(\xi)/\mathbb{Q}}(a\xi^3 + b\xi^2 + c\xi + d) \\ &= a^4 + b^4 + c^4 + d^4 + 2a^2c^2 + 2b^2d^2 + 4a^2bd + 4acd^2 - 4ab^2c - 4bc^2d \end{aligned}$$

with $a, b, c, d \in \mathbb{Z}$. We now get the three identities

$$\left.\begin{array}{llll} l = u^2 + v^2 & \text{with}\ \ u = a^2 - c^2 + 2bd & \text{and} & v = d^2 - b^2 + 2ac \\ l = x^2 - 2y^2 & \text{with}\ \ x = a^2 + b^2 + c^2 + d^2 & \text{and} & y = ab - ad + bc + cd \\ l = z^2 + 2w^2 & \text{with}\ \ z = a^2 - b^2 + c^2 - d^2 & \text{and} & w = ab + ad - bc + cd \end{array}\right\} \quad (4.8)$$

So we have showed the (well-known) existence of the three representations (4.3). The conditions (4.4) are easily checked, replacing (a, b, c, d) by $(b, c, d, -a)$ if necessary.

The statements (4.6) and (4.7) follow directly from (4.3) and (4.4).

To show (4.5), first note that v and z are unique modulo change of sign. So the conditions $8 \mid v$ and $z \equiv 1, 7$ (mod 8) are independent of the representations (4.3). The positive fundamental unit of $\mathbb{Q}(\sqrt{2})$ is $3 + 2\sqrt{2}$. So if $l = x^2 - 2y^2$ is one representation with $x > 0$, then all such representations come from the transformation $(x, y) \mapsto (3x \pm 4y, \pm 2x + 3y)$. It follows that the condition $x \equiv 1, 3$ (mod 8) is also independent of the representation (4.4). So to show (4.5), we may assume that the representations (4.3) are of the form (4.8). Notice that a and c must have opposite parity, whereas b and d have the same parity (because u is odd, and v is even). It is now seen that all three conditions of (4.5) are equivalent to

$$4 \mid ac \ \Leftrightarrow\ b^2 \equiv d^2 \text{ (mod 8)}.$$

The last statement of the lemma follows immediately from (4.5), (4.6), and (4.7). □

4.6 The form class group of discriminant $-4l$ for a prime $l \equiv 1 \pmod 4$

Consider a prime $l \equiv 1 \pmod 4$ and put $D = -4l$. Let $\mathscr{C}$ be the group of equivalence classes of positive definite quadratic forms of discriminant D. The class number $h = h(D)$ is the order of $\mathscr{C}$. The 2-part of $\mathscr{C}$ is cyclic and

$$2 \mid h.$$

We investigate when $4 \mid h$ and when $8 \mid h$.

The neutral element in $\mathscr{C}$, i.e. the principal class, is represented by the principal form

$$(1, 0, l) := X^2 + lY^2.$$

The unique element of order 2 in $\mathscr{C}$ is the class represented by the form

$$f = (2, 2, (l + 1)/2).$$

The principal genus of $\mathscr{C}$ is the subgroup of squares $\mathscr{C}^2$. We also say that a form is in the principal genus if its class is. So

$$4 \mid h \;\Leftrightarrow\; f \text{ is in the principal genus.}$$

The assigned characters modulo D are the two Kronecker symbols

$$\left(\frac{-4}{}\right) \quad\text{and}\quad \left(\frac{l}{\cdot}\right).$$

Let m be an arbitrary integer representable by f and with $(m, D) = 1$. Then f is in the principal genus iff the assigned characters $(-4/m)$ and (l/m) are both 1. Since the product of the assigned characters is $(D/m) = 1$, it suffices to compute one of them. The form f clearly represents $m = (l + 1)/2$ which is prime to D. Thus

$$4 \mid h \;\Leftrightarrow\; \left(\frac{-4}{m}\right) = 1 \;\Leftrightarrow\; m \equiv 1 \pmod 4 \;\Leftrightarrow\; l \equiv 1 \pmod 8$$

by quadratic reciprocity. This criterion goes back to Rédei and Reichardt [23].

Henceforth assume $l \equiv 1 \pmod 8$. To see when $8 \mid h$, we construct a form class of order 4 and investigate when it is in the principal genus. We may write

$$l = x^2 - 2y^2 \;\text{ with } x > 0 \tag{4.9}$$

since l splits in the principal ideal domain $\mathbb{Q}(\sqrt{2})$ (or by Lemma 36). Clearly x is odd, y is even, and $(x, y) = 1$.

Consider the form

$$g = (x+y, 2y, x-y) \tag{4.10}$$

which is positive definite of discriminant $4y^2 - 4(x+y)(x-y) = D$. We have the following equivalences of forms:

$$g \sim (x-y, -2y, x+y) \sim (x-y, -2x, 8x+8y) =: g_0$$

where g_0 is "composable" with g (see [8], for instance). Dirichlet composition gives

$$g^2 \sim g \cdot g_0 = (4x^2-4y^2, -2x, 2) \sim (2, 2x, 4x^2-4y^2) \sim (2, 2, (l+1)/2) = f.$$

I.e. g represents a form class of order 4. So

$$8 \mid h \;\Leftrightarrow\; g \text{ is in the principal genus.}$$

Since g represents $x+y$ which is prime to D, we conclude

$$8 \mid h \;\Leftrightarrow\; \left(\frac{-4}{x+y}\right) = 1 \;\Leftrightarrow\; x+y \equiv 1 \pmod 4.$$

This criterion is due to Hasse [13].

Combining the above with Lemma 36 gives the alternative criterion

$$8 \mid h \;\Leftrightarrow\; l \text{ is of the form } X^2 + 32Y^2$$

due to Barrucand and Cohn [2].

The principal class in $\mathscr{C}$ is related to the unique class of order 2 by the following *duplication formula* (as an identity in $\mathbb{Z}[U,V]$):

$$\left(2U^2 + 2UV + \frac{l+1}{2}V^2\right)^2 = X^2 + lY^2$$

with

$$X = 2U^2 + 2UV - \frac{l-1}{2}V^2 \quad \text{and} \quad Y = 2UV + V^2.$$

Now assume that $l \equiv 1 \pmod 8$. Then 4 divides the class number $h(D)$. Write l as in (4.9). Then the form

$$(x+y)S^2 + 2yST + (x-y)T^2$$

has order 4, and we have the duplication formula

$$\big((x+y)S^2 + 2yST + (x-y)T^2\big)^2 = 2U^2 + 2UV + \frac{l+1}{2}V^2 \tag{4.11}$$

with

$$U = ((x-1)/2+y)S^2 + (x+1)ST + ((1-x)/2+y)T^2 \quad \text{and} \quad V = S^2 - 2ST - T^2.$$

4.7 The form class group of discriminant $-8l$ for an odd prime l

Let l be an odd prime and put $D' = -8l$. Consider the group $\mathscr{C}'$ of equivalence classes of positive definite quadratic forms of discriminant D'. The class number $h' = h(D')$ is the order of $\mathscr{C}'$. The 2-part of $\mathscr{C}'$ is cyclic and

$$2 \mid h'.$$

We give criteria for $4 \mid h'$ and $8 \mid h'$.

The principal form

$$(1, 0, 2l)$$

represents the principal class in $\mathscr{C}'$. The unique element of order 2 in $\mathscr{C}'$ is the class represented by the form

$$f' := (2, 0, l).$$

So

$$4 \mid h' \;\Leftrightarrow\; f' \text{ is in the principal genus.}$$

The assigned characters modulo D' are the two Kronecker symbols

$$\left(\frac{d_1}{-}\right) \quad \text{and} \quad \left(\frac{d_2}{-}\right)$$

where

$$d_1 = (-1)^{(l+1)/2} 8 \quad \text{and} \quad d_2 = l^* = (-1)^{(l-1)/2} l.$$

The form f' clearly represents $2 + l$ which is prime to D'. Thus

$$4 \mid h' \;\Leftrightarrow\; \left(\frac{2}{l}\right) = \left(\frac{d_2}{2+l}\right) = 1 \;\Leftrightarrow\; l \equiv 1, 7 \pmod 8).$$

by quadratic reciprocity. This criterion is due to Rédei and Reichardt [23].

Henceforth assume $l \equiv 1, 7 \pmod 8$. Then we again have a representation (4.9). Clearly x is odd and prime to y.

Consider the form

$$g' = (x, 4y, 2x) \tag{4.12}$$

which is positive definite of discriminant $16y^2 - 8x^2 = D'$. Composition of forms gives

$$g' \cdot g' = (x^2, 4y, 2) \sim (2, -4y, x^2) \sim (2, 0, l).$$

I.e. g' represents a form class of order 4. So

$$8 \mid h' \;\Leftrightarrow\; g' \text{ is in the principal genus.}$$

Since g' represents x which is prime to D',

$$8 \mid h' \;\Leftrightarrow\; \left(\frac{d_1}{x}\right) = 1.$$

If $l \equiv 7 \pmod 8$, then $d_1 = 8$ and

$$\left(\frac{8}{x}\right) = 1 \;\Leftrightarrow\; x \equiv 1, 7 \pmod 8 \;\Leftrightarrow\; l \equiv 15 \pmod{16}$$

where the last implication follows elementarily from (4.9). If $l \equiv 1 \pmod 8$, then $d_1 = -8$ and

$$\left(\frac{-8}{x}\right) = 1 \;\Leftrightarrow\; x \equiv 1, 3 \pmod 8.$$

We conclude

$$8 \mid h' \;\Leftrightarrow\; \begin{cases} l \equiv 15 \pmod{16} & \text{for } l \equiv 7 \pmod 8, \\ x \equiv 1, 3 \pmod 8 & \text{for } l \equiv 1 \pmod 8. \end{cases}$$

This criterion is due to Hasse [14]. Combining this with Lemma 36 gives an alternative criterion when $l \equiv 1 \pmod 8$:

$$8 \mid h' \;\Leftrightarrow\; l \text{ is of the form } X^2 + 64Y^2.$$

Hasse credits Barrucand for deducing this alternative criterion from his own[1].

The principal class in $\mathscr{C}'$ is related to the unique class of order 2 by the following duplication formula

$$\left(2U^2 + lV^2\right)^2 = X^2 + 2lY^2$$

with

$$X = 2U^2 - lV^2 \quad \text{and} \quad Y = 2UV.$$

Now assume that $l \equiv 1, 7 \pmod 8$. Then 4 divides the class number $h' = h(D')$. Write l as in (4.9). Then the form

$$xS^2 + 4yST + 2xT^2$$

has order 4, and we have the duplication formula

$$\left(xS^2 + 4yST + 2xT^2\right)^2 = 2U^2 + lV^2$$

with

$$U = yS^2 + 2xST + 2yT^2 \quad \text{and} \quad V = S^2 - 2T^2.$$

[1] There is a typo in the statement, however, so that the relevant form erroneously appears to be $X^2 + 16Y^2$.

4.8 The form class group of discriminant $-ll'$ with two primes l, l'

Let l, l' be primes with $l \equiv 1 \pmod 4$ and $l' \equiv 3 \pmod 4$ and put $D'' = -ll'$. The principal form of discriminant D'' is

$$\left(1, 1, \frac{ll'+1}{4}\right).$$

The form

$$f'' = \left(l, l, \frac{l+l'}{4}\right)$$

represents the unique class of order 2. The assigned characters modulo D'' are $(l/\cdot)$ and $(-l'/\cdot)$. Since f'' represents $m = (l+l')/4$, we get the following criterion for the class number $h'' = h(D'')$:

$$4 \mid h'' \;\Leftrightarrow\; (l/m) = 1 \;\Leftrightarrow\; (l/l') = 1.$$

Hasse gives in [15] a criterion for $8 \mid h''$ analogous to the criteria for $8 \mid h$ and $8 \mid h'$. However it seems not possible to display a "canonical" form of order 4 and thus giving an alternative proof of Hasse's criterion in this case.

The principal class of discriminant D'' is related to the class of order 2 by the duplication formula

$$\left(lU^2 + lUV + \frac{l+l'}{4}V^2\right)^2 = X^2 + XY + \frac{ll'+1}{4}Y^2$$

with

$$X = lU^2 + (l-1)UV + \frac{l-l'-2}{4}V^2 \quad \text{and} \quad Y = (2U+V)V.$$

4.9 The fields $\mathbb{Q}(\sqrt{-l})$ with an odd prime l

Let $K = \mathbb{Q}(\sqrt{-l})$ with an odd prime l. The 2-class group of K is cyclic (possibly trivial), and we write its order as 2^μ. There holds

$$\mu \geq 1 \;\Leftrightarrow\; l \equiv 1 \pmod 4.$$

In case $l \equiv 1 \pmod 4$, K's genus field

$$K_{\text{gen}} = K(\sqrt{-1})$$

is the first step of the 2-class field. From section 4.6 we have

$$\mu \geq 2 \;\Leftrightarrow\; l \equiv 1 \pmod 8$$

and

$$\mu \geq 3 \ \Leftrightarrow \ l \text{ is of the form } x^2 + 32y^2$$

We give first an algorithm that determines ν and $K_{\text{anti}}^{(1)}$. We then use this algorithm to give an explicit expression for ν and $K_{\text{anti}}^{(1)}$ in most cases.

THEOREM 37. *Consider the field $K = \mathbb{Q}(\sqrt{-l})$ with a prime $l \equiv 1 \pmod 4$. Pick a prime p with $p \equiv 3 \pmod 4$ and $(-l/p) = 1$. Write*

$$p^h = X^2 + lY^2$$

with relatively prime $X, Y \in \mathbb{Z}$ and let $t = v_2(X)$ be the dyadic valuation of X.

If $t < \mu + 1$, then the number of unramified steps of K_{anti} is

$$\nu = \mu + 1 - t > 0,$$

and the first step is $K_{anti}^{(1)} = K(\sqrt{-1})$.

If $t = \mu + 1$, then the number of unramified steps of K_{anti} is $\nu = 0$, and the first step is

$$K_{anti}^{(1)} = \begin{cases} K(\sqrt{2}) & \textit{if } p \equiv 3 \pmod 8 \\ K(\sqrt{-2}) & \textit{if } p \equiv 7 \pmod 8 \end{cases}$$

If $t > \mu + 1$, then the number of unramified steps of K_{anti} is $\nu = 0$, and the first step is

$$K_{anti}^{(1)} = \begin{cases} K(\sqrt{-2}) & \textit{if } p \equiv 3 \pmod 8 \\ K(\sqrt{2}) & \textit{if } p \equiv 7 \pmod 8 \end{cases}$$

Proof. By assumption p is inert in $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{l})$, whereas $p = \mathfrak{p}\mathfrak{q}$ splits in K. The 2-class field of K is cyclic, and $\mathfrak{p}$ is inert in it because $\mathfrak{p}$ is inert in its first step $K(\sqrt{-1})/K$.

It follows from Theorem 34 (or rather from Remark 35 (a)) that p splits in $K_{\text{anti}}^{(n)}$ iff $t \geq n + \mu - \nu + 1$. In particular $t \geq \mu - \nu + 1$.

If $\nu \geq 1$, then $\mathfrak{p}$ is inert in $K_{\text{anti}}^{(1)} = K(\sqrt{-1})$ and hence $t = \mu - \nu + 1 < \mu + 1$. If on the other hand $\nu = 0$, then $t \geq \mu + 1$. From this follows the determination of ν.

Further, if $t = \mu + 1$, then $\mathfrak{p}$ is inert in $K_{\text{anti}}^{(1)} = K(\sqrt{a})$ where $a \in \{2, -2\}$. Since p is inert in $\mathbb{Q}(\sqrt{a})$, we have $(a/p) = -1$ which determines a.

Finally, if $t > \mu + 1$, then $\mathfrak{p}$ splits in $K_{\text{anti}}^{(1)} = K(\sqrt{a})$ where still $a \in \{2, -2\}$. Since p now splits in $\mathbb{Q}(\sqrt{a})$, we have $(a/p) = 1$ which again determines a. □

THEOREM 38. *Let $K = \mathbb{Q}(\sqrt{-l})$ with an odd prime l. The number of unramified* *steps of K_{anti} satisfies*

$$\nu = \begin{cases} 0 & \text{for } l \equiv 3 \ (\mathit{mod}\ 4), \\ 1 & \text{for } l \equiv 5 \ (\mathit{mod}\ 8), \\ 0 & \text{for } l \equiv 1 \ (\mathit{mod}\ 8) \text{ and } \mu = 2, \\ \mu - 2 & \text{for } l \equiv 9 \ (\mathit{mod}\ 16) \text{ and } \mu \geq 3, \\ 0 & \text{for } l \equiv 1 \ (\mathit{mod}\ 16) \text{ and } \mu = 3, \\ 0, \ldots, \mu - 3 & \text{for } l \equiv 1 \ (\mathit{mod}\ 16) \text{ and } \mu \geq 4. \end{cases}$$

Proof. The theorem is clear for $l \equiv 3 \pmod 4$ since then $\mu = 0$. So assume $l \equiv 1 \pmod 4$ and thus $\mu \geq 1$. Pick a prime p satisfying the conditions of Theorem 37. Then $p = \mathfrak{p}\mathfrak{q}$ splits in K, and the order of $\mathfrak{p}$ in K's class group is divisible by 2^μ (since $\mathfrak{p}$ is inert in K's 2-class field). Write

$$p^h = X^2 + lY^2 \tag{4.13}$$

with relatively prime $X, Y \in \mathbb{Z}$ and put $t = v_2(X)$. Then

$$\nu = \max\{\mu + 1 - t, 0\}$$

by Theorem 37. Necessarily

$$t \geq 1,$$

so X is even, and Y is odd (this also follows directly from Remark 35(a)). Note that $p^h \equiv 1 \pmod 8$ since h is even. If $l \equiv 5 \pmod 8$, then (4.13) gives $1 \equiv X^2 + 5 \pmod 8$. This implies $4 \nmid X$, i.e. $t = 1$ and thus $\nu = \mu = 1$.

Now assume $l \equiv 1 \pmod 8$ and thus $\mu \geq 2$. The ideal power $\mathfrak{p}^{h/2}$ has order 2 in the class group. Hence $p^{h/2}$ is primitively representable by a form of order 2 in the class group. We know from section 4.6 that $(2, 2, (l+1)/2)$ is a such form, i.e.

$$p^{h/2} = 2U^2 + 2UV + \frac{l+1}{2}V^2$$

with some relatively prime $U, V \in \mathbb{Z}$. Clearly V is odd. Note that $p^{h/2} \equiv 1 \pmod 8$ since $4 \mid h$. The duplication formula from section 4.6 gives the primitive representation

$$p^h = \left(2U^2 + 2UV + \frac{l+1}{2}V^2\right)^2 = \left(2U^2 + 2UV - \frac{l-1}{2}V^2\right)^2 + l\left(2UV + V^2\right)^2$$

and thus

$$X = 2U^2 + 2UV - \frac{l-1}{2}V^2 = p^{h/2} - lV^2. \tag{4.14}$$

This expression implies $X \equiv 1 - V^2 \equiv 0 \pmod 8$ and therefore

$$t \geq 3.$$

This proves the theorem when $\mu = 2$.

Finally assume $l \equiv 1 \pmod 8$ and $\mu \geq 3$. We must show

$$16 \mid X \;\Leftrightarrow\; l \equiv 1 \pmod{16}. \tag{4.15}$$

Note that $p^{h/2} \equiv 1 \pmod{16}$ and therefore $X \equiv 1 - lV^2 \pmod{16}$ by (4.14). So (4.15) amounts to showing

$$V^2 \equiv 1 \pmod{16} \tag{4.16}$$

or, equivalently, $V \equiv 1, 7 \pmod 8$. We can write $l = x^2 - 2y^2$ with $x > 0$ odd and y even by Lemma 36. (Actually Hasse's criterion gives $x + y \equiv 1 \pmod 4$ since $8 \mid h$, but we don't need this). By the same argument as above, $p^{h/4}$ is primitively representable by a form of order 4 in the form class group. We have earlier found that $(x + y, 2y, x - y)$ is a such form and therefore get

$$p^{h/4} = (x + y)S^2 + 2yST + (x - y)T^2 \tag{4.17}$$

with relatively prime $S, T \in \mathbb{Z}$. It is clear from (4.17) that S and T have opposite parity. Using the duplication formula (4.11) shows

$$V = S^2 - 2ST - T^2. \tag{4.18}$$

Now $V \equiv 1, 7$ (mod 8) follows from (4.18) and the fact that S and T have opposite parity, and we are done. □

Corollary 39. *Let $K = \mathbb{Q}(\sqrt{-l})$ with an odd prime l. Regarding K's ring class field of conductor 2^∞, we have*

$$Gal(N(2^\infty)/K) \cong \begin{cases} \mathbb{Z}_2 \times \mathbb{Z}/2 \times U & \text{for } l \equiv 3, 5, 7 \ (mod\ 8), \\ \mathbb{Z}_2 \times \mathbb{Z}/8 \times U & \text{for } l \equiv 1 \ (mod\ 8) \text{ and } \mu = 2, \\ \mathbb{Z}_2 \times \mathbb{Z}/8 \times U & \text{for } l \equiv 9 \ (mod\ 16) \text{ and } \mu \geq 3, \\ \mathbb{Z}_2 \times \mathbb{Z}/2^t \times U & \text{for } l \equiv 1 \ (mod\ 16) \text{ and } \mu \geq 3, \end{cases}$$

where U is either the non-2-part of K's class group, or a triple cover thereof. In the last case t is an integer with $4 \leq t \leq \mu + 1$. □

Proof. $\mathrm{Gal}(N(2^\infty)/K_H)$ is isomorphic to either $\mathbb{Z}_2 \times \mathbb{Z}/2$ or $\mathbb{Z}_2 \times \mathbb{Z}/6$ by Lemma 33. By definition, $\mathrm{Gal}(K_H/K) \cong \mathbb{Z}/2^\mu \times$ (non-2-part). The 2-rank of $\mathrm{Gal}(N(2^\infty)/K)$

is $r+1=2$ by section 4.3. This gives $\mathrm{Gal}(N(2^\infty)/K) \cong \mathbb{Z}_2 \times \mathbb{Z}/2^{\mu+1-\nu} \times U$, and the corollary follows from Theorem 38. □

The first step of K's anti-cyclotomic extension is contained in $K_{\text{elem}} = K(\sqrt{-1}, \sqrt{2})$ by section 4.3. Hence it is of the form $K = \mathbb{Q}(\sqrt{a})$ with $a \in \{-1, 2, -2\}$. Prime decomposition allows us to determine a for $l \not\equiv 1 \pmod 8$.

Theorem 40. *Consider the field $K = \mathbb{Q}(\sqrt{-l})$ with an odd prime $l \not\equiv 1 \pmod 8$. Then the first step of the anti-cyclotomic extension is*

$$K_{\text{anti}}^{(1)} = \begin{cases} K(\sqrt{-2}) & \text{if } l \equiv 3 \pmod 8, \\ K(\sqrt{-1}) & \text{if } l \equiv 5 \pmod 8, \\ K(\sqrt{2}) & \text{if } l \equiv 7 \pmod 8. \end{cases}$$

Proof. Since $l = \mathfrak{l}^2$ ramifies in K, $\mathfrak{l}$ splits in K_{anti}, and therefore $(a/l) = 1$. This determines a whenever $l \not\equiv 1 \pmod 8$. □

When $l \equiv 1 \pmod 8$, using Theorem 37 and Theorem 38 gives the following partial result:

Theorem 41. *Consider the field $K = \mathbb{Q}(\sqrt{-l})$ with a prime $l \equiv 1 \pmod 8$. Then the first step of the anti-cyclotomic extension is*

$$K_{\text{anti}}^{(1)} = \begin{cases} K(\sqrt{-2}) & \text{if } l \equiv 9 \pmod{16} \text{ and } \mu = 2, \\ K(\sqrt{-1}) & \text{if } l \equiv 9 \pmod{16} \text{ and } \mu \geq 3, \\ K(\sqrt{2}) & \text{if } l \equiv 1 \pmod{16} \text{ and } \mu = 2, \\ K(\sqrt{2}), K(\sqrt{-2}) & \text{if } l \equiv 1 \pmod{16} \text{ and } \mu = 3, \\ K(\sqrt{-1}), K(\sqrt{2}), K(\sqrt{-2}) & \text{if } l \equiv 1 \pmod{16} \text{ and } \mu \geq 4. \end{cases}$$

Proof. If $l \equiv 9 \pmod{16}$ and $\mu \geq 3$, then $\nu > 0$ by Theorem 38 and hence $K_{\text{anti}}^{(1)} = K_{\text{gen}} = K(\sqrt{-1})$.

If $l \equiv 1 \pmod{16}$ and $\mu = 3$, then $\nu = 0$ by Theorem 38 and hence $K_{\text{anti}}^{(1)} \neq K(\sqrt{-1})$.

Finally assume $\mu = 2$. Then Theorem 38 again gives $K_{\text{anti}}^{(1)} \neq K(\sqrt{-1})$, but we can say more than this. Pick a prime $p \equiv 7 \pmod 8$ as in Theorem 37. Then $p^{h/2} \equiv 1 \pmod{16}$. The proof of Theorem 38 shows $t \geq 3$ and

$$t \geq 4 \;\Leftrightarrow\; l \equiv 1 \pmod{16}.$$

Theorem 37 now gives the claim. □

Theorem 40 and Theorem 41 are proved samewhat differently in [12].

4.10 The fields $\mathbb{Q}(\sqrt{-2l})$ with an odd prime l

Let $K = \mathbb{Q}(\sqrt{-2l})$ with an odd prime l. The 2-class group of K is cyclic of order 2^μ with $\mu \geq 1$ (see the section 4.7). The first step of K's 2-class field is its genus field

$$K_{\text{gen}} = \begin{cases} K(\sqrt{-2}) & \text{if } l \equiv 1 \pmod 4, \\ K(\sqrt{2}) & \text{if } l \equiv 3 \pmod 4. \end{cases}$$

We give first an algorithm that determines ν and $K_{\text{anti}}^{(1)}$. We then use this algorithm to give an explicit expression for ν and $K_{\text{anti}}^{(1)}$ in most cases.

Theorem 42. *Consider the field $K = \mathbb{Q}(\sqrt{-2l})$ with an odd prime l. Pick a prime p with $(-2l/p) = 1$ and*

$$p \equiv \begin{cases} 5,7 \ (\textit{mod}\ 8) & \textit{if } l \equiv 1 \ (\textit{mod}\ 4) \\ 3,5 \ (\textit{mod}\ 8) & \textit{if } l \equiv 3 \ (\textit{mod}\ 4) \end{cases}$$

Write

$$p^h = X^2 + 2lY^2$$

with relatively prime $X, Y \in \mathbb{Z}$ and let $t = v_2(Y)$ be the dyadic valuation of Y.

If $t < \mu$, then the number of unramified steps of K_{anti} is $\nu = \mu - t > 0$, and the first step is

$$K_{anti}^{(1)} = \begin{cases} K(\sqrt{-2}) & \textit{if } l \equiv 1 \ (\textit{mod}\ 4) \\ K(\sqrt{2}) & \textit{if } l \equiv 3 \ (\textit{mod}\ 4) \end{cases}$$

If $t = \mu$, then the number of unramified steps of K_{anti} is $\nu = 0$, and the first step is

$$K_{anti}^{(1)} = \begin{cases} K(\sqrt{-1}) & \textit{if } p \equiv 3,7 \ (\textit{mod}\ 8) \\ K(\sqrt{2}) & \textit{if } p \equiv 5 \ (\textit{mod}\ 8),\ l \equiv 1 \ (\textit{mod}\ 4) \\ K(\sqrt{-2}) & \textit{if } p \equiv 5 \ (\textit{mod}\ 8),\ l \equiv 3 \ (\textit{mod}\ 4) \end{cases}$$

If $t > \mu$, then the number of unramified steps of K_{anti} is $\nu = 0$, and the first step is

$$K_{anti}^{(1)} = \begin{cases} K(\sqrt{-1}) & \textit{if } p \equiv 5 \ (\textit{mod}\ 8) \\ K(\sqrt{2}) & \textit{if } p \equiv 7 \ (\textit{mod}\ 8) \\ K(\sqrt{-2}) & \textit{if } p \equiv 3 \ (\textit{mod}\ 8) \end{cases}$$

Proof. By assumption p splits in K ($p = \mathfrak{p}\mathfrak{q}$). The 2-class field of K is cyclic, and $\mathfrak{p}$ is inert in it because $\mathfrak{p}$ is inert in its first step $K(\sqrt{\pm 2})/K$.

It follows from Theorem 34 that p splits in $K_{\text{anti}}^{(n)}$ iff $t \geq n+\mu-\nu$. In particular $t \geq \mu - \nu$.

If $\nu \geq 1$, then $\mathfrak{p}$ is inert in $K_{\text{anti}}^{(1)} = K(\sqrt{\pm 2})$ and hence $t = \mu - \nu < \mu$. If on the other hand $\nu = 0$, then $t \geq \mu$. From this follows the determination of ν.

Further, if $t = \mu$, then $\mathfrak{p}$ is inert in $K_{\text{anti}}^{(1)} = K(\sqrt{a})$. Since p is inert in $\mathbb{Q}(\sqrt{a})$, we have $(a/p) = -1$ which determines a.

Finally, if $t > \mu$, then $\mathfrak{p}$ splits in $K_{\text{anti}}^{(1)} = K(\sqrt{a})$. Since p now splits in $\mathbb{Q}(\sqrt{a})$, we have $(a/p) = 1$ which again determines a. □

Theorem 43. *Let $K = \mathbb{Q}(\sqrt{-2l})$ with an odd prime l. The number of unramified steps of K_{anti} satifies*

$$\nu = \begin{cases} 0 & \text{for } l \equiv 3, 5 \ (\text{mod } 8), \\ \mu - 1 & \text{for } l \equiv 7 \ (\text{mod } 8), \\ 0 & \text{for } l \equiv 1 \ (\text{mod } 8) \text{ and } \mu = 2, \\ \mu - 2 & \text{for } l \equiv 9 \ (\text{mod } 16) \text{ and } \mu \geq 3, \\ 0 & \text{for } l \equiv 1 \ (\text{mod } 16) \text{ and } \mu = 3, \\ 0, \ldots, \mu - 3 & \text{for } l \equiv 1 \ (\text{mod } 16) \text{ and } \mu \geq 4. \end{cases}$$

Proof. Pick a prime p satisfying the conditions of Theorem 42. Then $p = \mathfrak{p}\mathfrak{q}$ splits in K, and the order of $\mathfrak{p}$ in K's class group is divisible by 2^μ since $\mathfrak{p}$ is inert in the 2-class field. We write

$$p^h = X^2 + 2lY^2$$

with relatively prime integers X, Y and put $t = v_2(Y)$. Then

$$\nu = \max\{\mu - t, 0\}$$

by Theorem 42. Computing modulo 4 shows that X is odd, Y is even, and thus

$$t \geq 1.$$

So for $l \equiv 3, 5 \pmod 8$ we are done since then $\mu = 1$.

Assume $l \equiv 1, 7 \pmod 8$. Then $\mu \geq 2$ by section 4.7. The ideal power $\mathfrak{p}^{h/2}$ has order 2 in the class group. Hence we can primitively represent $p^{h/2}$ by a form of order 2 in the form class group:

$$p^{h/2} = 2U^2 + lV^2.$$

Clearly V is odd, and U is even iff $l \equiv 1 \pmod{8}$. Composition of forms gives the primitive representation

$$p^h = (U^2 - 2lV^2)^2 + 2l(2UV)^2.$$

So we may assume $Y = 2UV$. This gives

$$t \geq 2 \;\Leftrightarrow\; l \equiv 1 \pmod{8}.$$

The claim follows unless $l \equiv 1 \pmod{8}$ and $\mu \geq 3$.

Now assume $l \equiv 1 \pmod{8}$ and $\mu \geq 3$. Then we can write

$$l = x^2 - 2y^2$$

with

$$x > 0\ , \quad x \equiv 1, 3 \pmod{8}\ , \quad y \text{ even}$$

by section refsectionfem. By the same argument as above, $p^{h/4}$ is primitively representable by a form of order 4 in the form class group. We have earlier found that $(x, 4y, 2x)$ is a such form, and therefore get

$$p^{h/4} = xS^2 + 4yST + 2xT^2.$$

One sees that S is odd, and that T is even iff $x \equiv 1 \pmod{8}$.

The duplication formula gives

$$p^{h/2} = 2(yS^2 + 2xST + 2yT^2)^2 + l(S^2 - 2T^2)^2.$$

So we may assume

$$U = yS^2 + 2xST + 2yT^2.$$

If $l \equiv 1 \pmod{16}$, then

$$x \equiv 1 \pmod{8} \;\Leftrightarrow\; 4 \mid y \;\Leftrightarrow\; T \text{ even},$$

showing $4 \mid U$ and hence

$$t \geq 3. \tag{4.19}$$

If $l \equiv 9 \pmod{16}$, then

$$x \equiv 1 \pmod{8} \;\Leftrightarrow\; 4 \nmid y \;\Leftrightarrow\; T \text{ even},$$

showing $4 \nmid U$ and hence

$$t = 2.$$

This finishes the proof. □

Similarly to Corollary 39, we get:

Corollary 44. *Let $K = \mathbb{Q}(\sqrt{-2l})$ with an odd prime l. Regarding K's ring class field of conductor 2^∞, we have*

$$Gal(N(2^\infty)/K) \cong \begin{cases} \mathbb{Z}_2 \times \mathbb{Z}/2 \times U & \text{for } l \equiv 3,5,7 \ (mod\ 8), \\ \mathbb{Z}_2 \times \mathbb{Z}/4 \times U & \text{for } l \equiv 1 \ (mod\ 8) \text{ and } \mu = 2, \\ \mathbb{Z}_2 \times \mathbb{Z}/4 \times U & \text{for } l \equiv 9 \ (mod\ 16) \text{ and } \mu \geq 3, \\ \mathbb{Z}_2 \times \mathbb{Z}/2^t \times U & \text{for } l \equiv 1 \ (mod\ 16) \text{ and } \mu \geq 3, \end{cases}$$

where U is the non-2-part of K's class group. In the last case t is an integer with $3 \leq t \leq \mu$. □

As in the previous section, the first step of the anti-cyclotomic extension is of the form $K(\sqrt{a})$ with $a \in \{-1, 2, -2\}$, and using that l ramifies in K and thus $(a/l) = 1$ determines a when $l \not\equiv 1 \pmod 8$:

Theorem 45. *Consider the field $K = \mathbb{Q}(\sqrt{-2l})$ with an odd prime $l \not\equiv 1 \ (mod\ 8)$. Then the first step of the anti-cyclotomic extension is*

$$K^{(1)}_{\text{anti}} = \begin{cases} K(\sqrt{-2}) & \text{if } l \equiv 3 \ (mod\ 8), \\ K(\sqrt{-1}) & \text{if } l \equiv 5 \ (mod\ 8), \\ K(\sqrt{2}) & \text{if } l \equiv 7 \ (mod\ 8). \ \square \end{cases}$$

When $l \equiv 1 \pmod 8$, using Theorem 42 and Theorem 43 gives the following partial result:

Theorem 46. *Consider the field $K = \mathbb{Q}(\sqrt{-2l})$ with an odd prime $l \equiv 1 \ (mod\ 8)$. Then the first step of the anti-cyclotomic extension is*

$$K^{(1)}_{\text{anti}} = \begin{cases} K(\sqrt{-1}) & \text{if } l \equiv 9 \ (mod\ 16) \text{ and } \mu = 2, \\ K(\sqrt{-2}) & \text{if } l \equiv 9 \ (mod\ 16) \text{ and } \mu \geq 3, \\ K(\sqrt{2}) & \text{if } l \equiv 1 \ (mod\ 16) \text{ and } \mu = 2, \\ K(\sqrt{-1}), K(\sqrt{2}) & \text{if } l \equiv 1 \ (mod\ 16) \text{ and } \mu = 3, \\ K(\sqrt{-1}), K(\sqrt{2}), K(\sqrt{-2}) & \text{if } l \equiv 1 \ (mod\ 16) \text{ and } \mu \geq 4. \end{cases}$$

Proof. If $l \equiv 9 \pmod{16}$ and $\mu \geq 3$, then $\nu > 0$ by Theorem 43 and hence $K^{(1)}_{\text{anti}} = K_{\text{gen}} = K(\sqrt{-2})$.

If $l \equiv 1 \pmod{16}$ and $\mu = 3$, then $\nu = 0$ by Theorem 43 and hence $K^{(1)}_{\text{anti}} \neq K(\sqrt{-2})$.

Finally assume $\mu = 2$. Then Theorem 43 again gives $K^{(1)}_{\text{anti}} \neq K(\sqrt{-2})$, but we can say more than this. Pick a prime $p \equiv 5 \pmod 8$ as in Theorem 42. Then $p^{h/4} \equiv 5 \pmod 8$. The same type of argument as in the proof of Theorem 43 shows $t \geq 3$ when $l \equiv 9 \pmod{16}$, and $t = 2$ when $l \equiv 1 \pmod{16}$. Theorem 42 gives the claim. □

Theorem 45 and Theorem 46 are proved samewhat differently in [12].

4.11 The fields $\mathbb{Q}(\sqrt{-ll'})$ with two primes $l \equiv 1 \pmod 4$ and $l' \equiv 3 \pmod 4$

Let $K = \mathbb{Q}(\sqrt{ll'})$ with two primes $l \equiv 1 \pmod 4$ and $l' \equiv 3 \pmod 4$. Note that the following Legendre symbols are equal:

$$\left(\frac{l}{l'}\right) = \left(\frac{l'}{l}\right).$$

The 2-class group of K is cyclic of order 2^{μ} with $\mu \geq 1$ (section 4.8). The first step of K's 2-class field is its genus field

$$K_{\text{gen}} = K(\sqrt{l}).$$

Theorem 47. *Consider the field $K = \mathbb{Q}(\sqrt{-ll'})$ with primes $l \equiv 1 \pmod 4$ and $l' \equiv 3 \pmod 4$. Pick an odd prime p with $(l/p) = (-l'/p) = -1$. Write*

$$X^2 + XY + \frac{ll'+1}{4}Y^2 = \begin{cases} p^{2h} & \textit{if } ll' \equiv 7 \pmod 8, \\ p^{6h} & \textit{if } ll' \equiv 3 \pmod 8, \end{cases}$$

with relatively prime $X, Y \in \mathbb{Z}$, and let $t = v_2(Y)$ be the dyadic valuation of Y.

If $t < \mu + 3$, then the number of unramified steps of K_{anti} is $\nu = \mu + 3 - t > 0$, and the first step is $K^{(1)}_{anti} = K(\sqrt{l})$.

If $t = \mu + 3$, then the number of unramified steps of K_{anti} is $\nu = 0$, and the *first step is one of two possibilities:*

$$K_{anti}^{(1)} = \begin{cases} K(\sqrt{2l}), K(\sqrt{-2l}) & \text{if } p \equiv 1 \ (mod\ 8) \\ K(\sqrt{2}), K(\sqrt{-2l}) & \text{if } p \equiv 3 \ (mod\ 8) \\ K(\sqrt{2}), K(\sqrt{-2}) & \text{if } p \equiv 5 \ (mod\ 8) \\ K(\sqrt{-2}), K(\sqrt{2l}) & \text{if } p \equiv 7 \ (mod\ 8) \end{cases}$$

If $t > \mu + 3$, then the number of unramified steps of K_{anti} is $\nu = 0$, and the first step is one of two possibilities:

$$K_{anti}^{(1)} = \begin{cases} K(\sqrt{2}), K(\sqrt{-2}) & \text{if } p \equiv 1 \ (mod\ 8) \\ K(\sqrt{-2}), K(\sqrt{2l}) & \text{if } p \equiv 3 \ (mod\ 8) \\ K(\sqrt{2l}), K(\sqrt{-2l}) & \text{if } p \equiv 5 \ (mod\ 8) \\ K(\sqrt{2}), K(\sqrt{-2l}) & \text{if } p \equiv 7 \ (mod\ 8) \end{cases}$$

Proof. It follows from the assumptions that $p = \mathfrak{p}\mathfrak{q}$ splits in K. Since p is inert in $\mathbb{Q}(\sqrt{l})$, $\mathfrak{p}$ is inert in $K_{\text{gen}} = K(\sqrt{l})$ and hence in the entire 2-class field. By Theorem 34, p splits in $K_{\text{anti}}^{(n)}$ iff $t \geq n + \mu - \nu + 3$. In particular $t \geq \mu - \nu + 3$.

If $\nu \geq 1$, then $\mathfrak{p}$ is inert in $K_{\text{anti}}^{(1)} = K(\sqrt{l})$, and so $t = \mu - \nu + 3 < \mu + 3$. If $\nu = 0$, then $t \geq \mu + 3$. This allows to compute ν from t.

$K_{\text{anti}}^{(1)}$ is contained in $K(\sqrt{-1}, \sqrt{2}, \sqrt{l})$ and hence of the form $K(\sqrt{a})$ with a unique $a \in \{-1, 2, -2, l, -l, 2l, -2l\}$. Since l' ramifies in K, it splits in $\mathbb{Q}(\sqrt{a})$ and so $(a/l') = 1$. This gives $a \neq -1$. Similarly one sees $a \neq -l$. If $\nu = 0$, then $a \neq l$. If $t = \mu + 3$, then $\mathfrak{p}$ is inert in $K(\sqrt{a})$ and hence $(a/p) = -1$. If $t > \mu + 3$, then similarly $(a/p) = 1$. Using all of the above information leaves only the stated possibilities for a. □

Theorem 48. *Let $K = \mathbb{Q}(\sqrt{-ll'})$ with primes $l \equiv 1 \ (mod\ 4)$ and $l' \equiv 3 \ (mod\ 4)$. If $(l/l') = -1$, the number of unramified steps of K_{anti} is*

$$\nu = 0.$$

If $(l/l') = 1$, then

$$\nu = \begin{cases} \mu - 1 & \text{for } l \equiv 5 \ (mod\ 8), \\ 0, \ldots, \mu - 2 & \text{for } l \equiv 1 \ (mod\ 8). \end{cases}$$

Proof. We may write

$$p^{h/2} = lS^2 + lST + \frac{l + l'}{4} T^2. \tag{4.20}$$

Then

$$p^h = U^2 + UV + \frac{ll'+1}{4}V^2$$

with $U = lS^2 + (l-1)ST + ((l-l'-2)/4)T^2$ and $V = (2S+T)T$. Now by Remark 35 we get an expression of p^{2h} or p^{6h} as

$$X^2 + XY + \frac{ll'+1}{4}Y^2$$

where $Y = V(2U+V)$ if $ll' \equiv 7 \pmod 8$, and

$$Y = V(2U+V)\left(U^2 + UV + \frac{1-3ll'}{4}V^2\right)\left(3U^2 + 3UV + \frac{3-ll'}{4}V^2\right)$$

if $ll' \equiv 3 \pmod 8$. We must show

$$16 \mid Y, \text{ and } \ 32 \mid Y \ \Leftrightarrow \ l \equiv 1 \pmod 8. \tag{4.21}$$

This can be done by brute force as follows: Let S, T run through all residue classes modulo 32, and let l, l' run through all residue classes modulo 128 such that $l \equiv 1 \pmod 4$ and $l' \equiv 3 \pmod 4$. If (4.20) is $\equiv 1 \pmod 8$, compute Y and check (4.21). □

The statement of Theorem 48 is somewhat less detailed than the analogous theorems 38 and 43. Numerical examples suggest that Theorem 48 can in fact not be refined. This is perhaps "caused" by the absence of a "canonical" form of order 4, as discussed at the end of section 4.8.

Similarly to Corollary 39, we get:

Corollary 49. *Let $K = \mathbb{Q}(\sqrt{-ll'})$ with two primes $l \equiv 1$ (mod 4) and $l' \equiv 3$ (mod 4). Regarding K's ring class field of conductor 2^∞, we have*

$$\mathit{Gal}(N(2^\infty)/K) \cong \begin{cases} \mathbb{Z}_2 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \times U & \text{for } (l/l') = -1 \text{ or } l \equiv 5 \ (\text{mod } 8), \\ \mathbb{Z}_2 \times \mathbb{Z}/2^t \times \mathbb{Z}/2 \times U & \text{for } (l/l') = 1 \text{ and } l \equiv 1 \ (\text{mod } 8), \end{cases}$$

where U is either the non-2-part of K's class group, or a triple cover thereof. In the last case t is an integer with $2 \le t \le \mu$. □

The first step of K's anti-cyclotomic extension is contained in $K_{\text{elem}} = K(\sqrt{-1}, \sqrt{2}, \sqrt{l})$ (see section 4.3). Hence it is of the form $K(\sqrt{a})$ with an $a \in \{-1, 2, -2, l, -l, 2l, -2l\}$.

Theorem 50. *Consider the field $K = \mathbb{Q}(\sqrt{-ll'})$ with primes $l \equiv 1 \pmod 4$ and $l' \equiv 3 \pmod 4$. If $(l/l') = 1$, then the first step of K's anti-cyclotomic extension satifies*

$$K_{\text{anti}}^{(1)} = \begin{cases} K(\sqrt{-2}), K(\sqrt{-2l}) & \text{for } l \equiv 1 \pmod 8,\ l' \equiv 3 \pmod 8, \text{ and } \mu = 2, \\ K(\sqrt{2}), K(\sqrt{2l}) & \text{for } l \equiv 1 \pmod 8,\ l' \equiv 7 \pmod 8, \text{ and } \mu = 2, \\ K(\sqrt{-2}), K(\sqrt{l}), K(\sqrt{-2l}) & \text{for } l \equiv 1 \pmod 8,\ l' \equiv 3 \pmod 8, \text{ and } \mu \geq 3, \\ K(\sqrt{2}), K(\sqrt{l}), K(\sqrt{2l}) & \text{for } l \equiv 1 \pmod 8,\ l' \equiv 7 \pmod 8, \text{ and } \mu \geq 3, \\ K(\sqrt{l}) & \text{for } l \equiv 5 \pmod 8. \end{cases}$$

If $(l/l') = -1$, then the first step of K's anti-cyclotomic extension is

$$K_{\text{anti}}^{(1)} = \begin{cases} K(\sqrt{-2}) & \text{for } l \equiv 1 \pmod 8 \text{ and } l' \equiv 3 \pmod 8, \\ K(\sqrt{2}) & \text{for } l \equiv 1 \pmod 8 \text{ and } l' \equiv 7 \pmod 8, \\ K(\sqrt{2l}) & \text{for } l \equiv 5 \pmod 8 \text{ and } l' \equiv 3 \pmod 8, \\ K(\sqrt{-2l}) & \text{for } l \equiv 5 \pmod 8 \text{ and } l' \equiv 7 \pmod 8. \end{cases}$$

Proof. Use that both l and l' ramify in K. Moreover, if $l \equiv 1 \pmod 8$ and $\mu = 2$, then $\nu = 0$ by Theorem 48 and hence $a \neq l$. □

Note that Theorem 47 and Theorem 50 together uniquely determine a.

4.12 Embeddability of 2-class fields into $\mathbb{Z}_2$-extensions

Theorem 51. *The imaginary quadratic fields K whose 2-class field L is non-trivial and embeddable into a $\mathbb{Z}_2$-extension of K which is prodihedral over $\mathbb{Q}$ are the fields $K = \mathbb{Q}(\sqrt{-l})$ with a prime $l \equiv 5 \pmod 8$.*

The imaginary quadratic fields K whose 2-class field L is non-trivial and embeddable into a $\mathbb{Z}_2$-extension of K are, in addition to the above, the fields $K = \mathbb{Q}(\sqrt{-2l})$ with a prime $l \equiv 3, 5 \pmod 8$ and the fields $K = \mathbb{Q}(\sqrt{-ll'})$ with two primes $l \equiv 5 \pmod 8$ and $l' \equiv 3 \pmod 8$.

Proof. Since L/K must be non-trivial cyclic, K is of the form $\mathbb{Q}(\sqrt{-l})$ with $l \equiv 1 \pmod 4$, $\mathbb{Q}(\sqrt{-2l})$ with l odd, or $\mathbb{Q}(\sqrt{-ll'})$ with $l \equiv 1 \pmod 4$ and $l' \equiv 3 \pmod 4$. The anti-cyclotomic extension K_{anti} is the unique $\mathbb{Z}_2$-extension of K which is prodihedral over $\mathbb{Q}$, and L is contained in K_{anti} iff $\nu = \mu$. Theorems 38, 43, and 48 show that this only occurs for $K = \mathbb{Q}(\sqrt{-l})$ with $l \equiv 5 \pmod 8$.

The composite $M = K_{\text{cycl}}K_{\text{anti}}$ is the unique $\mathbb{Z}_2 \times \mathbb{Z}_2$-extension of K, and any $\mathbb{Z}_2$-extension of K is contained in M. Further, any finite cyclic subextension of

M/K is $\mathbb{Z}_2$-embeddable. If L is contained in M, then L is contained in $M \cap N(2^\infty) = K_{\text{anti}}(\sqrt{2})$. Conclude

$$L/K \text{ is } \mathbb{Z}_2\text{-embeddable} \;\Leftrightarrow\; L \text{ is contained in } K_{\text{anti}}(\sqrt{2}). \tag{4.22}$$

A necessary condition for (4.22) is that $\nu = \mu - 1$ (we ignore the case $\nu = \mu$ which is already treated). The remainder of the proof is divided into four cases according to the type of K.

Case 1. Assume $K = \mathbb{Q}(\sqrt{-l})$. Then the equation $\nu = \mu - 1$ never holds by Theorem 38.

Case 2. Assume $K = \mathbb{Q}(\sqrt{-2l})$. Then $\nu = \mu - 1$ holds for $l \equiv 3, 5, 7 \pmod 8$ by Theorem 43.

If $l \equiv 3 \pmod 8$, then $L = K(\sqrt{2})$ is the first step of K_{cycl} and hence $\mathbb{Z}_2$-embeddable.

If $l \equiv 5 \pmod 8$, then $L = K(\sqrt{-2})$ and $K_{\text{anti}}^{(1)} = K(\sqrt{-1})$, so L is contained in $K_{\text{anti}}(\sqrt{2})$ (but neither in K_{anti} nor K_{cycl}).

If $l \equiv 7 \pmod 8$, then L is not contained in $K_{\text{anti}}(\sqrt{2}) = K_{\text{anti}}$ since $\nu < \mu$, see Theorem 40.

Case 3. Assume $K = \mathbb{Q}(\sqrt{-ll'})$ with $(l/l') = -1$. Then $\nu = \mu - 1$ by Theorem 48. Now $L = K(\sqrt{l})$ is contained $K_{\text{anti}}(\sqrt{2})$ exactly when $K_{\text{anti}}^{(1)} = K(\sqrt{2l})$. This happens when $l \equiv 5 \pmod 8$ and $l' \equiv 3 \pmod 8$ by Theorem 50.

Case 4. Finally assume $K = \mathbb{Q}(\sqrt{-ll'})$ with $(l/l') = 1$. Then $\nu = \mu - 1$ holds for $l \equiv 5 \pmod 8$ by Theorem 48. So assume $l \equiv 5 \pmod 8$. From $\nu = \mu - 1$ follows that the composite $K_{\text{anti}}L$ is a $\mathbb{Z}_2 \times \mathbb{Z}/2$-extension of K (and prodihedral over $\mathbb{Q}$). Both K_{anti} and L have $K(\sqrt{l})$ as their first step over K (Theorem 50). The socle (i.e. the maximal elementary abelian 2-subextension) of $K_{\text{anti}}L$ over K is contained in $K(\sqrt{-1}, \sqrt{2}, \sqrt{l})$. It follows that $K_{\text{anti}}L = K_{\text{anti}}(\sqrt{a})$ for an $a \in \{-1, 2, -2\}$.

The prime $l = \mathfrak{l}^2$ ramifies in K, and hence $\mathfrak{l}$ splits totally in K_{anti} by section 4.4. Since $\mathfrak{l}$ has order 2 modulo K's principal ideals, $\mathfrak{l}$ does not split totally in L. So $\mathfrak{l}$ cannot split in $K(\sqrt{a})$. This shows $(a/l) \neq 1$ and thus $a \neq -1$. A similar argument gives $(a/l') \neq 1$ and therefore

$$a = \begin{cases} 2 & \text{for } l' \equiv 3 \pmod 8, \\ -2 & \text{for } l' \equiv 7 \pmod 8. \end{cases}$$

Conclude that L is contained in $K_{\text{anti}}(\sqrt{2})$ if and only if $l' \equiv 3 \pmod 8$. □

Of the quadratic fields K mentioned in the theorem, only the $K = \mathbb{Q}(\sqrt{-ll'})$ with two primes $l \equiv 5 \pmod 8$ and $l' \equiv 3 \pmod 8$ satisfying $(l/l') = 1$ have 2-class field L of degree $[L : K] > 2$.

The question of $\mathbb{Z}_p$-embeddability of p-class fields is somewhat different for $p = 2$ compared to the case of an odd prime p. In the latter case, $\mathbb{Z}_p$-embeddability of the p-class field is equivalent to the p-class field being contained in K's anti-cyclotomic extension.

For all (odd or even) primes p, it seems that there exist imaginary quadratic fields with $\mathbb{Z}_p$-embeddable p-class field of arbitrarily high degree, although proving this is probably difficult.

4.13 Interrelations between $\mathbb{Q}(\sqrt{-l})$ and $\mathbb{Q}(\sqrt{-2l})$

Consider a prime $l \equiv 1 \pmod 8$ and put $K = \mathbb{Q}(\sqrt{-l})$ and $K' = \mathbb{Q}(\sqrt{-2l})$. There are some quite surprising interrelations between these two fields. Let h and h' be the class numbers of K and K', respectively, and put $\mu = v_2(h)$ and $\mu' = v_2(h')$. Recall that h and h' are both divisible by 4 (section 4.6 and 4.7).

Theorem 52. *If $l \equiv 1 \pmod{16}$, then*

$$8 \mid h \;\Leftrightarrow\; 8 \mid h'.$$

If $l \equiv 9 \pmod{16}$, then

$$8 \mid h \;\Leftrightarrow\; 8 \nmid h'.$$

Proof. We have

$$\begin{aligned} 8 \mid h \quad &\Leftrightarrow \quad l \text{ is of the form } X^2 + 32Y^2, \\ 8 \mid h' \quad &\Leftrightarrow \quad l \text{ is of the form } X^2 + 64Y^2 \end{aligned}$$

by section 4.6 and 4.7. Combining this with Lemma 36 gives the statement. □

There are also some interrelations between the anti-cyclotomic extensions of K and K' as we shall now see. The following lemma is proved along with the next two theorems at the end of the section.

Lemma 53. *Assume $l \equiv 1 \pmod{16}$ and that h and h' are divisible by 8. Pick a prime number $p \equiv 7 \pmod 8$ such that $(-l/p) = 1$. Write*

$$p^h = X^2 + lY^2 \quad \text{and} \quad p^{h'} = U^2 + 2lV^2$$

with relatively prime $X, Y \in \mathbb{Z}$ and relatively prime $U, V \in \mathbb{Z}$. Put $t = v_2(X)$ and $t' = v_2(V)$. Then $t \geq 4$ and $t' \geq 3$. Further, the truth or falsity of the implication

$$t = 4 \;\Leftrightarrow\; t' = 3 \tag{$*$}$$

is independent of the choice of p.

So $(*)$ only depends on l. We will have more to say later on the question which primes l in fact *have* property $(*)$.

THEOREM 54. *Assume $l \equiv 1 \pmod{16}$ and that h and h' are both divisible by 16. Assume further that l has the property $(*)$ of Lemma 53. Let ν and ν' be the number of unramified steps of K_{anti} and K'_{anti}, respectively. Then*

$$\nu = \mu - 3 \;\Leftrightarrow\; \nu' = \mu' - 3.$$

This should be seen in light of Theorem 38 and Theorem 43. The next result relates to Theorem 41 and Theorem 46.

THEOREM 55. *Assume $l \equiv 1 \pmod{16}$ and that h and h' are both divisible by 8. Assume further that l has the property $(*)$ of Lemma 53. Let $a, a' \in \{-1, 2, -2\}$ be such that $K(\sqrt{a})$ and $K'(\sqrt{a'})$ are the first steps of K_{anti} and K'_{anti}, respectively.*

(i) If $\mu = 3$ and $\mu' = 3$, then $(a, a') \in \{(2, 2), (-2, -1)\}$.

(ii) If $\mu = 3$ and $\mu' = 4$, then $(a, a') \in \{(2, -1), (2, 2), (-2, -2)\}$.

(iii) If $\mu = 3$ and $\mu' \geq 5$, then $(a, a') \in \{(2, -1), (2, 2), (2, -2), (-2, -2)\}$.

(iv) If $\mu = 4$ and $\mu' = 3$, then $(a, a') \in \{(-1, -1), (2, 2), (-2, 2)\}$.

(v) If $\mu \geq 5$ and $\mu' = 3$, then $(a, a') \in \{(-1, -1), (-1, 2), (2, 2), (-2, 2)\}$.

(vi) If $\mu = 4$ and $\mu' = 4$, then

$$(a, a') \in \{(-1, -2), (2, -1), (2, 2), (-2, -1), (-2, 2)\}.$$

(vii) If $\mu = 4$ and $\mu' \geq 5$, then

$$(a, a') \in \{(-1, -2), (2, -1), (2, 2), (2, -2), (-2, -1), (-2, 2), (-2, -2)\}.$$

(iix) If $\mu \geq 5$ and $\mu' = 4$, then

$$(a, a') \in \{(-1, -1), (-1, 2), (-1, -2), (2, -1), (2, 2), (-2, -1), (-2, 2)\}.$$

Proof of Lemma 53, Theorem 54, and Theorem 55. Pick a prime p as in Lemma 53. Then

$$t \geq \mu - \nu + 1 \geq 4$$

by Theorem 34 and Theorem 38. Theorem 37 gives

$$\begin{array}{llllll}
\text{for } \mu = 3\text{:} & t = 4 & \Leftrightarrow & & & a = -2, \\
\text{for } \mu = 4\text{:} & t = 4 & \Leftrightarrow & \nu = \mu - 3 & \Leftrightarrow & a = -1, \\
\text{for } \mu \geq 5\text{:} & t = 4 & \Leftrightarrow & \nu = \mu - 3 & \Rightarrow & a = -1.
\end{array}$$

This shows that in fact the property $t = 4$ is independent of the choice of p.

Similarly, Theorem 34 and Theorem 43 give

$$t' \geq \mu' - \nu' \geq 3,$$

and Theorem 42 gives

$$\begin{array}{llllll}
\text{for } \mu' = 3\text{:} & t' = 3 & \Leftrightarrow & & & a' = -1, \\
\text{for } \mu' = 4\text{:} & t' = 3 & \Leftrightarrow & \nu' = \mu' - 3 & \Leftrightarrow & a' = -2, \\
\text{for } \mu' \geq 5\text{:} & t' = 3 & \Leftrightarrow & \nu' = \mu' - 3 & \Rightarrow & a' = -2.
\end{array}$$

This shows that the property $t' = 3$ is also independent of the choice of p. If l satisfies $(*)$, i.e. if $t = 4 \Leftrightarrow t' = 3$, the conclusions of Theorem 54 and Theorem 55 follow from the above implications. □

Theorem 54 and Theorem 55 are perhaps more interesting given the following:

Conjecture 56. *All primes l satisfying the assumptions of Lemma 53 have property* $(*)$.

The author has verified this conjecture for all l less than 14 millions, but has not found a proof.

4.14 Numerical examples

The purpose of this section is to show by numerical examples that the results of the previous sections are strongest possible – or at least that they have no immediate strengthenings.

Consider a prime $l \equiv 1 \pmod{16}$ and put $K = \mathbb{Q}(\sqrt{-l})$ and $K' = \mathbb{Q}(\sqrt{-2l})$. Let h and h' be the class numbers of K and K', respectively, and put $\mu = v_2(h)$ and $\mu' = v_2(h')$. Let ν and ν' be the number of unramified steps of the anticyclotomic extension of K and K', respectively. When $\mu \geq 4$, we only know $\nu = 0, \ldots, \mu - 3$ (Theorem 38), and similarly for ν' when $\mu' \geq 4$ (Theorem 43). The following two tables give good evidence that these statements are best possible:

l	μ	μ'	ν
353	4	3	0
1201	4	3	1
1249	5	3	0
7393	5	3	1
18593	5	3	2
53201	6	3	0
30881	6	3	1
13441	6	3	2
8273	6	3	3

l	μ	μ'	ν'
2593	3	4	0
4273	3	4	1
5393	3	5	0
3089	3	5	1
1553	3	5	2
3361	3	6	0
33569	3	6	1
48337	3	6	2
2689	3	6	3

If $\mu \geq 4$ and $\mu' \geq 4$ simultaneously, Theorem 54 in conjunction with Conjecture 56 gives that $\nu = \mu - 3$ if and only if $\nu' = \mu' - 3$. This also seems to be optimal, as the following table (and the two tables above) shows:

l	μ	μ'	ν	ν'
9473	4	4	0	0
257	4	4	1	1
36097	5	4	0	0
8609	5	4	1	0
2833	5	4	2	1
48497	4	5	0	0
44449	4	5	0	1

l	μ	μ'	ν	ν'
4289	4	5	1	2
25409	5	5	0	0
236449	5	5	1	0
1217	5	5	0	1
103393	5	5	1	1
2657	5	5	2	2

Now let $a, a' \in \{-1, 2, -2\}$ be such that $K(\sqrt{a})$ and $K'(\sqrt{a'})$ are the first steps of K_{anti} and K'_{anti}, respectively. Theorem 41 rules out one value for a when $\mu = 3$ and says nothing when $\mu \geq 4$. Similarly for the value of a' by Theorem 46. Further, Theorem 55 and Conjecture 56 rule out some (*a priori* expectable) combinations (a, a') when $\mu = 3, 4$ or $\mu' = 3, 4$. The following table shows that these results are best possible. For example it is seen that all 9 pairs

(a, a') occur when $\mu = \mu' = 5$.

l	μ	μ'	a	a'
337	3	3	2	2
113	3	3	-2	-1
2593	3	4	2	-1
12641	3	4	2	2
4273	3	4	-2	-2
5393	3	5	2	-1
44129	3	5	2	2
3089	3	5	2	-2
1553	3	5	-2	-2
1201	4	3	-1	-1
12161	4	3	2	2
353	4	3	-2	2
18593	5	3	-1	-1
7393	5	3	-1	2
10337	5	3	2	2
1249	5	3	-2	2
257	4	4	-1	-2
31649	4	4	2	-1
9601	4	4	2	2
12577	4	4	-2	-1
9473	4	4	-2	2
4289	4	5	-1	-2
84449	4	5	2	-1
243137	4	5	2	2
44449	4	5	2	-2
116881	4	5	-2	-1
48497	4	5	-2	2
58337	4	5	-2	-2
26177	5	4	-1	-1
8609	5	4	-1	2
2833	5	4	-1	-2
36097	5	4	2	-1
175361	5	4	2	2
299393	5	4	-2	-1
57697	5	4	-2	2
236449	5	5	-1	-1
412193	5	5	-1	2
2657	5	5	-1	-2
159857	5	5	2	-1
809569	5	5	2	2
1217	5	5	2	-2
586433	5	5	-2	-1
444529	5	5	-2	2
670177	5	5	-2	-2

Finally consider the fields $K = \mathbb{Q}(\sqrt{-ll'})$ with two primes $l \equiv 1 \pmod 8$ and $l' \equiv 3 \pmod 4$. Let $\mu = v_2(h)$ be the dyadic valuation of K's class number h. When $\mu \geq 3$, the number ν is one of $0, \ldots, \mu - 2$ by Theorem 48. It appears that ν can take all of these values:

l	l'	μ	ν
41	83	3	0
41	31	3	1
73	71	4	0
17	47	4	1
41	23	4	2
41	163	5	0
97	103	5	1
113	227	5	2
113	7	5	3

One can obtain tables similar to the above where l and l' belong to prescribed residue classes modulo higher powers of 2.

Chapter 5

Non-abelian fibre products as Galois groups

5.1 Introduction: rank, socle, fibre product

Let G be a pro-p-group. Recall that the **Frattini subgroup** $\Phi(G)$ of G is the closed subgroup generated by all p'th powers and commutators. It is the minimal closed normal subgroup of G such that the quotient is elementary abelian. The **rank** of G is the dimension over $\mathbb{F}_p$ of $G/\Phi(G)$. By Burnside's "Basis Theorem", the rank of G is equal to the cardinality of any minimal generating subset. The example $\mathbb{Z}/6$ shows that the assumption that G is a p-group is essential.

If the Galois group $G = \mathrm{Gal}(L/K)$ of some Galois extension L/K is a pro-p-group, the **socle** of L/K is defined as the fixed field of $\Phi(G)$. In other words, the socle of L/K is the composite of all $\mathbb{Z}/p$-subextensions.

Let $\varphi : X \to Z$ and $\psi : Y \to Z$ be group homomorphisms. Define the **fibre product** with respect to these homomorphisms as the group

$$X \times_Z Y := \{(x, y) \in X \times Y \mid \varphi(x) = \psi(y)\}$$

(see also [17] or [10]).

As an example, consider the sign homomorphism $S_n \to \mathbb{Z}/2$ and reduction modulo 2: $\mathbb{Z}/4 \to \mathbb{Z}/2$. Then the fibre product

$$S_n \times_{\mathbb{Z}/2} \mathbb{Z}/4 = \{(\sigma, a) \in S_n \times \mathbb{Z}/4 \mid \mathrm{sign}(\sigma) \equiv a \pmod 2\}$$

is a non-split double cover[1] of the symmetric group S_n.

[1] Non-split double cover of S_n: group, other than $S_n \times \mathbb{Z}/2$, of order $2 \cdot n!$ having S_n as a homomorphic image. See for instance [25].

Fibre products play a role in Galois theory for the following reason. Let L/K and M/K be Galois extensions contained in the same algebraic closure of K. Then there is an natural isomorphism

$$\mathrm{Gal}(LM/K) \cong \mathrm{Gal}(L/K) \times_Z \mathrm{Gal}(M/K)$$

where the fibre product is defined with respect to the restrictions from $\mathrm{Gal}(L/K)$ and $\mathrm{Gal}(M/K)$ onto $Z = \mathrm{Gal}(L \cap M/K)$.

We shall be concerned with the realisation of certain fibre products of pro-p-groups as Galois groups over number fields. For a field K and a pro-finite group G, let us denote by $\nu(G, K)$ the number of G-extensions of K (inside a fixed algebraic closure of K). This number might well be zero, for instance $\nu(\mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Q}) = 0$. We will also see examples where $\nu(G, K)$ is non-zero, but finite. So the situation of infinite, pro-finite groups is quite different compared to that of finite groups.

5.2 The p-adic prodihedral groups $\mathbb{D}_p$

For a prime p, define the **p-adic prodihedral group** $\mathbb{D}_p$ as the natural projective limit of the dihedral groups of order $2p^n$, $n \geq 1$:

$$\mathbb{D}_p = \varprojlim D_{p^n}.$$

$\mathbb{D}_p$ contains the procyclic group $\mathbb{Z}_p$ as the unique abelian subgroup of index 2. Any element $\tau \in \mathbb{D}_p \backslash \mathbb{Z}_p$ has order 2 and inverts $\mathbb{Z}_p$ by conjugation. So we may write $\mathbb{D}_p$ as the semidirect product

$$\mathbb{D}_p = \mathbb{Z}_p \rtimes \mathbb{Z}/2.$$

Let us write $\mathbb{D}_p$ additively. If a field extension L/K has $\mathrm{Gal}(L/K) \cong \mathbb{D}_p$, we denote the subfield corresponding to the subgroup $\mathbb{Z}_p$ as the **(quadratic) base** of the $\mathbb{D}_p$-extension.

We now turn to the dyadic prodihedral group $\mathbb{D}_2$. The Frattini subgroup of $\mathbb{D}_2$ coincides with the commutator subgroup

$$\Phi(\mathbb{D}_2) = \mathbb{D}_2' = 2\mathbb{Z}_2.$$

The quotient $\mathbb{D}_2/2\mathbb{Z}_2$ is isomorphic to Klein's 4-group and has representatives $0, 1, \tau, 1 + \tau$.

Example. Let p be an odd prime and consider two imaginary quadratic number fields K and K'. Then the cyclotomic p-extension $\mathbb{Q}_{\mathrm{cycl}}$ and the anti-cyclotomic extensions K_{anti} and K'_{anti} (as defined in section 1.6) are linearly disjoint over $\mathbb{Q}$. Hence their composite M has $\mathrm{Gal}(M/\mathbb{Q}) \cong \mathbb{Z}_p \times \mathbb{D}_p \times \mathbb{D}_p$. Further, the composite KK' has Iwasawa number $a(KK') = 3$, and M is the $(\mathbb{Z}_p)^3$-extension of KK'. If K'' is the real quadratic subfield of KK', the dihedral Iwasawa number of KK'/K'' is $a(KK'/K'') = a(KK') - a(K'') = 2$, and $K_{\text{anti}}K''$ and $K'_{\text{anti}}K''$ are independent $\mathbb{D}_p$-extensions with quadratic base KK'/K''.

The situation is more complicated for $p = 2$. This is the subject of the next section.

5.3 Realising fibre products of $\mathbb{D}_2$ with itself

We now consider 2-extensions. Let K and K' be distinct imaginary quadratic fields. Let N denote the composite of the anti-cyclotomic 2-extensions K_{anti} and K'_{anti}. There are now four possibilities for $\mathrm{Gal}(N/\mathbb{Q})$:

Case 1. K_{anti} and K'_{anti} are linearly disjoint over $\mathbb{Q}$. Then $\mathrm{Gal}(N/\mathbb{Q}) \cong \mathbb{D}_2 \times \mathbb{D}_2$.

Case 2. The intersection of K_{anti} and K'_{anti} is a quadratic field different from K and K'. Then $\mathrm{Gal}(N/\mathbb{Q})$ is isomorphic to the fibre product $\mathbb{D}_2 \times_{\mathbb{Z}/2} \mathbb{D}_2$ defined by the single homomorphism $\varphi : \mathbb{D}_2 \to \mathbb{Z}/2$ given by $\ker(\varphi) = 2\mathbb{Z}_2 \cup \tau + 2\mathbb{Z}_2$.

Case 3. The intersection of K_{anti} and K'_{anti} is either K or K'. Then $\mathrm{Gal}(N/\mathbb{Q})$ is isomorphic to the fibre product $\mathbb{D}_2 \times_{\mathbb{Z}/2} \mathbb{D}_2$ defined by the homomorphism φ above and the homomorphism $\varphi' : \mathbb{D}_2 \to \mathbb{Z}/2$ given by $\ker(\varphi') = \mathbb{Z}_2$.

Case 4. The socles of K_{anti} and K'_{anti} coincide and thus equal the intersection of K_{anti} and K'_{anti}. Then $\mathrm{Gal}(N/\mathbb{Q})$ is isomorphic to the fibre product

$$\mathfrak{H} := \mathbb{D}_2 \times_V \mathbb{D}_2$$

defined by two surjective homomorphisms

$$\psi, \psi' : \mathbb{D}_2 \to V = \mathbb{Z}/2 \times \mathbb{Z}/2$$

with $\psi(\mathbb{Z}_2) \neq \psi'(\mathbb{Z}_2)$.

The composite of N with $\mathbb{Q}_{\text{cycl}}$ is a $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$-extension of the biquadratic field KK', but even more possibilities for the Galois group over $\mathbb{Q}$ appear according to the intersection of N with $\mathbb{Q}_{\text{cycl}}$. We do not go into further details about this.

In the next section we investigate realisations of the fibre product $\mathfrak{H}$ over $\mathbb{Q}$. Let us first note that $\mathfrak{H}$ can be represented by generators and relations as follows[2]:

$$\mathfrak{H} \cong \langle a, b \mid ba = a^{-1}b^{-1},\ ba^{-1} = ab^{-1}\rangle.$$

LEMMA 57. *Regarding the commutator subgroup of $\mathfrak{H}$, one has*

$$\mathfrak{H}/\mathfrak{H}' \cong \mathbb{Z}/4 \times \mathbb{Z}/2.$$

Proof. We use that $\mathfrak{H}$ is generated by two elements a, b satisfying the relations $ba = a^{-1}b^{-1}$ and $ba^{-1} = ab^{-1}$. Let $\mathfrak{H}^*$ be the closed normal subgroup of $\mathfrak{H}$ generated by the 3 commutators

$$[a^2, b] = a^4\ ,\ [b^2, a] = b^4\ ,\ [a, b^{-1}] = a^2b^2.$$

Then

$$\mathfrak{H}/\mathfrak{H}^* = \langle \overline{a} \rangle \times \langle \overline{ab} \rangle \cong \mathbb{Z}/4 \times \mathbb{Z}/2.$$

It follows that $\mathfrak{H}^*$ is the commutator subgroup $\mathfrak{H}'$ of $\mathfrak{H}$, and we are done. □

5.4 $\mathbb{D}_2$-extensions with different base, but common socle

Consider an imaginary field $K = \mathbb{Q}(\sqrt{-\Delta})$ and put $K' = \mathbb{Q}(\sqrt{-2\Delta})$. Assume that the anti-cyclotomic 2-extensions K_{anti} and K'_{anti} have common socle $\mathbb{Q}(\sqrt{-\Delta}, \sqrt{2})$. Then

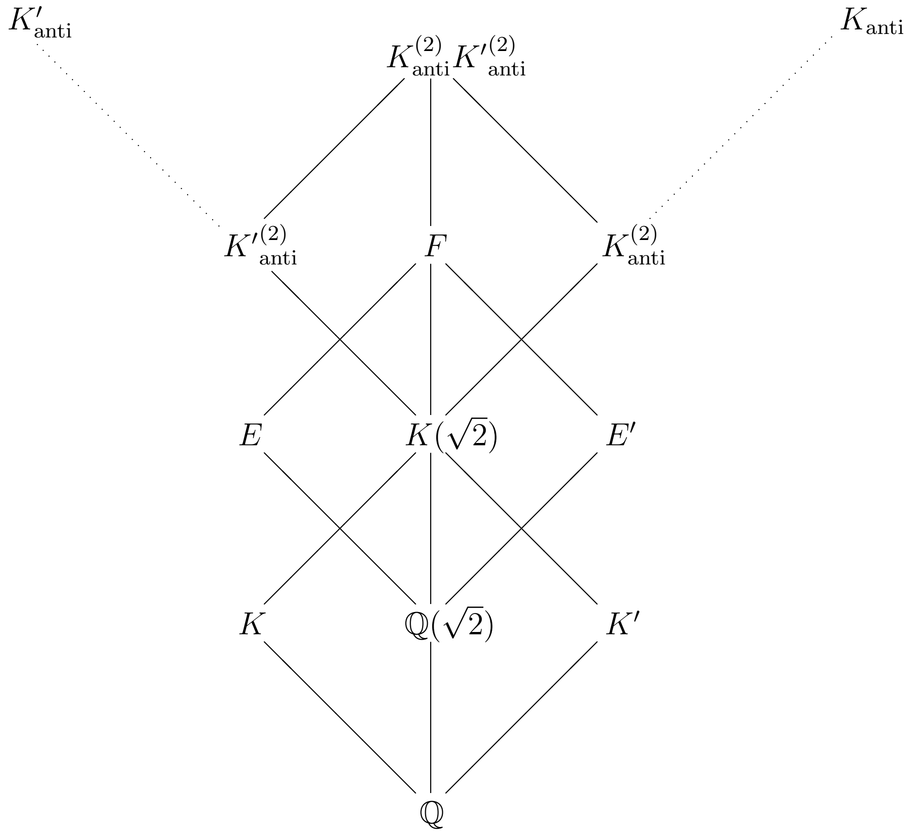
$$\mathrm{Gal}(K_{\text{anti}}K'_{\text{anti}}/\mathbb{Q}) \cong \mathfrak{H}$$

as defined in the previous section. Hence the maximal abelian subextension F of $K_{\text{anti}}K'_{\text{anti}}$ has Galois group

$$\mathrm{Gal}(F/\mathbb{Q}) \cong \mathbb{Z}/4 \times \mathbb{Z}/2$$

by Lemma 57. There are two subfields E and E' of F that are $\mathbb{Z}/4$-extensions of $\mathbb{Q}$. They both contain $\mathbb{Q}(\sqrt{2})$ since neither $K/\mathbb{Q}$ nor $K'/\mathbb{Q}$ is $\mathbb{Z}/4$-embeddable. Thus F is a $\mathbb{Z}/4$-extension of K and K' and a $\mathbb{Z}/2 \times \mathbb{Z}/2$-extension of $\mathbb{Q}(\sqrt{2})$. We have the following diagram of subfields:

[2] This is to be understood thus: Let F be the free pro-2-group with 2 generators. Let N be the closed, normal subgroup generated by the relations. Then $\mathfrak{H}$ is isomorphic to F/N. For a definition of the free pro-2-group, see [10] section 15.5.



Example 58. Assume $\Delta = 1$, i.e. $K = \mathbb{Q}(i)$ and $K' = \mathbb{Q}(\sqrt{-2})$. We know that both K_{anti} and K'_{anti} have socle $\mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}^{(8)}$, the 8'th cyclotomic field. The $\mathbb{Z}/4 \times \mathbb{Z}/2$-extension $F/\mathbb{Q}$ is unramified outside $\{2, \infty\}$. Only one such extension exists, namely the 16'th cyclotomic field, so $F = \mathbb{Q}^{(16)}$. Consider a prime p that splits in $\mathbb{Q}^{(8)}$, i.e. with $p \equiv 1 \pmod 8$. We have

$$\begin{array}{lcl} p \text{ splits in } K_{\text{anti}}^{(2)} & \Leftrightarrow & p \text{ is of the form } X^2 + 64Y^2, \\ p \text{ splits in } K'^{(2)}_{\text{anti}} & \Leftrightarrow & p \text{ is of the form } X^2 + 32Y^2, \\ p \text{ splits in } F = \mathbb{Q}^{(16)} & \Leftrightarrow & p \equiv 1 \pmod{16} \end{array}$$

by Theorem 34. We see again (see Lemma 36) that p is representable by both or none of the forms $X^2 + 32Y^2$ and $X^2 + 64Y^2$ if $p \equiv 1 \pmod{16}$, whereas p is representable by one, but not both of these forms if $p \equiv 9 \pmod{16}$. However, this second proof also shows that there are no such relations for the forms $X^2 + 128Y^2$, $X^2 + 256Y^2$ etc. that can be expressed by congruence conditions, say modulo 32, since $K_{\text{anti}}K'_{\text{anti}}$ contains no abelian subfield greater than $\mathbb{Q}^{(16)}$.

Let us compute $K_{\text{anti}}^{(2)}$ and $K'^{(2)}_{\text{anti}}$ explicitly. First, $K_{\text{anti}}^{(2)}$ is a $\mathbb{Z}/2 \times \mathbb{Z}/2$-extension of $K' = \mathbb{Q}(\sqrt{-2})$ unramified outside 2. Only one such extension exists, namely

$$K^{(2)}_{\text{anti}} = \mathbb{Q}(i, \sqrt[4]{-2}) = \mathbb{Q}(i, \sqrt[4]{2}).$$

Similarly,

$$K'^{(2)}_{\text{anti}} = \mathbb{Q}(\sqrt{2}, \sqrt{1+i})$$

is the unique $\mathbb{Z}/2 \times \mathbb{Z}/2$-extension of $K = \mathbb{Q}(i)$ unramified outside 2.

Combining the above gives the following criteria for an odd prime p:

$$\begin{array}{lcl} p \text{ is of the form } X^2 + 32Y^2 & \Leftrightarrow & x^4 - 2x^2 + 2 \text{ has 4 roots modulo } p, \\ p \text{ is of the form } X^2 + 64Y^2 & \Leftrightarrow & x^4 - 2 \text{ has 4 roots modulo } p. \end{array}$$

This ends our Example 58. □

Now assume that Δ equals an odd prime l. Then l is tamely ramified in $F/\mathbb{Q}$. It follows that l is unramified in either E or E', say in E. So $E/\mathbb{Q}$ is a $\mathbb{Z}/4$-extension unramified outside $\{2, \infty\}$. The only such extensions are the two subfields

$$E = \mathbb{Q}\left(\sqrt{\sqrt{2}+2}\right) \quad \text{and} \quad E = \mathbb{Q}\left(\sqrt{\sqrt{2}-2}\right)$$

of $\mathbb{Q}^{(16)}$. We have proved:

Lemma 59. *Let $K = \mathbb{Q}(\sqrt{-l})$ and $K' = \mathbb{Q}(\sqrt{-2l})$ with an odd prime l such that K_{anti} and K'_{anti} have common socle. Then the composite $K_{anti}K'_{anti}$ contains a square root of either $\sqrt{2}+2$ or $\sqrt{2}-2$.* □

Let h and h' be the class numbers of K and K', respectively. The assumption of the lemma, that K_{anti} and K'_{anti} have the same socle, is satisfied when $l \equiv 7 \pmod 8$, when $l \equiv 1 \pmod{16}$ and h and h' are not divisible by 8, and sometimes when $l \equiv 1 \pmod{16}$ and h and h' *are* divisible by 8 (see section 4.9 and 4.10). The determination of the right square root in these cases is not trivial.

Theorem 60. *Let $K = \mathbb{Q}(\sqrt{-l})$ and $K' = \mathbb{Q}(\sqrt{-2l})$ with a prime $l \equiv 7$ (mod 8). Pick a prime $p \equiv 7$ (mod 8) with $(-l/p) = 1$. Write*

$$p^h = X^2 + XY + \frac{l+1}{4}Y^2 \quad \textit{and} \quad p^{h'} = U^2 + 2lV^2$$

with relatively prime $X, Y \in \mathbb{Z}$ and relatively prime $U, V \in \mathbb{Z}$. Put $t = v_2(X + Y/2)$ and $t' = v_2(V)$. Then $t, t' \geq 2$. Further, the statement

$$\left.\begin{array}{ll} \textit{for } p \equiv l \ (\textit{mod } 16): & t = 2 \ \Leftrightarrow \ t' = 2 \\ \textit{for } p \not\equiv l \ (\textit{mod } 16): & t = 2 \ \Leftrightarrow \ t' > 2 \end{array}\right\} \qquad (**)$$

is equivalent to the statement that the composite $K_{anti}K'_{anti}$ *contains a square root of*

$$\begin{cases} \sqrt{2}+2 & \mathit{if}\ l \equiv 15\ (\mathit{mod}\ 16), \\ \sqrt{2}-2 & \mathit{if}\ l \equiv 7\ (\mathit{mod}\ 16). \end{cases}$$

Proof. First note (again) that K_{anti} and K'_{anti} have the same socle by Theorems 40 and 45. Pick a prime p as in the theorem. Theorem 34, Remark 35, Theorem 38, and Theorem 43 give

$$\begin{aligned} p \text{ splits in } K_{\text{anti}}^{(n)} \quad &\Leftrightarrow \quad t \geq n+\mu-\nu+1 = n+1, \\ p \text{ splits in } K'^{(n)}_{\text{anti}} \quad &\Leftrightarrow \quad t' \geq n+\mu'-\nu' = n+1. \end{aligned}$$

It follows from the assumptions that p splits in K and K' and hence in

$$KK' = \mathbb{Q}(\sqrt{2}, \sqrt{-l}) = K_{\text{anti}}^{(1)} = K'^{(1)}_{\text{anti}}.$$

There follows $t, t' \geq 2$. Now note

$$\begin{aligned} p \text{ splits in } \mathbb{Q}\left(\sqrt{\sqrt{2}+2}\right) \quad &\Leftrightarrow \quad p \equiv 1, 15 \text{ (mod 16)}, \\ p \text{ splits in } \mathbb{Q}\left(\sqrt{\sqrt{2}-2}\right) \quad &\Leftrightarrow \quad p \equiv 1, 7 \text{ (mod 16)} \end{aligned}$$

(this follows from the law about prime decomposition in cyclotomic fields). Let F be the maximal abelian subfield of $K_{\text{anti}}K'_{\text{anti}}$.

If p splits in F, i.e. if *either* $\sqrt{\sqrt{2}+2} \in F$ and $p \equiv 15$ (mod 16), *or* $\sqrt{\sqrt{2}-2} \in F$ and $p \equiv 7$ (mod 16), then

$$p \text{ splits in } K_{\text{anti}}^{(2)} \ \Leftrightarrow\ p \text{ splits in } K'^{(2)}_{\text{anti}}$$

and thus

$$t > 2 \ \Leftrightarrow\ t' > 2.$$

If, on the other hand, p does not split in F, i.e. if *either* $\sqrt{\sqrt{2}+2} \in F$ and $p \equiv 7$ (mod 16), *or* $\sqrt{\sqrt{2}-2} \in F$ and $p \equiv 15$ (mod 16), then p splits in one, but not both of $K_{\text{anti}}^{(2)}$ and $K'^{(2)}_{\text{anti}}$ and thus

$$t = 2 \ \Leftrightarrow\ t' > 2.$$

The theorem follows. □

The theorem gives in particular that $(**)$ only depends on l. We put forth a conjecture at the end of the section regarding which primes l have property $(**)$.

The proof of the next theorem is quite similar to the above and is therefore omitted.

Theorem 61. *Let $K = \mathbb{Q}(\sqrt{-l})$ and $K' = \mathbb{Q}(\sqrt{-2l})$ with a prime $l \equiv 1 \ (mod\ 16)$ such that the class numbers h and h' of K and K' are not divisible by 8. Pick a prime number $p \equiv 7 \ (mod\ 8)$ such that $(-l/p) = 1$. Write*

$$p^h = X^2 + lY^2 \quad \text{and} \quad p^{h'} = U^2 + 2lV^2$$

with relatively prime $X, Y \in \mathbb{Z}$ and relatively prime $U, V \in \mathbb{Z}$. Put $t = v_2(X)$ and $t' = v_2(V)$. Then $t \geq 4$ and $t' \geq 3$. Furhter, the statement

$$\left.\begin{array}{ll} \text{for } p \equiv 15 \ (mod\ 16): & t = 4 \ \Leftrightarrow \ t' = 3 \\ \text{for } p \equiv 7 \ (mod\ 16): & t = 4 \ \Leftrightarrow \ t' > 3 \end{array}\right\} \qquad (***)$$

is equivalent to the statement that the composite $K_{anti}K'_{anti}$ contains a square root of $\sqrt{2} + 2$. □

Again we se that the property $(***)$ only depends on l.

Conjecture 62. All primes $l \equiv 7$ (mod 16) have property $(**)$ of Theorem 60. All primes $l \equiv 1$ (mod 16) such that the class numbers of $\mathbb{Q}(\sqrt{-l})$ and $\mathbb{Q}(\sqrt{-2l})$ are not divisible by 8 have property $(***)$ of Theorem 61.

This conjecture has been confirmed by the author for all l up to 8 millions. Note the similarity with Conjecture 56.

Theorem 60 and 61 give an easy, effective method (which is independent of the truth or falsity of Conjecture 62) to determine whether $K_{\text{anti}}K'_{\text{anti}}$ contains a square root of $\sqrt{2} + 2$ or of $\sqrt{2} - 2$.

When $l \equiv 1$ (mod 16) and the class numbers h and h' are divisible by 8, there seems to be no simple criterion giving the right square root as the following example shows.

Example. (a) Let $l = 337$ with $l \equiv 1$ (mod 16). Then $h = 8$ and $h' = 24$ are divisible by 8, and K_{anti} and K'_{anti} have common socle. The same argument as in the proof of Theorem 60 gives that the composite $K_{\text{anti}}K'_{\text{anti}}$ contains a square root of $\sqrt{2} - 2$.

(b) Let $l = 593$ with $l \equiv 1$ (mod 16). Then $h = 24$ and $h' = 24$ are divisible by 8, and K_{anti} and K'_{anti} have common socle. One sees similarly that now $K_{\text{anti}}K'_{\text{anti}}$ contains a square root of $\sqrt{2} + 2$. □

5.5 Realising the fibre product of $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{D}_2$

Consider the pro-2-groups $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{D}_2$. They both have rank 2, so there are surjective homomorphisms

$$\varphi : \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}/2 \times \mathbb{Z}/2 \ \ , \ \ \psi : \mathbb{D}_2 \to \mathbb{Z}/2 \times \mathbb{Z}/2$$

with the respective Frattini subgroups as kernels. We may therefore define the fibre product

$$\mathfrak{G} := (\mathbb{Z}_2 \times \mathbb{Z}_2) \times_{\mathbb{Z}/2\times\mathbb{Z}/2} \mathbb{D}_2$$

with respect to φ and ψ. This pro-2-group is independent of the choice of φ and ψ since any automorphism of $(\mathbb{Z}_2 \times \mathbb{Z}_2)/\ker(\varphi) = \mathbb{Z}/2 \times \mathbb{Z}/2$ can be lifted to an automorphism of $\mathbb{Z}_2 \times \mathbb{Z}_2$.

We can also represent $\mathfrak{G}$ (as pro-2-group) by generators and relations:

$$\mathfrak{G} \cong \langle x, y \mid xy^2 = y^2x,\ x^2y = yx^2\rangle.$$

Since $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{D}_2$ have no common homomorphic image greater than $\mathbb{Z}/2 \times \mathbb{Z}/2$, the problem of realising $\mathfrak{G}$ as Galois group over some field K is equivalent to realising both $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{D}_2$ over K in such a way that the socles of the two extensions coincide.

Clearly the number of $\mathfrak{G}$-extensions of $\mathbb{Q}$ is $\nu(\mathfrak{G}, \mathbb{Q}) = 0$, since $\mathbb{Q}$ has no $\mathbb{Z}_2 \times \mathbb{Z}_2$-extension. Similarly, $\nu(\mathfrak{G}, K) = 0$ for a real quadratic field K.

Theorem 63. *Let $K = \mathbb{Q}(\sqrt{-l})$ with an odd prime l. If $l \equiv 3, 5 \pmod 8$ or $l \equiv 9 \pmod{16}$, then*

$$\nu(\mathfrak{G}, K) = 3.$$

If $l \equiv 15 \pmod{16}$ and l has property $(**)$ of Theorem 60, then

$$1 \leq \nu(\mathfrak{G}, K) \leq 3.$$

If $l \equiv 7 \pmod{16}$ and l has property $(**)$ of Theorem 60, then

$$0 \leq \nu(\mathfrak{G}, K) \leq 2.$$

The same statements hold for the field $K = \mathbb{Q}(\sqrt{-2l})$.

Proof. We prove the theorem only for $K = \mathbb{Q}(\sqrt{-l})$. K has a unique $\mathbb{Z}_2 \times \mathbb{Z}_2$-extension $K_{\mathbb{Z}_2}$. Note that $\mathfrak{G}$ has only one quotient isomorphic to $\mathbb{D}_2$. Hence $\nu(\mathfrak{G}, K)$ equals the number of $\mathbb{D}_2$-extensions of K having the same socle as $K_{\mathbb{Z}_2}/K$.

Each of the three quadratic subextensions K_i of $K_{\mathbb{Z}_2}/K$ has dihedral Iwasawa number

$$a(K_i/K) = a(K_i) - a(K) = 3 - 2 = 1,$$

i.e. there is a unique $\mathbb{D}_2$-extension L_i/K with quadratic base K_i. So to compute $\nu(\mathfrak{G}, K)$, we must compare the socles of $K_{\mathbb{Z}_2}/K$ and L_i/K for each $i = 1, 2, 3$. In particular,

$$\nu(\mathfrak{G}, K) = 0, 1, 2, 3.$$

Also note that a $\mathfrak{G}$-extension is necessarily unramified outside 2 since $\mathbb{Z}_2$-extensions are unramified outside 2.

First assume $l \equiv 3, 5 \pmod 8$. Then the socle of $K_{\mathbb{Z}_2}/K$ is $K(\sqrt{-1}, \sqrt{2})$ by Theorem 40. Since K is 2-rational by Theorem 10, this is the only $\mathbb{Z}/2 \times \mathbb{Z}/2$-extension of K unramified outside 2. Hence this socle coincides with the socles of all three $\mathbb{D}_2$-extensions L_i, and we get $\nu(\mathfrak{G}, K) = 3$.

Assume $l \equiv 9 \pmod{16}$. By Theorem 41, the socle of $K_{\mathbb{Z}_2}/K$ is again $K(\sqrt{-1}, \sqrt{2})$. The anti-cyclotomic extension $\mathbb{Q}(\sqrt{-1})_{\text{anti}}$ is a $\mathbb{D}_2$-extension of $\mathbb{Q}$ with base $\mathbb{Q}(\sqrt{-1})$ and socle $\mathbb{Q}(\sqrt{-1}, \sqrt{2})$. Hence the composite of $\mathbb{Q}(\sqrt{-1})_{\text{anti}}$ and K is a $\mathbb{D}_2$-extension of K with base $K(\sqrt{-1})$ and socle $K(\sqrt{-1}, \sqrt{2})$. This gives one $\mathfrak{G}$-extension of K.

Similarly, $\mathbb{Q}(\sqrt{-2})_{\text{anti}}K$ is a $\mathbb{D}_2$-extension of K with base $K(\sqrt{-2})$ and socle $K(\sqrt{-1}, \sqrt{2})$. This gives a second $\mathfrak{G}$-extension of K.

$\mathbb{Q}(\sqrt{-2l})_{\text{anti}}$ is a $\mathbb{D}_2$-extension of $\mathbb{Q}$ with base $\mathbb{Q}(\sqrt{-2l})$ and socle $\mathbb{Q}(\sqrt{-1}, \sqrt{-2l})$ or $\mathbb{Q}(\sqrt{-2}, \sqrt{-2l})$ by Theorem 46. Hence $\mathbb{Q}(\sqrt{-2l})_{\text{anti}}K$ is a $\mathbb{D}_2$-extension of K with base $K(\sqrt{2})$ and socle $K(\sqrt{-1}, \sqrt{2})$. This gives a third $\mathfrak{G}$-extension of K.

Finally assume $l \equiv 7 \pmod 8$. Then both K_{cycl} and K_{anti} have $K(\sqrt{2})$ as their first step. So the socle of $K_{\mathbb{Z}_2}/K$ is a D_4-extension of $\mathbb{Q}$ contained in the composite of

$$K_{\text{cycl}}^{(2)} = K\left(\sqrt{\sqrt{2} + 2}\right)$$

and $K_{\text{anti}}^{(2)}$.

$\mathbb{Q}(\sqrt{-2l})_{\text{anti}}$ is a $\mathbb{D}_2$-extension of $\mathbb{Q}$ with base $\mathbb{Q}(\sqrt{-2l})$ and socle $K(\sqrt{2})$. Hence $\mathbb{Q}(\sqrt{-2l})_{\text{anti}}$ is a $\mathbb{D}_2$-extension of K with base $K(\sqrt{2})$ and socle $\mathbb{Q}(\sqrt{-2l})_{\text{anti}}^{(2)}$. The question is whether this socle coincides with that of $K_{\mathbb{Z}_2}/K$. By the above, this happens exactly when the composite of $K_{\text{anti}}^{(2)}$ and $\mathbb{Q}(\sqrt{-2l})_{\text{anti}}^{(2)}$ contains $\sqrt{\sqrt{2} + 2}$. Now Theorem 60 gives the claim. □

Example. We show $\nu(\mathfrak{G}, K) = 2$ for $K = \mathbb{Q}(\sqrt{-353})$. We know from section 4.14 that $K_{\mathbb{Z}_2}/K$ has socle $K(\sqrt{-1}, \sqrt{2})$. The $\mathbb{D}_2$-extensions of K with bases

$K(\sqrt{-1})$ and $K(\sqrt{-2})$ both have socle $K(\sqrt{-1}, \sqrt{2})$ as in the proof above, so this gives two $\mathfrak{G}$-extensions of K.

From section 4.14 follows that $\mathbb{Q}(\sqrt{-2 \cdot 353})_{\text{anti}}$ is a $\mathbb{D}_2$-extension of K with base $K(\sqrt{2})$ and socle $\mathbb{Q}(\sqrt{-2 \cdot 353})^{(2)}_{\text{anti}}$. Since this socle is a D_4-extension of $\mathbb{Q}$, it does not coincide with that of $K_{\mathbb{Z}_2}/K$. Hence there is no third $\mathfrak{G}$-extension of K. □

Remark. When $K = \mathbb{Q}(\sqrt{-l})$ or $K = \mathbb{Q}(\sqrt{-2l})$ with a prime $l \equiv 3, 5 \pmod 8$, then K is 2-rational (Theorem 10). Hence the Galois group over K of the maximal 2-extension unramified outside 2 has rank 2. It follows from another result of Shafarevich (Theorem 5 in [26]) that the number of relations in this Galois group is 0. Thus it is isomorphic to the free pro-2-group F of rank 2. Now one gets immediately from Theorem 63 that F has exactly 3 closed, normal subgroups N with $F/N \cong \mathfrak{G}$ (although this of course could also be demonstrated directly). It follows that F can not be realised over a number field K if $\nu(\mathfrak{G}, K) < 3$ which is the case for instance for $K = \mathbb{Q}(\sqrt{-353})$ by the above example. It is not clear if there are any non-2-rational quadratic fields over which F is realisable.

Bibliography

[1] J. A. Antoniadis, *Diedergruppe und Reziprozitätsgesetz*, J. Reine Angew. Math. **377** (1987), 197–209.

[2] P. Barrucand, H. Cohn, *Notes on primes of type x^2+32y^2, class number and residuacity*, J. Reine Angew. Math. **238** (1969), 67–70.

[3] D. Brink, *On $\mathbb{Z}_p$-embeddability of cyclic p-class fields*, C. R. Math. Acad. Sci. Soc. R. Can. **27** (2005), 48–53.

[4] D. Brink, *Prime decomposition in the anti-cyclotomic extension* (submitted).

[5] G. Bruckner, *Charakterisierung der galoisschen Zahlkörper, deren zerlegte Primzahlen durch binäre quadratische Formen gegeben sind*, Math. Nachr. **32** (1966), 317–326.

[6] A. Brumer, *On the units of algebraic number fields*, Mathematika **14** (1967), 121–124.

[7] J. E. Carroll, H. Kisilevsky, *Initial layers of $\mathbb{Z}_l$-extensions of complex quadratic fields,* Compositio Math. **32** (1976), no. 2, 157–168.

[8] D. A. Cox, *Primes of the form x^2+ny^2*, Wiley, New York, 1989.

[9] L. E. Dickson, *Introduction to the theory of numbers*, University of Chicago, 1929. [Republished by Dover Publications, New York, 1957.]

[10] M. D. Fried, M. Jarden, *Field Arithmetic*, Springer, Berlin, 1986.

[11] C. F. Gauss, *Disquisitiones Arithmeticae*, Leipzig, 1801. [Republished as volume 1 in *Werke*, Königliche Gesellschaft der Wissenschaften zu Göttingen, 1870.]

[12] W.-D. Geyer, C. U. Jensen, *Prodihedral groups as Galois groups over number fields,* J. Number Theory **60** (1996), no. 2, 332–372.

[13] H. Hasse, *Über die Klassenzahl des Körpers $P(\sqrt{}-p)$ mit einer Primzahl $p \equiv 1$ mod. 2^3,* Aequationes Math. **3** (1969), 165–169.

[14] H. Hasse, *Über die Klassenzahl des Körpers $P(\sqrt{}-2p)$ mit einer Primzahl $p \neq 2$,* J. Number Theory **1** (1969), 231–234.

[15] H. Hasse, *Über die Teilbarkeit durch* 2^3 *der Klassenzahl imaginärquadratischer Zahlkörper mit genau zwei verschiedenen Diskriminantenprimteilern,* J. Reine Angew. Math. **241** (1970), 1–6.

[16] E. Hecke, *Theorie der Algebraischen Zahlen*, Akademische Verlagsgesellschaft, Leipzig, 1923.

[17] B. Huppert, *Endliche Gruppen I*, Springer, Berlin, 1967.

[18] K. Iwasawa, *On $\mathbb{Z}_l$-extensions of algebraic number fields*, Ann. of Math. (2) **98** (1973), 246–326.

[19] J.-P. Jaulent, T. Nguyen Quang Do, *Corps p-rationnels, corps p-réguliers, et ramification restreinte,* J. Théor. Nombres Bordeaux **5** (1993), 343–363.

[20] T. Kubota, *Über den bizyklischen biquadratischen Zahlkörper,* Nagoya Math. J. **10** (1955), 65–85.

[21] H. W. Leopoldt, *Zur Arithmetik in abelschen Zahlkörpern,* J. Reine Angew. Math. **209** (1962), 54–71.

[22] J. Neukirch, *Algebraische Zahlentheorie*, Springer, Berlin, 1992.

[23] L. Rédei, H. Reichardt, *Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers,* J. Reine Angew. Math. **170** (1934), 69–74.

[24] A. Scholz, *Über die Beziehung der Klassenzahlen quadratischer Körper zueinander,* J. Reine Angew. Math. **166** (1932), 201–203.

[25] J.-P. Serre, *Topics in Galois Theory*, Jones and Bartlett, Boston, 1992.

[26] I. R. Shafarevich, *Extensions with given ramification points* (Russian), Inst. Hautes Études Sci. Publ. Math. **18** (1963), 71–95. [Translation in *Collected mathematical papers*, Springer, Berlin, 1989, pp. 295–316.]

[27] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer, New York, 1982.