ABSTRACT

Title of Dissertation: CYCLOTOMIC $\mathbb{Z}_2$-EXTENSION OF REAL QUADRATIC FIELDS WITH CYCLIC IWASAWA MODULE

Josue Avila Artavia
Doctor of Philosophy, 2024

Dissertation Directed by: Professor Niranjan Ramachandran
Department of Mathematics

For a number field K and a prime p, let K_∞ denote the cyclotomic $\mathbb{Z}_p$-extension of K, and A_n denote the p-primary part of the class group of its n-th layer K_n. Greenberg conjectured that for a totally real field, the order of A_n becomes constant for sufficiently large n.

Motivated by the work of Mouhib and Movahhedi, we focus on the case where $p = 2$ and K is a real quadratic field such that the Iwasawa module $X_\infty = \varprojlim A_n$ is cyclic. They determined all such fields and proved that Greenberg's conjecture holds for some cases.

In this dissertation, we provide new examples of infinite families of real quadratic fields satisfying Greenberg's conjecture which were not covered completely in the work of Mouhib and Movahhedi. To achieve this, we use the theory of binary quadratic forms and biquadratic extensions to determine a fundamental system of units and the class number of the first few layers of the cyclotomic $\mathbb{Z}_2$-extension. Additionally, in certain cases, we can determine the size of the module X_∞ and the level of the cyclotomic tower where the size of A_n becomes constant.

CYCLOTOMIC $\mathbb{Z}_2$-EXTENSION OF REAL QUADRATIC FIELDS WITH CYCLIC IWASAWA MODULE

by

Josue Avila Artavia

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland, College Park in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
2024

Advisory Committee:
Professor Niranjan Ramachandran, Chair/Advisor
Professor Lawrence Washington
Professor Amin Gholampour
Professor Harry Tamvakis
Professor William Gasarch

ACKNOWLEDGMENTS

This has been a long journey and I would like to dedicate a couple of pages to thank everyone who supported me during this process.

First and foremost, I would like to thank my advisor Professor Niranjan Ramachandran. He has been really helpful in guiding me throughout these years. Being able to find this project gave me a lot of motivation towards the end and reignited my passion for mathematics. I am forever grateful for the time and effort invested in me.

I would also like to thank Professor Lawrence Washington for always keeping his door open to me and helping me so much in this project. Discussing math with him was one of my favorite parts of the graduate program and I will always be thankful for this opportunity.

I would like to thank my family for their support during this process, especially my mom, brothers, dad, and late uncle, who were always there for me. To all my friends back home, for which I particularly mention Natalia (who helped me with some of the coding to test the cases), Rebeca, Carlos, Raquel, Xinia, Karla, Eva, Oscar, Nathaly, and Daniela. To my math and actuarial sciences friends from Costa Rica who keep in contact with me despite all of us going to different parts of the world: Aurelio, Alex, Jorge, Andy, German, Sofia, Ana.

To all the great people I met at the University of Maryland, all my math friends who helped me through this process: Nelson, Tahseen (who helped me with the coding and the presentation), Geoffrey, Keith, Chengze, Haeyun, and everyone from the original crew. To all my friends outside of mathematics: Mark, Jack, my Latin friends from whom I mention Jose and Jhayron, and all the members of my soccer team. You all were a big part of my graduate school experience and I will treasure all the moments we had together. I apologize

if I let someone out.

Finally, I would like to thank the University of Costa Rica for preparing me to study abroad and providing financial support when needed. This institution provided me with all the bases I needed for my first years of graduate school and for that I am grateful.

Table of Contents

List of Tables

Chapter 1

Introduction and background

1.1 Introduction

Let $K = \mathbb{Q}(\sqrt{D})$ be a real quadratic field and $\mathbb{Z}_2 = \varprojlim \mathbb{Z}/2^n\mathbb{Z}$ is the additive group of 2-adic integers. We shall use K_∞ to denote the cyclotomic $\mathbb{Z}_2$-extension of K. Let K_n denote its n-th layer and A_n the 2-Sylow subgroup of the class group of K_n, which we refer to simply as the 2-class group of K_n.

In [25], Mouhib and Movahhedi determined all real quadratic fields with non-trivial cyclic Iwasawa module X_∞ (Theorem 2.3.9) and proved that Greenberg's conjecture is satisfied under certain restrictions, as will be presented in Chapter 2. In this dissertation, we will focus our attention on the following cases:

1. $D = pq$, with $p \equiv 5 \mod 8$ and $q \not\equiv 1 \mod 8$.

2. $D = pq_1q_2$ with $p \equiv 5 \mod 8$, $q_1 \equiv 3 \mod 8$ and $q_2 \equiv 3 \mod 4$.

3. $D = pq$, with $p \equiv 5 \mod 8$ and $q \equiv 1 \mod 8$, with $\left(\frac{2}{q}\right)_4 \neq (-1)^{\frac{p-1}{8}}$.

These are infinite families of real quadratic fields (by Dirichlet's theorem on arithmetic progressions), and they were not covered completely in [25] or analyzed by anyone else:

In the first case, it is known since [27] that X_∞ is finite. In Chapter 3, we prove that for $q \equiv 3 \mod 4$ the Iwasawa module X_∞ is isomorphic to A_0. For $q \equiv 5 \mod 8$ this holds in some cases of Theorem 1.2.6. This case will be discussed in Chapter 3 and Chapter 4, as it leads to possible ideas for future research.

In the second case, when $q_2 \equiv 7 \mod 8$ the Iwasawa module X_∞ is finite [25]. Moreover, in [14] the authors proved that $X_\infty \cong A_0$ under certain restrictions for $q_2 \equiv 3 \mod 4$, using the properties of the biquadratic field K_1. In Chapter 3, we draw some conclusions about their results using our methods and provide a new example of Greenberg's conjecture using the field K_2 instead.

Finally, in the third case, we use some of the conditions present in [29] (Theorem 1.2.6) and the ideas in [25], to provide new examples in Chapter 3.

It is worth mentioning that similar problems can be found in the literature. For instance, if $K = \mathbb{Q}(\sqrt{-D})$ is an imaginary quadratic extension, it is known that the Hilbert 2-class field tower is infinite if D has at least 6 prime divisors ([6], Chapter 9). It has been conjectured that the same is true if D has at least 5 prime divisors, but only case-by-case analysis works (see for example, [5]).

1.2 Preliminary concepts

In this section, we introduce some of the main concepts from number theory that will be used throughout this dissertation. For readers less familiar with the topic, we start with a background discussion on class groups and prime factorization on number fields. After that, we discuss some of the main results and ideas that will serve as references in the next chapters. The notation we will use will be defined within the text, mainly in the first two

chapters.

1.2.1 Class groups and ramification ([26])

We define a number field K as a finite extension of $\mathbb{Q}$. An element α of K is an algebraic integer if it satisfies a monic polynomial equation of the form

$$\alpha^n + c_1\alpha^{n-1} + \cdots + c_n = 0,$$

with coefficients $c_1, \cdots, c_n$ in $\mathbb{Z}$. The set of algebraic integers forms a subring $\mathcal{O}_K$ of K, known as the ring of integers. Moreover, $\mathcal{O}_K$ is a Dedekind domain, which implies that every ideal has a unique factorization into prime ideals.

A fractional ideal of K is a finitely generated $\mathcal{O}_K$-submodule of K. The group $\mathcal{I}_K$ of fractional ideals is the free abelian group generated by the nonzero prime ideals of $\mathcal{O}_K$ under multiplication. The subgroup $\mathcal{P}_K$ of principal fractional ideals consists of elements generated by non-zero elements of K. The subgroup $\mathcal{P}_K^+$ of $\mathcal{P}_K$ is the set of principal ideals generated by elements that are positive under all real embeddings. We define the class group $Cl(K)$ and the narrow class group $Cl^+(K)$ of K as:

$$Cl(K) = \mathcal{I}_K/\mathcal{P}_K.$$
$$Cl^+(K) = \mathcal{I}_K/\mathcal{P}_K^+.$$

Both of these two groups are finite. The orders of these groups are the class number $h(K)$ and the narrow class number $h^+(K)$. For brevity, we will denote them as h and h^+ when the underlying field is clear. We are interested in predicting the growth of the class number within specific chains of number fields, using ramification and genus theory.

Let K/k be a finite Galois extension of number fields. Each prime ideal p of $\mathcal{O}_k$ has a unique factorization in $\mathcal{O}_K$ of the form

$$p\mathcal{O}_K = (\mathcal{B}_1 \cdots \mathcal{B}_g)^e .$$

For any $\mathcal{B}_i$, the degree $f = [\mathcal{O}_K/\mathcal{B}_i : \mathcal{O}_k/p]$ remains the same, and it is called the inertia degree. The prime p is ramified if $e > 1$, and it is totally ramified if $g = f = 1$. The prime p splits completely, or simply splits, if $e = f = 1$. The prime is inert if $g = e = 1$ (i.e. if it remains a prime ideal in $\mathcal{O}_K$). For the sake of simplicity, the extension K/k is said to be ramified at infinity whenever k is real and K is imaginary, as we will only focus on Galois extensions.

One of the main results of Class Field Theory, which we will utilize, is the existence of a unique finite Galois extension H/K corresponding to the maximal unramified abelian extension of K, such that the Galois group $\mathrm{Gal}(H/K)$ is isomorphic to the class group of K via the Artin map. This extension is commonly known as the Hilbert class field of K, and by the Galois correspondence, every abelian unramified extension of K corresponds to a subextension of H/K. In particular, there is an unramified extension, called the p-class field of K, such that its Galois group over K is the p-Sylow subgroup of $Cl(K)$. We will refer to this group simply as the p-class group of K. An ideal I of $\mathcal{O}_K$ capitulates in an extension L if $I\mathcal{O}_L$ is principal. Through the Artin map, one can deduce that a prime splits completely in H if and only if it is principal in K ([8], Corollary 5.21, Corollary 5.25).

We will focus on quadratic extensions of $\mathbb{Q}$, which are fields of the form $K = \mathbb{Q}(\sqrt{D})$ with D being a square-free integer. As they are well understood, we write down some of

their main properties. The ring of integers $\mathcal{O}_K$ can be characterized as:

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}\left[\sqrt{d_K}\right] & \text{if } D \equiv 2,\ 3 \mod 4, \\ \mathbb{Z}\left[\frac{1+\sqrt{d_K}}{2}\right] & \text{if } D \equiv 1 \mod 4. \end{cases}$$

Define the discriminant d_K as:

$$d_K = \begin{cases} D & \text{if } D \equiv 1 \mod 4, \\ 4D & \text{if } D \equiv 2, 3 \mod 4. \end{cases}$$

Then a prime ramifies in $\mathcal{O}_K$ if and only if it divides d_K. Furthermore, if p is an odd prime we can define the Legendre (or Jacobi) symbol by

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

where a is a quadratic residue if the equation $x^2 \equiv a \mod p$ has a solution.

It can be extended multiplicatively by $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, and it determines the factorization in K, as a prime p splits in K if and only if $\left(\frac{d_K}{p}\right) = 1$. For the case $p = 2$, the prime splits if $D \equiv \pm 1 \mod 8$ and it is inert if $D \equiv \pm 5 \mod 8$. Thus, we can simply define the Legendre symbol for $a \equiv 1 \mod 4$ by $\left(\frac{a}{p}\right) = 1$ if and only if p splits in $\mathbb{Q}(\sqrt{a})$. This will become important once we discuss Rédei matrices. If r is a positive divisor of d_K with $r \equiv 1 \mod 4$, it is a well-known result ([31], Exercise 9.3) that the extension $K(\sqrt{r})/K$ is unramified at all primes.

Finally, for any real number field K of degree n over $\mathbb{Q}$, let $E(K)$ represent the unit group

of $\mathcal{O}_K$. Then by Dirichlet's unit theorem, $E(K)$ is isomorphic to $\langle -1 \rangle \times \mathbb{Z}^{n-1}$, meaning its torsion is generated by -1 and its $\mathbb{Z}$-rank is $n-1$. In particular, for real quadratic fields, we can choose a generator $\varepsilon > 1$, referred to as the fundamental unit of K.

Remark 1.2.1. An important fact we will use is that the class group and narrow class group are equal if and only if $N_{K/\mathbb{Q}}(\varepsilon) = -1$, where $N_{K/\mathbb{Q}}$ denotes the norm map from K to $\mathbb{Q}$. Otherwise, if $N_{K/\mathbb{Q}}(\varepsilon) = 1$, we have $2h = h^+$, Several properties regarding fundamental units will be discussed in future sections.

1.2.2 Binary quadratic forms and genus theory ([8] , [12], [18])

In this section, we discuss the relation between binary quadratic forms and the class groups of quadratic fields. It is worth noting that the standard notations for this topic are the ones used in Cox's book [8], which primarily focuses on imaginary quadratic fields. For real quadratic fields, the main ideas were originally introduced by Gauss [12]. As it is one of our main references, we will adhere to the notation presented by Kaplan [18], just for consistency with our results. We are particularly interested in Pell's equation

$$x^2 - ny^2 = -1 \text{ or } -4,$$

as it determines whether the norm of the fundamental unit is -1 or not. Thus, the binary quadratic form $x^2 - ny^2$ is one of our main objects of study.

A binary quadratic form is a homogeneous polynomial of degree 2 in $\mathbb{Z}[x, y]$. We only consider those of the form $Q(x, y) = ax^2 + 2bxy + cy^2$, where the second coefficient is even. We denote the form by $Q = [a, b, c]$. The condition regarding the second coefficient is the main difference from the usual definition. As established in [18], there is a map between the group we will define using this restriction and the usual definition, where the kernel is

a group of order 1 or 3 (in the latter case, it is isomorphic to $SL_2(\mathbb{Z}/2\mathbb{Z})$). Since we will mainly focus on the 2-part of a group, there will be no difference in the overall theory.

A form $Q(x,y) = [a,b,c]$ is primitive if $g.c.d.\,(a,2b,c) = 1$. We say that an integer m is represented by Q if the equation $Q(x,y) = m$ has an integral solution, and it is properly represented if x, y can be chosen such that $gcd(x,y) = 1$. The discriminant of Q is defined as $D = b^2 - ac$ (which is different from the usual definition, since it disregards the factor of 4).

The group $SL_2(\mathbb{Z})$ (invertible matrices with integral coefficients and determinant 1) has a discriminant-preserving action on the group of quadratic forms. If $Q = [a,b,c]$ and $M = \left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$, then M acts on Q by

$$M \cdot Q(x,y) = Q(px + ry, qx + sy).$$

Two forms are equivalent if they lie in the same orbit. We denote the equivalence classes of forms of discriminant D by $C(D)$, which form a group under what is known as Gauss composition: for two given classes $\mathcal{Q}_1, \mathcal{Q}_2$, there exist representatives of the form $[A, B, A'C]$, $[A', B, AC]$ respectively. Then the composition is defined as the class of the form $[AA', B, C]$. The unit of this group is given by the class $\mathcal{F}$ of $f = [1, 0, -D]$, which will be referred to as the principal form. As established in ([12],[18]), the 2-part of the narrow class group of $K = \mathbb{Q}(\sqrt{D})$ is isomorphic to 2-part of $C(D)$.

The ambiguous classes of $C(D)$ are the elements of order 2. A quadratic form is ambiguous simple if it is of the form $[A, 0, C]$ with $|A| < |C|$, or $[2B, B, E]$ with $|B| < |2E - B|$. The second type only exists if $D \not\equiv 1 \mod 4$. When $D > 0$, each ambiguous class contains two ambiguous simple representatives, whereas there is only one for $D < 0$. In particular, every ambiguous class represents divisors of the discriminant of K, as equivalent classes rep-

resent the same numbers. The divisors of d_K represented by the principal form are called the principal factors. To illustrate how to use these concepts, if $[1, 0, -D]$ and $[-1, 0, D]$ are in the same class, then -1 is represented by $[1, 0, -D]$, implying it is a norm from the corresponding quadratic extension.

For a finite abelian group G, we can define the 2^n-rank of G as

$$r_{2^n}(G) = \dim_{\mathbf{F}_2} \left(G^{2^{n-1}} / G^{2^n} \right),$$

where $\mathbf{F}_2$ represents the finite field of 2 elements. A result due to Gauss is that the 2-rank of the narrow class group of K, denoted by r_2 for simplicity, satisfies

$$r_2 = r - 1, \tag{1.1}$$

where r is the number of divisors of the discriminant d_K.

Similar to the case for imaginary quadratic fields [8], one can define the generic characters of a given form as follows: If p is an odd divisor of D, any integer m relatively prime to p, that is represented by a form Q of discriminant D, has the same value $e_p(Q) = \left(\frac{m}{p}\right)$, called the generic character associated to p. Similarly, if 2 divides the discriminant, the character $e_2(Q)$ is defined as:

$$e_2(Q) = \begin{cases} \left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}} & \text{if } D \equiv -1 \mod 4, \\ \left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}} & \text{if } D \equiv 2 \mod 8, \\ \left(\frac{-2}{m}\right) & \text{if } D \equiv 6 \mod 8. \end{cases}$$

Two classes are in the same genus if their generic characters have the same values. We define the principal genus to be the genus of the principal form. In particular, a class is

in the principal genus if the value of every generic character is equal to 1. Similar to the imaginary case, let s be the number of ambiguous simple forms in the principal genus, then

$$s = 2^{\,r_4+1}, \tag{1.2}$$

where r_4 is the 4-rank of the group $Cl^+(K)$. We provide an example of how to use these ideas, but a better criterion will be introduced with the Rédei-Reichardt matrix.

Example 1.2.2. Let $D = pq$ with $p \equiv 5 \mod 8$ and $q \equiv 3 \mod 4$. The simple ambiguous forms for $K = \mathbb{Q}(\sqrt{D})$ are given by ([18], Proposition A_3):

$$f = [1, 0, -pq],\ g = [p, 0, -q],\ h = \left[2, 1, \frac{1-pq}{2}\right],\ l = \left[2p, p, \frac{p-q}{2}\right],$$

$$\overline{f} = [-1, 0, pq],\ \overline{g} = [q, 0, -p],\ \overline{h} = \left[-2, 1, \frac{pq-1}{2}\right],\ \bar{l} = \left[2q, q, \frac{q-p}{2}\right].$$

Let $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = \tau$, $\left(\frac{2}{p}\right) = \tau'$ and $\left(\frac{2}{q}\right) = \tau''$. The generic characters are the ones in the following table:

	f	$\overline{f}$	g	$\overline{g}$	h	$\overline{h}$	l	$\bar{l}$
$\left(\frac{m}{p}\right)$	1	1	τ	τ	τ'	τ'	$\tau\tau'$	$\tau\tau'$
$\left(\frac{m}{q}\right)$	1	-1	τ	$-\tau$	τ''	τ''	$\tau\tau''$	$-\tau\tau''$
$(-1)^{\frac{m-1}{2}}$	1	-1	1	-1	$\tau'\tau''$	$-\tau'\tau''$	$\tau'\tau''$	$-\tau'\tau''$

Table 1.1: Generic character for $D = pq$, $p \equiv 5 \mod 8$, $q \equiv 3 \mod 8$

By the modular conditions, we have $\tau' = -1$. In particular, depending on the values of τ and τ'', exactly one of the forms g, l or $\bar{l}$ is in the principal genus. Hence $r_4 = 0$, as there are only 2 forms in the principal genus. Since $r_2 = 2$, one can easily conclude that the 2-part

of the narrow class group is isomorphic to $C_2 \times C_2$, where C_2 represents the cyclic group of 2 elements.

1.2.3 Rédei-Reichardt matrix [28]

In this section, we present what is known as the Rédei-Reichardt criterion, as it will be easier to determine the 4-rank this way. As explained in the previous section, $r_2(Cl^+(K)) = r - 1$, where r is equal to the number of divisors of the discriminant. Therefore, the 2-torsion group $Cl^+(K)[2]$ is isomorphic to $\mathbf{F}_2^{r-1}$.

Consider the group $Cl^+(K)/Cl^+(K)^2$. Since it is a quotient of $Cl^+(K)$, there is a corresponding intermediate extension H^* of H/K, where H is the Hilbert class field of K, such that $\mathrm{Gal}(H^*/K) \cong Cl^+(K)/Cl^+(K)^2$ via the Galois correspondence. This extension is known as the genus field of K [8], and it corresponds to the maximal abelian extension of K that is unramified at the finite primes and is also abelian over $\mathbb{Q}$.

This is proved in ([8], Theorem 6.1) for imaginary quadratic fields, but the same ideas work here: Let H_2 be the narrow class field of K; i.e., the abelian unramified extension of K such that $\mathrm{Gal}(H_2/K) \cong Cl^+(K)$. Then there is an exact sequence

$$1 \longrightarrow Cl^+(K) \longrightarrow \mathrm{Gal}(H_2/\mathbb{Q}) \longrightarrow \mathrm{Gal}(K/\mathbb{Q}) \longrightarrow 1.$$

If $\mathrm{Gal}(K/\mathbb{Q}) = \langle\sigma\rangle$, since the class group of $\mathbb{Q}$ is trivial, the norm map from K to $\mathbb{Q}$ is trivial in ideal classes. Thus, σ acts as inversion in $\mathrm{Gal}(H_2/\mathbb{Q})$ and this group is dihedral over $\mathbb{Q}$ (in particular, the Hilbert class field can be non-abelian over $\mathbb{Q}$). From here, the proof follows the same steps as in ([8], Theorem 6.1), with the only difference being that the genus field extension might be ramified at the infinite places since the class group and narrow class group can be different. It is worth noting that we can only draw conclusions

on the 2-part of the class groups, which is an advantage that disappears when working with any other prime.

The genus field is determined in the following way: if p is an odd prime number we can define $p^* = (-1)^{\frac{p-1}{2}}p$; otherwise, for $p = 2$ the definition relates to the corresponding generic character, since

$$2^* = \begin{cases} -4 & \text{if } D \equiv 3 \mod 4, \\ 8 & \text{if } D \equiv 2 \mod 8, \\ -8 & \text{if } D \equiv 6 \mod 8. \end{cases}$$

Then H^* is the composite of the quadratic extensions $\mathbb{Q}(\sqrt{p^*})$ such that $p \mid d_K$. In particular, $\mathrm{Gal}(H^*/K) \cong Cl^+(K)/Cl^+(K)^2$ injects into $\mathrm{Gal}(H^*/\mathbb{Q}) \cong \mathbf{F}_2^{r-1}$.

To determine the 4-rank of $Cl^+(K)$, we can consider a series of maps. We have a surjection

$$\mathbf{F}_2^r \longrightarrow Cl^+(K)[2].$$

Restricting the natural projection of $Cl^+(K)$ onto $Cl^+(K)/Cl^+(K)^2$ to the torsion subgroup, we have a map

$$Cl^+(K)[2] \xrightarrow{\psi} Cl^+(K)/Cl^+(K)^2.$$

Composing these maps with the injection into $\mathrm{Gal}(H^*/\mathbb{Q})$, we get the Rèdei-Reichardt map

$$\mathbf{F}_2^r \xrightarrow{\Psi} \mathbf{F}_2^r.$$

One can see that the kernel of this map has order equal to 2^{r_4}. Therefore,
$r_4 = r - 1 - \mathrm{rank}_{\mathbf{F}_2}(\Psi)$. This map corresponds to a matrix R with $\mathbf{F}_2$ coefficients, which are easily determined by the Artin symbol (for quadratic fields, it is determined by the Legendre symbol).

Let $R = (a_{ij})$ and suppose $d_k = p_1 \cdots p_n$ is written as a product of primes. Then for $i \neq j$ we have

$$(-1)^{a_{ij}} = \left(\frac{p_j^*}{p_i}\right).$$

The sum of the entries in every row is 0, hence the entries c_{ii} are easily determined. This matrix is known as the Rédei-Reichardt matrix of K and we have the following formula

$$r_4 = r - 1 - \text{rank}(R) = r_2 - \text{rank}(R) \tag{1.3}$$

Example 1.2.3. We present as an example again what happens if $K = \mathbb{Q}(\sqrt{pq})$ with $p \equiv 5 \mod 8$ and $q \equiv 3 \mod 4$. By the modular condition, both symbols with respect to $p = 2$ are equal to -1, and by quadratic reciprocity we have $\left(\frac{p^*}{q}\right) = \left(\frac{q^*}{p}\right)$. Since $d_K = 4pq$, there are 3 divisors of the discriminant and we get a 3×3 matrix. If $\left(\frac{p}{q}\right) = 1$, the two possible matrices are

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix};$$

both of rank 2, which implies $r_4 = 3 - 1 - 2 = 0$.

Similarly, when $\left(\frac{p}{q}\right) = -1$, the 2 possible matrices are

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix};$$

where again, we get $r_4 = 0$. We can then conclude that the 2-part of $Cl^+(K)$ is $C_2 \times C_2$.

Remark 1.2.4. A well-known result we present is that the fundamental unit has norm equal to 1 whenever a prime $q \equiv 3 \mod 4$ divides D, where $K = \mathbb{Q}(\sqrt{D})$. Let $\varepsilon_D = x + y\sqrt{pq}$ with x, y integers and assume by contradiction that $x^2 - Dy^2 = -1$. Then $x^2 \equiv -1 \mod q$ leads to $\left(\frac{-1}{q}\right) = (-1)^{\frac{q-1}{2}} = 1$, which is absurd. In the previous example, this implies that the class group differs by 2 from the narrow class group (Remark 1.2.4), and the 2-class group of K is isomorphic to C_2. In particular, since the extension $\mathbb{Q}(\sqrt{p}, \sqrt{q})$ is unramified of degree 2, it corresponds to the 2-class field.

1.2.4 Biquadratic symbol and the 8-rank of the class group ([18], [12])

The conditions for the 8-rank are far more complicated. We must consider the classes Q that have a square root $\overline{Q}$; i.e., $Q = \overline{Q}^2$. Let $r_8 = r_8\left(Cl^+(K)\right)$ be the 8-rank of the narrow class group of K. Then $2^{\,r_8+1}$ is equal to the number of simple ambiguous forms such that there is a square root in the principal genus. Thus, we need to calculate the generic characters of the square roots to determine which ones belong to the principal genus. To this end, we introduce the biquadratic symbol:

For $p \equiv 1 \mod 4$, whenever $\left(\frac{a}{p}\right) = 1$, the biquadratic symbol $\left(\frac{a}{p}\right)_4$ is equal to 1 if a is a biquadratic residue modulo p (meaning the equation $x^4 \equiv a \mod p$ has a solution), and it is equal to -1 otherwise.

We can also define the biquadratic symbol for $p = 2$ whenever $a \equiv 1 \mod 8$. Then $\left(\frac{a}{2}\right)_4 = (-1)^{\frac{a-1}{8}}$, where it is equal to 1 if $a \equiv 1 \mod 16$ and it is -1 if $a \equiv 9 \mod 16$.

Example 1.2.5. Suppose $D = pq$ with $p \equiv q \equiv 1 \mod 4$. Let $g = [p, 0, -q]$. By [18], there exists a square root φ of g such that $e_p(\varphi) = \left(\frac{p}{q}\right)_4$. Thus, the generic character of a square root depends entirely on the biquadratic symbol.

We end this section with the following result by Scholz, which will be significant to our analysis:

Theorem 1.2.6. *([29], **cf.** [17] , Proposition 2.2), Let N denote the norm map from K to $\mathbb{Q}$, and h, h^+ denote respectively the class number and the narrow class number of K. Assume $p \equiv q \equiv 1 \pmod 4$. The following statements hold:*

1. *If $\left(\frac{p}{q}\right) = -1$, then $h^+ \equiv h \equiv 2 \pmod 4$ and $N(\varepsilon_D) = -1$.*
2. *If $\left(\frac{p}{q}\right) = 1$, then:*
   - *(i) If $\left(\frac{p}{q}\right)_4 = -\left(\frac{q}{p}\right)_4$, then $h^+ \equiv 2h \equiv 4 \pmod 8$ and $N(\varepsilon_D) = 1$.*
   - *(ii) If $\left(\frac{p}{q}\right)_4 = \left(\frac{q}{p}\right)_4 = -1$, then $h^+ \equiv h \equiv 4 \pmod 8$ and $N(\varepsilon_D) = -1$.*
   - *(iii) If $\left(\frac{p}{q}\right)_4 = \left(\frac{q}{p}\right)_4 = 1$, then $h^+ \equiv 0 \pmod 8$.*

Remark 1.2.7. These conditions mainly determine which ambiguous simple classes are equivalent to the unit, since the biquadratic symbols determine the generic characters. For example, the condition $\left(\frac{p}{q}\right)_4 = \left(\frac{q}{p}\right)_4 = -1$ is equivalent to $[-1, 0, D]$ being the only form equivalent to $[1, 0, -D]$, hence -1 is a norm from the quadratic field to $\mathbb{Q}$.

The condition $\left(\frac{p}{q}\right)_4 = -\left(\frac{q}{p}\right)_4 = 1$ implies that the class of $[q, 0, -p]$ is equivalent to $[1, 0, -D]$ instead. Hence, the equation $x^2 - Dy^2 = q$ has a solution instead. In this case, the prime q is a principal factor of K. As mentioned in [17], only one of p, q, -1 is represented by $[1, 0, -D]$. This will be relevant to our analysis in future chapters.

1.3 $\mathbb{Z}_p$-extensions and Iwasawa theory [31], [16]

Let $\mathbb{Z}_p$ denote the additive group of p-adic integers. A $\mathbb{Z}_p$-extension of a given number field K is an extension K_∞/K with $\mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$. The intermediate fields of this extension correspond to the closed subgroups of $\mathbb{Z}_p$. Thus, for each $n \geq 0$ there is a unique extension K_n/K contained in K_∞ with $\mathrm{Gal}(K_n/K) \cong \mathbb{Z}/p^n\mathbb{Z}$. All $\mathbb{Z}_p$-extensions are unramified at primes that do not lie over p. Furthermore, at least one prime over p ramifies, and there exists an $n_0 \geq 0$ such that every ramifying prime is totally ramified in K_∞/K_{n_0}. We denote n_0 to be the smallest integer with this property.

Let $\Gamma = \mathrm{Gal}(K_\infty/K)$. Let L_n denote the maximal unramified abelian p-extension of K_n, so that the Galois group $X_n = \mathrm{Gal}(L_n/K_n)$ is isomorphic to the p-class group of K_n, which we denote by A_n. Let $L = \bigcup_{n=o}^{\infty} L_n$. The inverse limit $X_\infty = \varprojlim A_n \cong \mathrm{Gal}(L/K_\infty)$ is known as the Iwasawa module of the extension. Let $\Lambda = \mathbb{Z}_p[\![T]\!]$. Then X is a finitely generated Λ-torsion module.

Let $|A_n| = p^{e_n}$. Using the structure of Λ-modules, Iwasawa proved that n for sufficiently large, there exist integers $\mu \geq 0$, $\lambda \geq 0$, and ν such that

$$e_n = \lambda n + \mu p^n + \nu.$$

As it will be our main object of study, we construct a particular $\mathbb{Z}_p$-extension. Let $q = p$ if p is odd and $q = 4$ if $p = 2$. Denote by ζ_{qp^n} a primitive qp^n root of unity. Since

$\mathrm{Gal}(\mathbb{Q}(\zeta_{qp^n}) \cong (\mathbb{Z}/q\mathbb{Z})^* \times \mathbb{Z}/p^n\mathbb{Z}$, there exists a subfield $\mathbb{Q}_n$, which is cyclic of degree p^n. Then $\mathbb{Q}_\infty = \bigcup_{n=o}^{\infty} \mathbb{Q}_n$ is a $\mathbb{Z}_p$-extension of $\mathbb{Q}$, and it can be easily shown that $K_\infty = K\dot{\mathbb{Q}}_\infty$ is a $\mathbb{Z}_p$-extension of K, which is referred to as the cyclotomic $\mathbb{Z}_p$-extension of K.

Since we will use genus theory, the results of binary quadratic forms in [18] and Kubota's work on biquadratic fields [19] as some of our main tools, we will restrict our attention to the case $p = 2$. We can easily describe $\mathbb{Q}_n = \mathbb{Q}(a_n)$ by the sequence $a_0 = 0$, $a_n = \sqrt{2 + a_{n-1}}$ for $n \geq 1$. If $K = \mathbb{Q}(\sqrt{D})$ is a real quadratic field, then $K_n = \mathbb{Q}(a_n, \sqrt{D})$. It is worth noting that the extension is the same if we replace D with $2D$, so we can use either extension at our convenience. We also point out that $K_1 = \mathbb{Q}(\sqrt{2}, \sqrt{D})$ and $K_2 = \mathbb{Q}\left(\sqrt{2+\sqrt{2}}, \sqrt{D}\right)$, since they will be significant to our analysis. In particular, K_1 is a biquadratic field, so we can use this in our favor to deduce some of the properties of the cyclotomic extension.

For abelian extensions $K/\mathbb{Q}$, it is well-known that the invariant μ of the cyclotomic extension is equal to 0 [9]. For totally real fields, it was conjectured by Greenberg [13] that both invariants λ, μ vanish, and the sequence stabilizes for large enough n. In the next chapter, we discuss some results related to real quadratic fields regarding this conjecture.

Chapter 2

Real quadratic fields with cyclic Iwasawa module

In this chapter, we lay out some of the main results and theorems that will be essential in the next chapter.

2.1 Greenberg's conjecture and results [13]

Let K be a totally real number field. Greenberg has conjectured (and this is expected to be true but has turned out to be very hard to prove in general) that the order of the class groups in the cyclotomic $\mathbb{Z}_p$ extension is uniformly bounded, which is equivalent to the invariants μ and λ from the previous chapter being equal to 0. For some of his results, Greenberg assumes that the field K satisfies Leopoldt's conjecture, which for totally real fields is equivalent to the p-adic regulator of the number field K being non-zero, in its simplest form. This conjecture has been proved for abelian extensions of $\mathbb{Q}$, so our main fields of interest will satisfy it. We present some of the results, as they will be useful in future chapters.

Let $\widetilde{K}$ be the composite of all $\mathbb{Z}_p$ extensions of K with $\mathrm{Gal}(\widetilde{K}/K) \cong \mathbb{Z}_p^n$. Then Leopoldt's conjecture is equivalent to $n = l_2 + 1$, where l_2 denotes the number of complex embeddings of K. In particular, for a totally real field, it is equivalent to the cyclotomic extension K_∞ being the only $\mathbb{Z}_p$ extension. Let M_0 denote the maximal abelian p-extension unramified outside of p, then $[M_0 : \widetilde{K}]$ is finite [31]. If K is totally real and satisfies Leopoldt's conjecture, this is equivalent to $[M_0 : K_\infty] < \infty$.

Let σ be a topological generator of $\mathrm{Gal}(K_\infty/K)$. By restricting σ to $\mathrm{Gal}(K_n/K)$, we have a generator of this group, which we also denote by σ. It acts on the class group A_n and we can consider the fixed elements of this action:

$$B_n = A_n^{\mathrm{Gal}(K_n/K)} = \{c \in A_n \mid c^\sigma = c\}.$$

Greenberg proves that if K is totally real and satisfies Leopoldt's conjecture, then for n sufficiently large, $|B_n| \leq [M_0 : K_\infty]$.

Moreover, it is worth mentioning the following criterion for the vanishing of the invariants, as it relates to the unit index studied in Theorem 2.3.4:

Theorem 2.1.1. *([13], Theorem 1) Let K be a totally real number field. Assume that only one prime of K lies over p and that this prime is totally ramified in K_∞/K. Then the following two statements are equivalent:*

(i) Every ideal class of A_0 becomes principal in K_n for some n.

(ii) $|A_n|$ is bounded as $n \to \infty$.

Let B_n' denote the subgroup of B_n consisting of ideal classes containing an ideal invariant under the action of $\mathrm{Gal}(K_n/K)$. Then from the proof of Theorem 2.1.1, the following holds:

$$B_n/B_n' \cong E(K)/N_{n,0}(E(K_n))$$

where $E(L)$ denotes the units of the ring of integers of L and $N_{n,0}$ is the norm map from K_n to K_0. This result will be relevant to our discussion in Chapter 4.

2.2 Biquadratic extensions and fundamental units [19]

We define a biquadratic extension as any extension of number fields L/K such that $\mathrm{Gal}(L/K) \cong C_2 \times C_2$. Most of the work on imaginary biquadratic extensions $L/\mathbb{Q}$ was done by Kuroda [21]. For real biquadratic extensions, we have the following result by Kubota, commonly known as the Kubota-Kuroda formula:

Theorem 2.2.1. *[19] Let $L/\mathbb{Q}$ be a totally real biquadratic extension, with unit group $E(L)$ and 2-class group $A(L)$. Let L_1, L_2, and L_3 be the quadratic subfields of L. Let ε_i be the fundamental unit of L_i, for $i = 1, 2$ and 3. Let $q(L) := [E(L) : \langle -1, \varepsilon_1, \varepsilon_2, \varepsilon_3 \rangle]$ be the Hasse unit index of L. Then we have*

$$|A(L)| = \frac{1}{4} \cdot q(L) \cdot |A(L_1)| \cdot |A(L_2)| \cdot |A(L_3)|.$$

Further, a system $\mathcal{F}$ of fundamental units of L (F.S.U) is one of the following possibilities.

1. $\{\varepsilon_1, \varepsilon_2, \varepsilon_3\}$,
2. $\{\sqrt{\varepsilon_1}, \varepsilon_2, \varepsilon_3\}$,
3. $\{\sqrt{\varepsilon_1}, \sqrt{\varepsilon_2}, \varepsilon_3\}$,
4. $\{\sqrt{\varepsilon_1\varepsilon_2}, \varepsilon_2, \varepsilon_3\}$,
5. $\{\sqrt{\varepsilon_1\varepsilon_2}, \varepsilon_2, \sqrt{\varepsilon_3}\}$,
6. $\{\sqrt{\varepsilon_1\varepsilon_2}, \sqrt{\varepsilon_1\varepsilon_3}, \sqrt{\varepsilon_2\varepsilon_3}\}$,
7. $\{\sqrt{\varepsilon_1\varepsilon_2\varepsilon_3}, \varepsilon_2, \varepsilon_3\}$.

Any unit ε_i that appears under the square root sign is assumed to have norm equal to 1, except for the last case, where all the units can have the same norm, either all 1 or all -1.

We also refer to a set of generators of the unit group modulo $\{1, -1\}$ of a biquadratic field as a fundamental system of units (F.S.U). We aim to use this formula to determine the order of the class group of the biquadratic field $K_1 = \mathbb{Q}(\sqrt{2}, \sqrt{D})$ and obtain a fundamental system of units.

Furthermore, we have the following generalization by Lemmermeyer [22]:

Theorem 2.2.2. *Let L/K be a biquadratic extension. Then*

$$h(L) = \frac{2^{d-\kappa-2-v} \cdot q(L) \cdot h_1 \cdot h_2 \cdot h_3}{h(K)^2}.$$

Where

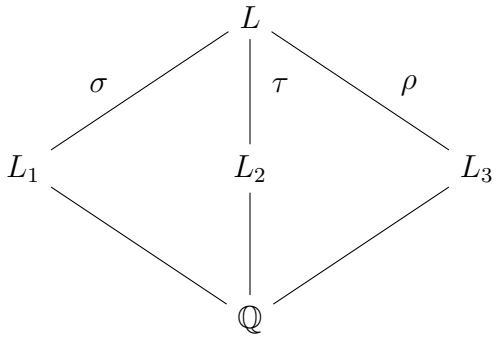
- *The values h_i denote the class numbers of the intermediate quadratic subextensions L_i.*
- *d is the number of infinite places ramifies in L/K.*
- *κ is the $\mathbb{Z}$-rank of $E(K)$.*
- *$q(L)$ is the index $[E(L) : E(L_1)E(L_2)E(L_3)]$.*
- *$v = 1$ if $L = K(\sqrt{\varepsilon}, \sqrt{\eta})$ for units $\varepsilon, \eta \in K$; and $v = 0$ otherwise.*

In particular, for a real biquadratic extension L of $\mathbb{Q}(\sqrt{2})$ where $v = 0$, we have:

$$h(L) = \frac{1}{8} \cdot q(L) \cdot h_1 \cdot h_2 \cdot h_3, \tag{2.1}$$

since $d = 0$ and $\kappa = 1$.

We conclude this section with an analysis of one specific case, as presented in [30] (the original result is in Kubota's paper). Suppose $L/\mathbb{Q}$ is biquadratic and that the norm of all the fundamental units is equal to -1. The F.S.U. of L depends on whether $\varepsilon_1 \cdot \varepsilon_2 \cdot \varepsilon_3$ is a square in L or not. The units of L are determined completely by the units of the quadratic subextensions L_1, L_2 and L_3. Furthermore, the group of units $E(L)$ is generated by the units of these subfields and the elements of $E(L_1)E(L_2)E(L_3)$ that are squares in L. Consider the following diagram:



where σ, τ and ρ are the non-trivial automorphisms of the corresponding Galois extensions.

Let $\eta = \varepsilon_1 \cdot \varepsilon_2 \cdot \varepsilon_3 - \varepsilon_1 - \varepsilon_2 - \varepsilon_3$ and $C = T(\eta) = \eta + \eta^\sigma + \eta^\tau + \eta^\rho$, where $T = T_{L/\mathbb{Q}}$ represents the trace map on an extension $L/\mathbb{Q}$. We calculate $\varepsilon_1 \cdot \varepsilon_2 \cdot \varepsilon_3 \cdot \eta^\sigma$:

$$\begin{aligned}\varepsilon_1 \cdot \varepsilon_2 \cdot \varepsilon_3 \cdot \eta^\sigma &= \varepsilon_1(\varepsilon_1 \cdot (\varepsilon_2 \cdot \varepsilon_2^\sigma)(\varepsilon_3 \cdot \varepsilon_3^\sigma) - \varepsilon_1 \cdot \varepsilon_2 \cdot \varepsilon_3 - \varepsilon_3 \cdot (\varepsilon_2 \cdot \varepsilon_2^\sigma) - \varepsilon_2 \cdot (\varepsilon_3 \cdot \varepsilon_3^\sigma)) \\ &= \varepsilon_1(\varepsilon_1 + \varepsilon_2 + \varepsilon_3 - \varepsilon_1 \cdot \varepsilon_2 \cdot \varepsilon_3) \\ &= -\varepsilon_1 \cdot \eta\end{aligned}$$

since ε_{2D}^σ and ε_2^σ are the conjugates, and the norm of both units is equal to -1.

Similarly, we get $\varepsilon_1 \cdot \varepsilon_2 \cdot \varepsilon_3 \cdot \eta^\tau = -\varepsilon_2 \cdot \eta$ and $\varepsilon_1 \cdot \varepsilon_2 \cdot \varepsilon_3 \cdot \eta^\rho = -\varepsilon_3 \cdot \eta$. Hence,

$$\varepsilon_1 \cdot \varepsilon_2 \cdot \varepsilon_3 \cdot C = \eta^2.$$

Therefore, as shown in [30], $\varepsilon_1 \cdot \varepsilon_2 \cdot \varepsilon_3$ is a square in L if and only if C is a square in L, with the advantage that C is an integer. Thus, $C = d \cdot t^2$ where d divides the discriminant of L, and this condition relies entirely on $\sqrt{d}$.

Let T be the trace map from L to $\mathbb{Q}$. We can define

$$c_1 = T(\varepsilon_1 \cdot \varepsilon_2 \cdot \varepsilon_3 - \varepsilon_1 - \varepsilon_2 - \varepsilon_3),$$
$$c_2 = T(\varepsilon_1 \cdot \varepsilon_2 \cdot \varepsilon_3 + \varepsilon_1 + \varepsilon_2 - \varepsilon_3),$$
$$c_3 = T(\varepsilon_1 \cdot \varepsilon_2 \cdot \varepsilon_3 + \varepsilon_1 - \varepsilon_2 + \varepsilon_3),$$
$$c_4 = T(\varepsilon_1 \cdot \varepsilon_2 \cdot \varepsilon_3 - \varepsilon_1 + \varepsilon_2 + \varepsilon_3).$$

With a similar argument, one can show that $\varepsilon_1 \cdot \varepsilon_2 \cdot \varepsilon_3$ is a square if and only if any of the c_i's is a square, and we have:

$$\sqrt{\varepsilon_1 \cdot \varepsilon_2 \cdot \varepsilon_3} = \frac{1}{4}(\sqrt{c_1} + \sqrt{c_2} + \sqrt{c_3} + \sqrt{c_3}).$$

We will talk about this condition in future chapters.

2.3 Quadratic fields with cyclic Iwasawa module [25]

We present some of the results in Mouhib and Movahhedi's paper, as it serves as our main point of reference for the cases we will be focusing on.

We maintain the notations from the previous chapter. Let K_∞/K be a $\mathbb{Z}_p$-extension with intermediate fields K_n, where K is a totally real field. Then L_n will denote the maximal unramified p-extension of K_n, corresponding to the p-class group A_n. The extension K_∞/K_{n_0} is totally ramified. Thus if we fix a prime a p-adic prime $\mathcal{P}_{n_0}$, there is only one prime $\mathcal{P}_n$ of K_n above $\mathcal{P}_{n_0}$ for each $n \geq n_0$.

Let F_n be the decomposition field of $\mathcal{P}_n$ in L_n/K_n, which is the largest subfield where the prime splits. Let $L'_n \subset F_n$ be the maximal subextension of L_n/K_n in which all p-adic primes split completely (not only $\mathcal{P}_n$). If K_{n_0} satisfies Leopoldt's conjecture at the prime p,

and the Iwasawa module X_∞ is cyclic, Mouhib and Movahhedi proved that $\mu = \lambda = 0$ as soon as $L_N \neq L'_N$ for some integer $N \geq n_0$, which is equivalent to a p-adic prime not splitting in L_N/K_N. It is difficult to determine the order of the module X_∞ using this criterion (Proposition 3.1.2).

We present the proof of the following result from their paper, as we can conclude an important corollary from it:

Proposition 2.3.1. *Suppose X_∞ is cyclic. Let $N \geq n_0$ be the smallest integer such that $A_N \neq 0$. Then X_∞ is finite as soon as there exists a non-trivial element of A_N which capitulates in K_∞.*

Proof. Let $Y_\infty = \mathrm{Gal}(L_\infty/K_\infty L_{n_0})$, which is a $\Lambda = \mathbb{Z}_p[\![T]\!]$-module [31]. Define $\omega_n = (1+T)^{p^n} - 1$ and $v_{m,n} = \omega_n/\omega_m$ for $n \geq m \geq 0$. It is known that $X_\infty/v_{n_0,n}Y_\infty \cong A_n$ for $n \geq n_0$. We have the following commutative diagram for $n \geq N$:

$$\begin{array}{ccc} A_N & \longrightarrow & X_\infty/v_{n_0,N}Y_\infty \\ \downarrow & & \downarrow{\scriptstyle v_{N,n}} \\ A_n & \longrightarrow & X_\infty/v_{n_0,n}Y_\infty \end{array}$$

where the horizontal maps are isomorphisms, and the map from A_N to A_n is the inclusion map.

Let $|A_N| = |X_\infty/v_{n_0,N}Y_\infty| = p^r$. By hypothesis, the vertical map $v_{N,n}$ is not injective for n large enough. Thus, its kernel is not trivial of size p^{r-k} for some $k < r$. In particular, we can easily see that $p^{r-1}X_\infty$ is contained in the kernel, so that

$$v_{N,n}p^{r-1}X_\infty \subset v_{n_0,n}Y_\infty.$$

Since X_∞ is cyclic, $p^r X_\infty = v_{n_0,n} Y_\infty$. Therefore,

$$v_{n_0,n} Y_\infty = v_{N,n} v_{n_0,N} Y_\infty = v_{N,n} p^r X_\infty$$

and we get

$$v_{N,n} p^{r-1} X_\infty \subset v_{N,n} p^r X_\infty = p(v_{N,n} p^{r-1} X_\infty).$$

Thus, $v_{N,n} p^{r-1} X_\infty = p(v_{N,n} p^{r-1} X_\infty)$. Since $v_{N,n} p^{r-1} X_\infty$ is finitely generated and p belongs to the maximal ideal of Λ, we can conclude by Nakayama's lemma [31] that $v_{N,n} p^{r-1} X_\infty = 0$. Then $v_{n_0,n} Y_\infty = 0$ and $X_\infty \cong X_\infty / v_{n_0,n} Y_\infty \cong A_n$. □

The following result is only mentioned in [25]. As it will be used to determine the group X_∞ in specific cases, we provide a proof:

Corollary 2.3.2. *Suppose X_∞ is cyclic and $A_{n_0} \neq 0$. Then $X_\infty \cong A_{n_0}$ if there exists a non-trivial element of A_{n_0} which capitulates in K_{n_0+1}.*

Proof. Using the notation from the previous result, we have $N = n_0$, and there exists a non-trivial element of A_N which capitulates in A_{N+1}. Then $v_{n_0,N}$ is the identity map and we have

$$v_{n_0,N+1} Y_\infty = p^r X_\infty,$$

which implies

$$A_{N+1} \cong X_\infty / v_{n_0,N+1} Y_\infty \cong X_\infty / p^r X_\infty.$$

Since A_{N+1} is cyclic, we have $|A_{N+1}| \leq |A_N| = p^r$. The extension is totally ramified, thus $|A_N| \leq |A_{N+1}|$. We can conclude that $X_\infty \cong A_N = A_{n_0}$, due to the following result by Fukuda. □

Theorem 2.3.3. *[10] Let K_∞/K be a $\mathbb{Z}_p$ extension such that K_∞/K is totally ramified. If $|A_1| = |A_0|$, then $|A_n| = |A_0|$ for all $n \geq 0$.*

For the cyclotomic extension, since any field K_n in the chain has the same extension, this can be simply stated as $X_\infty \cong A_n$ if $n \geq n_0$ and $|A_{n+1}| = |A_n|$. That is, as soon as the extension is totally ramified and two consecutive fields have the same class group, the size of the class groups in the chain stabilizes.

We will discuss some other important results from [25] at the end of this chapter, but first, we talk about some results from genus theory that will be relevant to our analysis.

2.3.1 Genus formula and Hilbert symbol ([7], [3])

The following result by Chevalley is commonly known as the ambiguous class number formula:

Theorem 2.3.4. *[7] Let L/K be a cyclic extension of degree p^n with Galois group $G = \mathrm{Gal}\,(L/K)$. Let $A(L)^G$ be the subgroup of the p-class group $A(L)$ consisting of the ideal classes that are fixed by the action of G on $A(L)$. Let $N_{L/K}$ denote the norm map from L to K. Let $E(L)$ and $E(K)$ be the unit groups of L and K, respectively. Then the following equation holds.*

$$\left|A(L)^G\right| = \frac{|A(K)| \cdot \prod e_v}{[L:K]\left[E(K) : E(K) \cap N_{L/K}(L^*)\right]}.$$

where e_v is the ramification index at v and the product is taken over all the places of L. Let $B(L)^G$ be the subgroup of $A(L)^G$ which consists of the ideal classes which contain an ideal fixed by the action of G on the ideals of K. Then,

$$\left|B(L)^G\right| = \frac{|A(K)| \cdot \prod e_v}{[L:K]\left[E(K) : N_{L/K}(E(L))\right]}.$$

Remark 2.3.5. If K_∞/K is totally ramified, using Greenberg's notation we have

$$|B_n| = \left|A(K_n)^G\right| = \frac{|A(K)|}{\left[E(K) : E(K) \cap N_{L/K}(L^*)\right]}$$

$$|B_n'| = \left|B(K_n)^G\right| = \frac{|A(K)|}{\left[E(K) : N_{L/K}(E(L)\right]}$$

since it is only ramified above $p = 2$ and $e_2 = 2^n = [K_n : K]$.

Restricting our attention to quadratic extensions, we have the following result known as the Genus formula.

Theorem 2.3.6. *Let L/K be a quadratic extension of number fields with Galois group $G = \mathrm{Gal}\,(L/K)$. Let $A(L)^G$ be the subgroup of the 2-class group $A(L)$ consisting of the ideal classes that are fixed by the action of G on $A(L)$. Let $N_{L/K}$ denote the norm map from L to K. Let $E(L)$ and $E(K)$ be the unit groups of L and K, respectively. If t is the number of places of K ramified in L, then the following equality holds.*

$$\left|A(L)^G\right| = |A(K)| \times \frac{2^{t-1}}{\left[E(K) : E(K) \cap N_{L/K}(L^*)\right]}.$$

Let $B(L)^G$ be the subgroup of $A(L)^G$ which consists of the ideal classes which contain an ideal fixed by the action of G on the ideals of L. Then,

$$\left|B(L)^G\right| = |A(K)| \times \frac{2^{t-1}}{\left[E(K) : N_{L/K}(E(L))\right]}.$$

When the 2-class group of K is trivial the 2-rank of $A(L)$ is determined by

$$r_2\left(A(L)\right) = t - e - 1, \tag{2.2}$$

where $e = r_2\left(E(K)/E(K) \cap N_{L/K}K^*\right)$, which we will often refer to as the norm unit index.

When we consider a quadratic extension $K/\mathbb{Q}$, since the class group of $\mathbb{Q}$ is trivial, we recover the formula for the 2-rank. (Equation (1.1))

Let $\mathbb{Q}_1 = \mathbb{Q}(\sqrt{2})$. The unit group $E(\mathbb{Q}_1)$ is generated by -1 and the fundamental unit $\varepsilon_2 = 1 + \sqrt{2}$ of negative norm. Hence, to determine the index e from before, we simply need to determine whether these generators are a norm from K^* or not. Let $K = \mathbb{Q}(\sqrt{D})$ with $D > 0$ a square-free integer. The biquadratic field $K_1 = \mathbb{Q}(\sqrt{2}, \sqrt{D})$ is the first step in the cyclotomic $\mathbb{Z}_2$ extension of K, and by using the extension $K_1/\mathbb{Q}_1$, it is possible to determine the 2-rank of $A_1 = A(K_1)$ by calculating the norm unit index.

Let $\mathcal{P}$ be a prime of K. Let $K_{\mathcal{P}}$ be a completion of K at that prime. The Hilbert symbol or norm residue symbol is defined as

$$\left(\frac{a, b}{\mathcal{P}}\right) = \frac{\sigma_a(\sqrt{b})}{\sqrt{b}} = \pm 1,$$

where σ_a is the automorphism corresponding to the Artin Symbol $\left(a, K_{\mathcal{P}}(\sqrt{b})/K_{\mathcal{P}}\right)$.

Remark 2.3.7. As established in [3], for an extension $K(\sqrt{b})/K$, a unit u in $E(K)$ is a norm if and only if $\left(\frac{u,b}{\mathcal{P}}\right) = 1$ for every prime $\mathcal{P}$ that ramifies in $K(\sqrt{b})$.

These conditions will be related to the quadratic and biquadratic symbols. For example, assume D has no divisors $q \equiv 3 \mod 4$, and a prime $p \equiv 1 \mod 8$ divides D. Then p splits into two primes ideals $\mathcal{P}_1, \mathcal{P}_2$ of $\mathbb{Q}_1$. From [3], we have

$$\left(\frac{\varepsilon_2, 2}{\mathcal{P}_1}\right) = \left(\frac{\varepsilon_2, 2}{\mathcal{P}_2}\right) = \left(\frac{2}{p}\right)_4 \left(\frac{p}{2}\right)_4 = \left(\frac{2}{p}\right)_4 (-1)^{\frac{p-1}{8}}.$$

In particular, a necessary condition for ε_2 to be a norm is that

$$\left(\frac{2}{p}\right)_4 = \left(\frac{p}{2}\right)_4 = (-1)^{\frac{p-1}{8}}$$

for all such primes.

Mouhib and Movahhedi used this to determine when the rank of the 2-class groups in the cyclotomic chain is equal to 1; i.e., the Iwasawa module X_∞ is cyclic.

2.3.2 Cyclic Iwasawa module

Throughout, we will restrict our attention to the $\mathbb{Z}_2$ extension of K. In [25], the authors proved the following results:

Theorem 2.3.8. *Real quadratic number fields $K = \mathbb{Q}(\sqrt{d})$ such that $X_\infty = 0$ are precisely:*

(i) $\mathbb{Q}(\sqrt{p})$ *or* $\mathbb{Q}(\sqrt{2p})$ *with* $p \equiv 5 \mod 8$*;*

(ii) $\mathbb{Q}(\sqrt{p})$ *or* $\mathbb{Q}(\sqrt{2p})$ *with* $p \equiv 1 \mod 8$ *and* $\left(\frac{2}{p}\right)_4 \neq (-1)^{\frac{p-1}{8}}$*;*

(iii) $\mathbb{Q}(\sqrt{p})$ *or* $\mathbb{Q}(\sqrt{2p})$ *with* $p \equiv 3 \mod 8$*;*

(iv) $\mathbb{Q}(\sqrt{pq})$ *or* $\mathbb{Q}(\sqrt{2pq})$ *with* $p \equiv 5 \mod 8$ *and* $q \equiv 3 \mod 8$*;*

where p and q denote distinct odd prime numbers

Theorem 2.3.9. *Real quadratic number fields $K = \mathbb{Q}(\sqrt{d})$ for which X_∞ is cyclic (non-trivial) are precisely:*

(i) $\mathbb{Q}(\sqrt{p})$ *or* $\mathbb{Q}(\sqrt{2p})$ *with* $p \equiv 1 \mod 8$ *and* $\left(\frac{2}{p}\right)_4 = (-1)^{\frac{p-1}{8}}$*, such that the 2-class group of* $\mathbb{Q}\left(\sqrt{2p+\sqrt{2p}}\right)$ *is isomorphic to* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$*;*

(ii) $\mathbb{Q}(\sqrt{pq})$ *or* $\mathbb{Q}(\sqrt{2pq})$ *with* $p \equiv 5 \mod 8$ *and such that* $\left(\frac{2}{q}\right)_4 \neq (-1)^{\frac{q-1}{8}}$ *whenever* $q \equiv 1 \mod 8$*;*

(iii) $\mathbb{Q}(\sqrt{pq})$ *or* $\mathbb{Q}(\sqrt{2pq})$ *with* $p \equiv q \equiv -1 \mod 8$ *and* $q \not\equiv -1 \mod 16$*;*

(iv) $\mathbb{Q}(\sqrt{pq_1q_2})$ *or* $\mathbb{Q}(\sqrt{2pq_1q_2})$ *with* $p \equiv 5 \mod 8$, $q_1 \equiv 3 \mod 8$ *and* $q_2 \equiv 3 \mod 4$

where p, q, q_1 *and* q_2 *denote distinct odd prime numbers*

The field $K_1' = \mathbb{Q}\left(\sqrt{2p+\sqrt{2}p}\right)$ is the proper subextension of K_2/Q_1 different from K_1 and $\mathbb{Q}_2$, and will be mentioned in future chapters. It is worth noting again that $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{2d})$ yield the same cyclotomic extension. Additionally, Ozaki-Taya had partially proved some of these results:

Theorem 2.3.10. *[27] Let* $K = \mathbb{Q}(\sqrt{m})$ *or* $\mathbb{Q}(\sqrt{2m})$*. Suppose that* m *is one of the following:*

1. $m = p$, *with* $p \equiv 1 \mod 8$ *and* $\left(\frac{2}{p}\right)_4 \neq (-1)^{\frac{p-1}{8}}$,
2. $m = pq$, *with* $p \equiv q \equiv 3 \mod 8$,
3. $m = pq$, *with* $p \equiv 3, q \equiv 5 \mod 8$,
4. $m = pq$, *with* $p \equiv 5, q \equiv 7 \mod 8$,
5. $m = pq$, *with* $p \equiv q \equiv 5 \mod 8$,

where p *and* q *denote distinct odd prime numbers. Then* $\lambda = 0$*, and* $\nu = 0$ *for (1) and (2), and* $\nu > 0$ *for (3), (4) and (5).*

The proof of the cases (3), (4), and (5) are included in [25], but it is worth mentioning that the case $p \equiv q \equiv 5 \mod 8$ follows a similar argument, based on the fact that the 2-adic prime does not split in some extension L_N/K_N.

2.3.3 Problem setup

We focus our attention on real quadratic fields with cyclic Iwasawa module, namely those mentioned in Theorem 2.3.9. In the next chapter, we determine some new examples of Greenberg's conjecture being valid and calculate the order of the cyclic module X_∞ when

possible. In [25], the authors proved that the λ-invariant vanishes in some of these cases. Denote the quadratic field by $K = \mathbb{Q}(\sqrt{D})$. We list some of the main results in the literature:

In the first case, with $D = p$, the Iwasawa module of K is finite if $\left(\frac{2}{p}\right)_4 = (-1)^{\frac{p-1}{8}} = -1$. Furthermore, when $\left(\frac{2}{p}\right)_4 = (-1)^{\frac{p-1}{8}} = 1$ and the norm of the fundamental unit ε_{2D} of $\mathbb{Q}(\sqrt{2p})$ is -1, the authors prove that $X_\infty \cong A_1$. We will use some of the ideas in this proof to provide some new examples in the next chapter.

For the second case, from the results of Ozaki-Taya, it is known that for $D = pq$ with $p \equiv 5 \mod 8$, and $q \not\equiv 1 \mod 8$, the λ-invariant is 0. As we will see in the next chapter, one can determine the size of the Iwasawa module in some cases. Furthermore, we present some new examples when $q \equiv 1 \mod 8$ and determine the size of the Iwasawa module, using some ideas from [25], [24], [1], and the analysis of quadratic forms in [18].

For the fourth case, the invariant is 0 when $K = \mathbb{Q}(\sqrt{pq_1q_2})$ with $p \equiv 5 \mod 8$, $q_1 \equiv 3 \mod 8$ and $q_3 \equiv 7 \mod 8$. In [14], the authors calculate the size of the Iwasawa module in some cases. Furthermore, they provide some new examples in the case where $q_3 \equiv 3 \mod 8$. Specifically, if $\left(\frac{q_1q_2}{p}\right) = -1$ or if $\left(\frac{q_1}{p}\right) = \left(\frac{q_2}{p}\right) = 1$ and the ideal over p in K is not principal. We give proof of some of these results using our methods and provide a new example where the λ-invariant is 0.

Finally, the cases that are left out present notable challenges using these techniques. For instance, in the fourth case, when the prime above p or q becomes principal in $\mathbb{Q}(\sqrt{D})$, the behavior seems to be rather unpredictable. These cases prove to be quite difficult to understand. We will provide some examples throughout the sections of the next chapter. As a new idea on how to deal with these cases, we work with the units of the intermediate fields of $K_1' = \mathbb{Q}\left(\sqrt{(2+\sqrt{2})D}\right)$ to derive some properties of the field K_2.

Chapter 3

Main results

In this chapter, we will focus on the second case and fourth case of Theorem 2.3.9. We present the main results we obtained during our research. Throughout, let $K = \mathbb{Q}(\sqrt{D})$, where the conditions on D will be given in each section. As before, K_∞ will denote the cyclotomic $\mathbb{Z}_2$-extension of K with intermediate fields K_n and 2-class groups A_n. We also denote by ε_D the fundamental unit of K.

Let $\mathbb{Q}_n$ the n-th layer of the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}$. Then $\mathbb{Q}_1 = \mathbb{Q}(\sqrt{2})$, and we denote its fundamental unit by $\varepsilon_2 = 1 + \sqrt{2}$. Following [20], we shall also denote K_n' to be the subfield of K_{n+1} containing $\mathbb{Q}_n$, different from K_n and $\mathbb{Q}_{n+1}$, and A_n' to be its 2-class group. Notably, we have $K_0' = K' = \mathbb{Q}(\sqrt{2D})$, and $K_1' = \mathbb{Q}\left(\sqrt{(2+\sqrt{2})pq}\right)$. We denote the fundamental unit of K' by ε_{2D}.

We divide this chapter in terms of the 3 cases mentioned before, in the following order:

1. $D = pq$, with $p \equiv 5 \mod 8$ and $q \not\equiv 1 \mod 8$.
2. $D = pq_1q_2$ with $p \equiv 5 \mod 8$, $q_1 \equiv 3 \mod 8$ and $q_2 \equiv 3 \mod 4$.
3. $D = pq$, with $p \equiv 5 \mod 8$ and $q \equiv 1 \mod 8$, with $\left(\frac{2}{q}\right)_4 \neq (-1)^{\frac{p-1}{8}}$.

3.1 First Case

Throughout this section, we assume that $D = pq$, with $p \equiv 5 \mod 8$ and $q \not\equiv 1 \mod 8$. As mentioned before, the corresponding Iwasawa module is finite. First, let us consider the case where $q \equiv 3 \mod 4$. Under these conditions, we show that the Iwasawa module is isomorphic to $A_0 = A(K)$:

Proposition 3.1.1. *Let $K = \mathbb{Q}(\sqrt{pq})$ with $p \equiv 5 \mod 8$ and $q \equiv 3 \mod 4$. Then $\{\sqrt{\varepsilon_D \varepsilon_{2D}}, \varepsilon_D, \varepsilon_2\}$ is a F.S.U. of K_1 and $X_\infty \cong A_0 \cong C_2$.*

Proof. As mentioned in Example 1.2.2, the simple ambiguous forms of K are

$$f = [1, 0, -pq],\ g = [p, 0, -q],\ h = \left[2, 1, \frac{1-pq}{2}\right],\ l = \left[2p, p, \frac{p-q}{2}\right],$$

$$\overline{f} = [-1, 0, pq],\ \overline{g} = [q, 0, -p],\ \overline{h} = \left[-2, 1, \frac{pq-1}{2}\right],\ \bar{l} = \left[2q, q, \frac{q-p}{2}\right].$$

where exactly only one of the forms g, l or $\bar{l}$ is in the principal genus (this is equivalent to all the generic characters being equal to 1 in Table 1.1). Thus, $r_4(Cl^+(K)) = 0$ (Equation (1.2)) and $A_0 \cong C_2$, since $N(\varepsilon_D) = 1$ (Remark 1.2.1).

Without loss of generality, let's assume that the form l is in the principal genus. Since there are only two forms, l is equivalent to $f = [1, 0, -pq]$. Furthermore, since l represents the number $2p$, so does f. Hence, the equation $x^2 - pqy^2 = 2p$ has an integral solution. Since both primes 2 and p ramify in K, the ideal generated by $2p$ factorizes as $\langle 2p \rangle = \mathcal{L}^2$ for some ideal $\mathcal{L}$ of K. Thus, from the equation

$$(x - y\sqrt{pq}) \cdot (x + y\sqrt{pq}) = 2p,$$

since the ideals $\langle x - y\sqrt{pq} \rangle$, $\langle x + y\sqrt{pq} \rangle$ are conjugates and the ideals over p and 2 are self-

conjugate, it follows by unique factorization that the ideal $\mathcal{L}$ is principal (this is why they are called principal factors). Consequently, we have $\langle 2p\rangle = \langle z\rangle^2$ for some fractional ideal $\langle z\rangle$ in K. Therefore,

$$2p = z^2 \cdot \varepsilon_D^n \text{ for some n.}$$

If n is even, then $\sqrt{2p} \in K_1$, which is impossible, as $K_1 = \mathbb{Q}(\sqrt{2}, \sqrt{pq})$. Thus, n is odd. Let $\alpha = |z| \cdot \varepsilon_D^{(n-1)/2}$, then

$$\sqrt{p} = \frac{\alpha \cdot \sqrt{\varepsilon_D}}{\sqrt{2}},$$

which implies that $K_1(\sqrt{p}) = K_1(\sqrt{\varepsilon_D})$. Since $K_1(\sqrt{p}) = K_1(\sqrt{q})$, the other cases follow in a similar manner. In any case, we can conclude that $\sqrt{\varepsilon_D} \notin K_1$.

Following the same lines, by Kaplan ([18], §6, Proposition A_4), the narrow 2-class group of K' is isomorphic to $C_2 \times C_2$. Since the norm of ε_{2D} is 1, we can conclude that $A_0' \cong C_2$. By analyzing the generic characters of K', we observe that exactly one of the forms $[-p, 0, 2q]$, $[q, 0, -2p]$ or $[-q, 0, 2p]$ is equivalent to the unit form $f = [1, 0, -2pq]$. Consequently, the ideal over one of the elements $2q$, $2p$, or q is principal in K_1, and $K_1\left(\sqrt{p}\right) = K_1\left(\sqrt{\varepsilon_{2D}}\right)$, reasoning as before. Therefore, $K_1(\sqrt{\varepsilon_D}) = K_1(\sqrt{\varepsilon_{2D}})$, which shortly implies that $\sqrt{\varepsilon_D\varepsilon_{2D}} \in K_1$.

By Theorem 2.2.1, the F.S.U of K_1 is $\{\sqrt{\varepsilon_D\varepsilon_{2D}}, \varepsilon_D, \varepsilon_2\}$ and the Hasse unit index $q(K_1)$ is equal to 2. Hence,

$$|A_1| = \frac{1}{2}\,|A_0| \cdot |A_0'| = |A_0|\,.$$

Finally, since the extension K_∞/K is totally ramified, as the prime 2 is ramifies in every quadratic subextension of $K_1/\mathbb{Q}$, it follows by Theorem 2.3.3 that $X_\infty \cong A_0$. □

The case $q \equiv 5 \mod 8$ turns out to be more complicated. Using the conditions in Theorem 1.2.6 and Remark 1.2.7, we prove the following result:

Proposition 3.1.2. *Let $K = \mathbb{Q}(\sqrt{pq})$ with $p \equiv q \equiv 5 \pmod 8$. Then the following hold:*

(i) Assume $\left(\frac{p}{q}\right) = 1$ and $\left(\frac{p}{q}\right)_4 = -\left(\frac{q}{p}\right)_4$. Then $\{\varepsilon_D, \varepsilon_{2D}, \varepsilon_2\}$ is a F.S.U of K_1, and $X_\infty \cong A_0$.

(ii) Assume either $\left(\frac{p}{q}\right) = -1$, or $\left(\frac{p}{q}\right) = 1$ with $\left(\frac{p}{q}\right)_4 = \left(\frac{q}{p}\right)_4 = -1$. Then

$$X_\infty \cong A_0 \iff \sqrt{\varepsilon_D \varepsilon_{2D} \varepsilon_2} \notin K_1.$$

In this case, $\{\varepsilon_D, \varepsilon_{2D}, \varepsilon_2\}$ is a F.S.U of K_1. Otherwise, $\{\sqrt{\varepsilon_D \varepsilon_{2D} \varepsilon_2}, \varepsilon_D, \varepsilon_2\}$ is the corresponding F.S.U and $|A_1| = 2 \cdot |A_0|$.

(iii) Assume $\left(\frac{p}{q}\right) = 1$ and $\left(\frac{p}{q}\right)_4 = \left(\frac{q}{p}\right)_4 = 1$.

(a) If $N(\varepsilon_D) = 1$, then $\{\varepsilon_D, \varepsilon_{2D}, \varepsilon_2\}$ is a F.S.U of K_1, and $X_\infty \cong A_0$.

(b) If $N(\varepsilon_D) = -1$, then

$$X_\infty \cong A_0 \iff \sqrt{\varepsilon_D \varepsilon_{2D} \varepsilon_2} \notin K_1.$$

In this case, $\{\varepsilon_D, \varepsilon_{2D}, \varepsilon_2\}$ is a F.S.U of K_1. Otherwise, $\{\sqrt{\varepsilon_D \varepsilon_{2D} \varepsilon_2}, \varepsilon_D, \varepsilon_2\}$ is the corresponding F.S.U and $|A_1| = 2 \cdot |A_0|$.

Proof. First, we work with the field K', independent of the conditions of quadratic and biquadratic symbols. From ([18], §4, Proposition A_2), the simple ambiguous forms are:

$$f = [1, 0, -2pq],\ g = [2, 0, -pq],\ h = [p, 0, -2q],\ l = [q, 0, -2q],$$

$$\overline{f} = [-1, 0, 2pq],\ \overline{g} = [-2, 0, pq],\ \overline{h} = [-p, 0, 2q],\ \overline{l} = [q, 0, -2q].$$

In this case, a form and its inverse are in the same class. Let $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = \tau$, $\left(\frac{2}{p}\right) = \tau'$ and $\left(\frac{2}{q}\right) = \tau''$. Then the generic characters are the ones in the following table:

	f, $\overline{f}$	g, $\overline{g}$	h, $\overline{h}$	l, $\overline{l}$
$\left(\frac{m}{p}\right)$	1	τ'	$\tau\tau'$	τ
$\left(\frac{m}{q}\right)$	1	τ''	τ	$\tau\tau''$
$(-1)^{\frac{m-1}{2}}$	1	$\tau'\tau''$	τ'	τ''

Table 3.1: Generic character for $D = pq$, $p \equiv q \equiv 5 \mod 8$

From the conditions $\left(\frac{2}{p}\right) = \left(\frac{2}{q}\right) = -1$ we can see that only $\overline{f}$ is in the principal genus. Hence, the 4-rank of narrow class group K' is 0 and $N(\varepsilon_{2D}) = -1$. Since the 2-class group of K' is the same, we have $A_0' \cong C_2 \times C_2$.

For the field K, only one of the forms $[-1, 0, pq]$, $[p, 0, -q]$ or $[q, 0, -p]$ is equivalent to $[1, 0, -pq]$, as these are the forms in the principal genus. If $N(\varepsilon_D) = 1$, the form $[-1, 0, pq]$ is not equivalent to the unit, so that either p or q is a principal factor. We can then conclude that either the ideal over p or q in K is principal and $K_1(\sqrt{p}) = K_1(\sqrt{\varepsilon_D})$, using a similar argument as before. Hence, $\sqrt{\varepsilon_D} \notin K_1$.

If $\left(\frac{p}{q}\right) = 1$ and $\left(\frac{p}{q}\right)_4 = -\left(\frac{q}{p}\right)_4$, then from Theorem 1.2.6, we can see that $N(\varepsilon_D) = 1$. Given that only the unit ε_D has norm 1, and $\sqrt{\varepsilon_D} \notin K_1$, it follows from Theorem 2.2.1 that $\{\varepsilon_D, \varepsilon_{2D}, \varepsilon_2\}$ is the F.S.U. of K_1 and the Hasse unit index $q(K_1) = 1$. Thus, from the Kubota-Kuroda formula we have $|A_1| = |A_0|$, and since $n_0 = 0$, it follows that $X_\infty \cong A_0$.

Now assume either $\left(\frac{p}{q}\right) = -1$, or $\left(\frac{p}{q}\right) = 1$ with $\left(\frac{p}{q}\right)_4 = \left(\frac{q}{p}\right)_4 = -1$. From Theorem 1.2.6 and the previous analysis on the generic characters, the norm of all the fun-

damental units is -1. The only possible fundamental systems for K_1 are $\{\varepsilon_D, \varepsilon_{2D}, \varepsilon_2\}$ or $\{\sqrt{\varepsilon_D\varepsilon_{2D}\varepsilon_2}, \varepsilon_{2D}, \varepsilon_2\}$. Therefore, $|A_1| = q(K_1)\,|A_0|$, and $|A_1| = |A_0|$ if and only if $\sqrt{\varepsilon_D\varepsilon_{2D}\varepsilon_2} \notin K_1$.

Finally, if $\left(\frac{p}{q}\right) = 1$ with $\left(\frac{p}{q}\right)_4 = \left(\frac{q}{p}\right)_4 = 1$, the result follows similarly, depending on whether $N(\varepsilon_D) = 1$ or not. □

Let $\varepsilon_D = \frac{x+y\sqrt{D}}{2}$ with $x^2 - Dy^2 = -4$. Since $D \equiv 1 \mod 8$, we have the equation $x^2 \equiv y^2 + 4 \mod 8$. Since odd squares are equal to 1 modulo 8 and even squares are equal to 0 or 4, both x and y must be even. Thus, we can assume $\varepsilon_D = x + y\sqrt{D}$, by clearing denominators, with $x^2 - Dy^2 = -1$, which implies that x is even and y is odd, by taking the equation modulo 4. Similarly, $\varepsilon_{2D} = r + s\sqrt{2D}$, where both r, s are odd in this case.

The traces mentioned in the previous chapter are easy to calculate:

$$c_1 = 4rx + 8sypq - 4 - 4x - 4r$$

$$c_2 = 4rx + 8sypq + 4 - 4x - 4r$$

$$c_3 = 4rx + 8sypq - 4 + 4x - 4r$$

$$c_4 = 4rx + 8sypq - 4 - 4x + 4r$$

where $\sqrt{\varepsilon_D\varepsilon_{2D}\varepsilon_2} \in K_1$ if and only if all the c_i's are squares in K_1.

Example 3.1.3. If $p = 5, q = 13$ then

$$c_0 = 2^3 \cdot 23^2$$

$$c_1 = 2^4 \cdot 17^2$$

$$c_2 = 2^3 \cdot 3^2 \cdot 5 \cdot 13$$

$$c_3 = 2^6 \cdot 5 \cdot 13$$

In this case, $\sqrt{\varepsilon_D \varepsilon_{2D} \varepsilon_2} \in K_1$, as all the square roots are in K_1. Computing the class numbers we get $|A_2| = |A_1| = 4$, thus $X_\infty \cong A_1 \cong C_4$. These cases are rather complicated, as it is hard to calculate the exact group in the chain where A_0 capitulates.

We present some examples obtained with PARI computing the sizes of the corresponding class groups:

p	q	c_0	X_∞
5	13	$(8)^2 \cdot 5 \cdot 13$	A_1
5	53	$(20)^2 \cdot 2 \cdot 5 \cdot 53$	A_1
5	677	$(4660145624)^2 \cdot 5 \cdot 677$	A_2
5	1493	$(96826)^2 \cdot 2 \cdot 5 \cdot 1493$	A_2
13	317	$(6956378008)^2 \cdot 13 \cdot 317$	A_1
13	421	$t^2 \cdot 13 \cdot 421$	A_1
13	229	$t^2 \cdot 2 \cdot 13 \cdot 229$	A_2
13	733	$t^2 \cdot 2 \cdot 13 \cdot 733$	A_2

Table 3.2: $X_\infty \neq A_0$ for $p \equiv q \equiv 5 \mod 8$

For some cases like $p = 5$, $q = 397$, the chain goes beyond the second level, since $|A_3| > |A_2|$.

If we take $p = 5$, $q = 37$, then $c_1 = 2^3 \cdot 5 \cdot 73^2$, from where it follows that $\sqrt{c_3} \notin K_1$, since $\sqrt{2p} \notin K_1$. In this case $X_\infty \cong A_0$.

We will come back to this condition in the final chapter, as it relates to the more complicated cases and gives possible ideas on how to treat them.

3.2 Second Case

We assume $D = pq_1q_2$ with $p \equiv 5 \mod 8$, $q_1 \equiv 3 \mod 8$ and $q_2 \equiv 3 \mod 4$ in this section. First, we give a different proof of some of the results in [14] using ideas from ([1], [2]). Later in this section, we provide a new case where the λ-invariant is 0. We present the proof of the following result by Azizi [1] for future reference.

Lemma 3.2.1. *Let $\varepsilon = x + y\sqrt{d}$ be the fundamental unit of $K = \mathbb{Q}(\sqrt{d})$ with d square-free, and x, y are integers or semi-integers. Assume that the norm of ε is equal to 1. Then $2(x \pm 1)$ and $2d(x \pm 1)$ are not squares in $\mathbb{Q}$.*

Proof. Since $x^2 - dy^2 = 1$, we can see that $4(x+1)(x-1) = 4dy^2$, which implies

$$\sqrt{2(x+1)}\sqrt{2(x-1)} = 2y\sqrt{d},$$

where all the elements inside the square roots are integers. Using the norm identity, we have the following equality:

$$\left(\sqrt{2(x+1} + \sqrt{2(x-1)}\right)^2 = 2(x+1) + 2(x-1) + 2\sqrt{4(x^2-1)} = 4(x + y\sqrt{d}).$$

Hence,

$$\sqrt{\varepsilon} = \frac{1}{2}\left(\sqrt{2(x+1)} + \sqrt{2(x-1)}\right).$$

From this, we can see that $\sqrt{\varepsilon}\sqrt{2(x \pm 1)} \in \mathbb{Q}(\sqrt{d})$, where one can conclude that $2(x \pm 1)$ is not a square, since $\sqrt{\varepsilon} \notin \mathbb{Q}(\sqrt{d})$. Then,

$$\sqrt{2d(x \pm 1)}\sqrt{2(x \mp 1)} = 2yd.$$

Therefore, $2d(x \pm 1)$ is not a square either. □

Remark 3.2.2. This proof works if we change the unit to any odd power of ε since the conclusion only needs $\sqrt{\varepsilon} \notin \mathbb{Q}(\sqrt{d})$

We provide an alternative proof to the following result from [14] using some techniques from [2], and we draw some conclusions regarding the fundamental units. The argument will help us understand the remaining cases. Moreover, in the cases that are not covered by the theorem, the unit $\varepsilon_D \varepsilon_{2D}$ is a square in K_1, and we can calculate its norm:

Theorem 3.2.3. *Let $K = \mathbb{Q}(\sqrt{pq_1q_2})$ such that $p \equiv 5 \mod 8$, $q_1 \equiv q_2 \equiv 3 \mod 8$, and $\left(\frac{p}{q_1}\right) = \left(\frac{p}{q_2}\right) = 1$. If the ideal above p in K is not principal, then the Iwasawa module X_∞ is isomorphic to A_0.*

Furthermore, the ideal above p is principal if and only if $\sqrt{\varepsilon_D\varepsilon_{2D}} \in K_1$. In this case, $|A_1| = 2\,|A_0|$ and $\{\sqrt{\varepsilon_D\varepsilon_{2D}}, \varepsilon_D, \varepsilon_2\}$ is a F.S.U of K_1. Moreover, $\sqrt{\varepsilon_D\varepsilon_{2D}}$ satisfies

$$N_{K_1/K}(\sqrt{\varepsilon_D\varepsilon_{2D}}) = \varepsilon_D,\ N_{K_1/K'}(\sqrt{\varepsilon_D\varepsilon_{2D}}) = -\varepsilon_{2D},\ N_{K_1/\mathbb{Q}_1}(\sqrt{\varepsilon_D\varepsilon_{2D}}) = -1.$$

Proof. Let $\varepsilon_D = \frac{x+y\sqrt{D}}{2}$ for some integers x, y, where $D = pq_1q_2$. Since the norm is equal to 1 (Remark 1.2.4), we have $x^2 - 4 = Dy^2$. Then the following equality holds:

$$\begin{aligned} 8\varepsilon_D^3 &= (x + y\sqrt{D})^3 \\ &= x(x^2 + 3Dy^2) + y(3x^2 + Dy^2)\sqrt{D} \\ &= x(x^2 + 3(x^2 - 4)) + y(3x^2 + x^2 - 4)\sqrt{D} \\ &= 4x(x^2 - 3) + 4y(x^2 - 1)\sqrt{D} \end{aligned}$$

Since x, y have the same parity, $\varepsilon_D^3 = w + z\sqrt{D}$ with w, z integers. We are interested in whether $\sqrt{\varepsilon_D} \in K_1$ or not, which is equivalent to $\sqrt{\varepsilon_D^3} \in K_1$. Thus, we may assume that $\varepsilon_D = x + y\sqrt{D}$ where x, y are integers, where the norm of ε_D is equal to 1. Consequently, we get the equation $x^2 = Dy^2 + 1 \equiv 5y^2 + 1 \mod 8$, where x must be odd and y must be divisible by 4, due to the congruences.

Since g.c.d$(x - 1, x + 1) = 2$ and only one of these factors is divisible by 4, from the equation $(x - 1)(x + 1) = Dy^2$, we must have

$$\begin{cases} x + 1 = 2d_1y_1^2, \\ x - 1 = 2d_2y_2^2, \end{cases}$$

for some integers satisfying $d_1d_2 = pq_1q_2 = D$ and $2y_1y_2 = y$.

From Lemma 3.2.1 and Remark 3.2.2, we cannot have $d_i = 1$ or $d_i = D$. it is worth mentioning y_i has no common factors with d_j when $i \neq j$, due to the g.c.d condition. We also make the following observation:

Let $z = y_1\sqrt{2d_1} + y_2\sqrt{2d_2}$, then

$$z^2 = (2d_1y_1^2 + 2d_2y_2^2 + 2y\sqrt{D}) = 2(x + y\sqrt{D}) = 2\varepsilon_D.$$

Hence, $z = \sqrt{2\varepsilon_D}$ and since

$$2\sqrt{d_1\varepsilon_D} = \sqrt{2d_1}z = 2(y_1d_1 + y_2\sqrt{D}),$$

we have $\sqrt{d_1\varepsilon_D} = y_1d_1 + y_2\sqrt{D} = \gamma_1 \in K$, where

$$N_{K/\mathbb{Q}}(\gamma_1) = d_1(d_1y_1^2 - d_2y_2^2) = d_1.$$

In particular, $K_1(\sqrt{\varepsilon_D}) = K_1(\sqrt{d_i})$ for some proper divisors d_1, d_2, which implies $\sqrt{\varepsilon_D} \notin K_1$. There are 8 possibilities for d_1, we already discarded two of them. Suppose $d_1 \in \{pq_1, pq_2, q_1, q_2\}$. From our previous analysis. we have $\sqrt{q_i\varepsilon_D} \in K$, and $K_1(\sqrt{\varepsilon_D}) = K_1(\sqrt{q_i})$.

We also notice that $K(\sqrt{\varepsilon_D}) = K(\sqrt{p})$ if and only if $d_1 = p$ or $d_1 = q_1q_2$. In particular, if $K(\sqrt{\varepsilon_D}) = K(\sqrt{p})$, then $p = \varepsilon_D\gamma^2$ for some $\gamma \in K$, and the ideal over p is principal. Conversely, if the ideal over p is principal, then $K(\sqrt{\varepsilon_D}) = K(\sqrt{p})$.

If $d_1 = q_1q_2$, then

$$\begin{cases} x + 1 = 2q_1q_2y_1^2, \\ x - 1 = 2py_2^2. \end{cases}$$

Therefore,

$$-1 = \left(\frac{2p}{q_1}\right) = \left(\frac{2py_2^2}{q_1}\right) = \left(\frac{x-1}{q_1}\right) = \left(\frac{x+1-2}{q_1}\right) = \left(\frac{-2}{q_1}\right) = 1,$$

which is absurd. Thus, we must have

$$\begin{cases} x+1 = 2py_1^2, \\ x-1 = 2q_1q_2y_2^2. \end{cases}$$

Then, as discussed previously,

$$\sqrt{p\varepsilon_D} = py_1 + y_2\sqrt{D} = \gamma_1 \in k$$

in this case, with $N_{K/\mathbb{Q}}(\gamma_1) = p$.

We now focus on $K' = \mathbb{Q}(\sqrt{2D})$. Let $\varepsilon_{2D} = r + s\sqrt{2D}$, where $r^2 = 2Ds^2 + 1$. Since $r^2 \equiv 2s^2 + 1 \mod 8$, r is odd and s is even. Since $(r+1)(r-1) = 2Ds^2$, we must have in this case:

$$\begin{cases} r \pm 1 = d_1s_1^2, \\ r \mp 1 = 2d_2s_2^2, \end{cases}$$

for some integers satisfying $d_1d_2 = D$ and $s_1s_2 = s$.

The cases $d_1 = 1$ and $d_1 = D$ are excluded again by Lemma 3.2.1, therefore $\sqrt{\varepsilon_{2D}} \notin K_1$. If $d_1 = pq_1$ or $d_1 = q_1$, then

$$\left(\frac{q_1}{q_2}\right) = \left(\frac{d_1}{q_2}\right) = \left(\frac{\pm 2}{q_2}\right),$$

and

$$\left(\frac{q_2}{q_1}\right) = -\left(\frac{2d_2}{q_1}\right) = -\left(\frac{\mp 2}{q_2}\right) = \left(\frac{\pm 2}{q_2}\right) = \left(\frac{q_1}{q_2}\right).$$

which is impossible due to quadratic reciprocity. By symmetry, we must have $d_1 = p$ or $d_1 = q_1 q_2$. If $d_1 = q_1 q_2$, then

$$\left(\frac{q_1 q_2}{p}\right) = \left(\frac{\pm 2}{p}\right) = -1,$$

which is impossible by the Legendre conditions. Thus, we must have

$$\begin{cases} r \pm 1 = p s_1^2, \\ r \mp 1 = 2 q_1 q_2 s_2^2. \end{cases}$$

If

$$\begin{cases} r + 1 = p s_1^2, \\ r - 1 = 2 q_1 q_2 s_2^2, \end{cases}$$

then

$$\left(\frac{p}{q_2}\right) = \left(\frac{2}{q_2}\right) = -1,$$

which contradicts our assumption. Therefore,

$$\begin{cases} r - 1 = p s_1^2, \\ r + 1 = 2 q_1 q_2 s_2^2. \end{cases}$$

Let $z = s_1\sqrt{p} + s_2\sqrt{2q_1q_2}$. Then, $z = \sqrt{2\varepsilon_{2D}}$ and

$$\sqrt{2}\sqrt{p\varepsilon_{2D}} = ps_1 + s_2\sqrt{2D} = \gamma_2 \in K',$$

with $N_{K'/\mathbb{Q}}(\gamma_2) = -2p$, and $K_1(\sqrt{\varepsilon_{2D}}) = K_1(\sqrt{p})$, since $\sqrt{2} \in K_1$.

We can conclude that $\sqrt{\varepsilon_D\varepsilon_{2D}} \in K_1$ if and only if $K_1(\sqrt{\varepsilon_{2D}}) = K_1(\sqrt{\varepsilon_D}) = K_1(\sqrt{p})$, which happens if and only if p is principal. In this case,

$$p \cdot \sqrt{2} \cdot \sqrt{\varepsilon_D\varepsilon_{2D}} = \gamma_1\gamma_2.$$

We first notice that $N_{K_1/K}(\sqrt{2}) = N_{K_1/K'}(\sqrt{2}) = -2$, since the corresponding automorphisms change the sign of $\sqrt{2}$. Taking norms on both sides of the equation we get the following:

$$\begin{aligned} -2p^2 N_{K_1/K}(\sqrt{\varepsilon_D\varepsilon_{2D}}) &= \gamma_1^2(-2p) = -2p^2\varepsilon_D; \\ -2p^2 N_{K_1/K'}(\sqrt{\varepsilon_D\varepsilon_{2D}}) &= p\gamma_2^2 = 2p^2\varepsilon_{2D}; \\ 2p^2 N_{K_1/\mathbb{Q}_1}(\sqrt{\varepsilon_D\varepsilon_{2D}}) &= (p)(-2p) = -2p^2. \end{aligned}$$

The assertion about the norms then follows.

The two possible Rédei-Reichardt matrices for K' are

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

The rank of both matrices is 3, from where it follows (Equation (1.3)) that the 4-rank

of $Cl^+(K')$ is 0. Consequently, $A'_0 \cong C_2 \times C_2$, as the 2-rank of the narrow class group is 3 (Equation (1.1)).

Finally, by Theorem 2.2.1,

$$|A_1| = \frac{1}{4} \cdot q(K_1) \cdot |A_0| \cdot |A'_0| = q(K_1) \cdot |A_0|,$$

from where we can conclude that $X_\infty \cong A_0$ when p is not principal, since $q(K_1) = 1$ in this case, and $|A_1| = 2\,|A_0|$ otherwise. □

Example 3.2.4. We present some examples when $p = 5$ and $q_1 = 11$ in the following table:

p	q_1	q_2	Is $\sqrt{\varepsilon_D \varepsilon_{2D}} \in k_1$?	X_∞
5	11	19	No	$A_0 = C_4$
5	11	59	No	$A_0 = C_4$
5	11	139	No	$A_0 = C_4$
5	11	179	No	$A_0 = C_4$
5	11	331	Yes	$A_1 = C_{16}$
5	11	691	Yes	$A_1 = C_8$
5	11	131	Yes	$A_2 = C_{16}$
5	11	211	Yes	$A_2 = C_{16}$

Table 3.3: X_∞ for second case with $\left(\frac{p}{q_1}\right) = \left(\frac{p}{q_2}\right) = 1$

It looks difficult to predict where the chain stops when $\sqrt{\varepsilon_D \varepsilon_{2D}} \notin K_1$, as it presents a similar behavior to the non-trivial case in Example 3.1.3.

In their paper [14], the authors proved that $X_\infty \cong A_0$ in the following cases:

1. $q_2 \equiv 3 \mod 8$, where $\left(\frac{q_1 q_2}{p}\right) = -1$.
2. $q_2 \equiv 3 \mod 8$, where $\left(\frac{q_1}{p}\right) = \left(\frac{q_2}{p}\right) = 1$, and the ideal above p in K is not principal. (Theorem 3.2.3)

3. $q_2 \equiv 7 \mod 8$, where $\left(\frac{q_2}{p}\right) = -1$.

4. $q_2 \equiv 7 \mod 8$, where $\left(\frac{q_2}{p}\right) = \left(\frac{q_1}{p}\right) = 1$, and the ideal above q_2 in K is not principal.

We could give an alternative proof to these results using the techniques from Theorem 3.2.3, but we would rather draw some conclusions on the following case:

Lemma 3.2.5. *Let $K = \mathbb{Q}(\sqrt{D})$ where $D = pq_1q_2$, such that $p \equiv 5 \mod 8$, $q_1 \equiv q_2 \equiv 3 \mod 8$, and $\left(\frac{p}{q_1}\right) = \left(\frac{p}{q_2}\right) = -1$. Then the ideal above p in K is principal. Furthermore, the only possible F.S.U. of K_1 are $\{\varepsilon_D, \varepsilon_{2D}, \varepsilon_2\}$ or $\{\sqrt{\varepsilon_D\varepsilon_{2D}}, \varepsilon_D, \varepsilon_2\}$.*
Let $\varepsilon_{2D} = r + s\sqrt{2D}$. Then $\sqrt{\varepsilon_D\varepsilon_{2D}} \in K_1$ if and only if $p(r+1)$ is a square. In this case,

$$N_{K_1/K}(\sqrt{\varepsilon_D\varepsilon_{2D}}) = -\varepsilon_D,\ N_{K_1/K'}(\sqrt{\varepsilon_D\varepsilon_{2D}}) = \varepsilon_{2D},\ N_{K_1/\mathbb{Q}_1}(\sqrt{\varepsilon_D\varepsilon_{2D}}) = -1.$$

Proof. The simple ambiguous forms of K are:

$$f = [1, 0, -pq_1q_2],\ g = [p, 0, -q_1q_2],\ h = [q_1, 0, -pq_2],\ l = [q_2, 0, -pq_1],$$

$$\overline{f} = [-1, 0, pq_1q_2],\ \overline{g} = [-p, 0, q_1q_2],\ \overline{h} = [-q_1, 0, pq_2],\ \overline{l} = [-q_2, 0, pq_1].$$

There are some minor typos in Kaplan's original paper ([18], Proposition A_5). Let $\left(\frac{p}{q_1}\right) = \tau$, $\left(\frac{p}{q_2}\right) = \tau'$ and $\left(\frac{q_1}{q_2}\right) = \tau''$. Then the table of generic characters is:

	f	$\overline{f}$	g	$\overline{g}$	h	$\overline{h}$	l	$\overline{l}$
$\left(\frac{m}{p}\right)$	1	1	$\tau\tau'$	$\tau\tau'$	τ	τ	τ'	τ'
$\left(\frac{m}{q_1}\right)$	1	-1	τ	$-\tau$	$\tau\tau''$	$-\tau\tau''$	$-\tau''$	τ''
$\left(\frac{m}{q_2}\right)$	1	-1	τ'	$-\tau'$	τ''	$-\tau''$	$-\tau'\tau''$	$\tau'\tau''$

Table 3.4: Generic characters for the second case with $q_2 \equiv 3 \mod 8$

Hence, $\overline{g}$ is the only form in the principal genus and the 2-part of the narrow class group is $C_2 \times C_2$. Since the norm of the fundamental unit is 1, we must have $A_0 \cong C_2$. Moreover, q_1q_2

is a principal factor, which implies that $K_1(\sqrt{\varepsilon_D}) = K_1(\sqrt{q_1q_2}) = K_1(\sqrt{p})$ and $\sqrt{\varepsilon_D} \notin K_1$.

We proceed as we did in Theorem 3.2.3. Let $D = pq_1q_2$. Replacing ε_D with ε_D^3 if necessary, we can assume that $\varepsilon_D = x + y\sqrt{D}$ with x odd, y even. Hence,

$$\begin{cases} x + 1 = 2d_1y_1^2, \\ x - 1 = 2d_2y_2^2, \end{cases}$$

with $d_1d_2 = D$ and $2y_1y_2 = y$. From the previous observations, we can assume that $d_1 = p$ or $d_1 = q_1q_2$. If $d_1 = p$, then

$$\begin{cases} x + 1 = 2py_1^2, \\ x - 1 = 2q_1q_2y_2^2, \end{cases}$$

implies

$$\left(\frac{2p}{q_1}\right) = \left(\frac{2}{q_1}\right) = -1,$$

which is impossible. Therefore,

$$\begin{cases} x + 1 = 2q_1q_2y_1^2, \\ x - 1 = 2py_2^2. \end{cases}$$

Let $z = y_2\sqrt{2p} + y_1\sqrt{2q_1q_2}$. Then $z = \sqrt{2\varepsilon_D}$, and we must have

$$2\sqrt{p\varepsilon_D} = \sqrt{2p} \cdot z = 2py_2 + 2y_1\sqrt{D}$$

Hence, $\sqrt{p\varepsilon_D} = py_2 + y_1\sqrt{D} = \gamma_1$, where γ_1 has norm $-p$ in $\mathbb{Q}$.

Let $\varepsilon_{2D} = r + s\sqrt{2D}$, where r is odd and s is even. Then

$$\begin{cases} r \pm 1 = d_1 s_1^2, \\ r \mp 1 = 2d_2 s_2^2, \end{cases}$$

with $d_1 d_2 = D$ and $s_1 s_2 = s$. The cases $d_2 = 1$ or D cannot happen due to Lemma 3.2.1. This immediately implies that $\sqrt{\varepsilon_{2D}} \notin K_1$, since $\sqrt{d_1 \varepsilon_{2D}} \in K_1$ for some proper divisor d_1 of D. In particular, $K_1(\sqrt{\varepsilon_{2D}}) = K_1(\sqrt{\varepsilon_D})$ if and only if one of d_1 is equal to p or $q_1 q_2$. If $d_2 = p$, then

$$\begin{cases} r \pm 1 = q_1 q_2 s_1^2, \\ r \mp 1 = 2ps_2^2. \end{cases}$$

Thus, we get

$$\left(\frac{q_1 q_2}{p}\right) = \left(\frac{\pm 2}{p}\right) = -1.$$

which is absurd.

Hence, in this case, we must have

$$\begin{cases} r \pm 1 = ps_1^2, \\ r \mp 1 = 2q_1 q_2 s_2^2. \end{cases}$$

If

$$\begin{cases} r - 1 = ps_1^2, \\ r + 1 = 2q_1 q_2 s_2^2, \end{cases}$$

then

$$\left(\frac{p}{q_1}\right) = \left(\frac{-2}{q_1}\right) = 1.$$

which is a contradiction. Therefore,

$$\begin{cases} r+1 = ps_1^2, \\ r-1 = 2q_1q_2s_2^2, \end{cases}$$

is the only possibility and $\sqrt{\varepsilon_D\varepsilon_{2D}} \in K_1$ if only if $p(r+1)$ is a square.

Let $w = s_1\sqrt{p} + s_2\sqrt{2q_1q_2}$. Then

$$w^2 = (ps_1^2 + 2q_1q_2s_2^2 + 2y\sqrt{2D}) = 2\varepsilon_{2D}.$$

Since $w = \sqrt{2\varepsilon_D}$, we have

$$\sqrt{2p\varepsilon_{2D}} = \sqrt{p} \cdot w = ps_1 + s_2\sqrt{2D} = \gamma_2,$$

where the norm of γ_2 is equal to $2p$.

Multiplying these equations, we obtain $\sqrt{2}p \cdot \sqrt{\varepsilon_D\varepsilon_{2D}} = \gamma_1\gamma_2$ and the result on the norms follows as before. □

Example 3.2.6. We give a list of examples where $\sqrt{\varepsilon_D\varepsilon_{2D}} \notin K_1$ for $p = 5$, $q = 3$:

p	q_1	q_2	X_∞
5	3	43	A_1
5	3	67	A_1
5	3	227	A_1
5	3	283	A_1
5	3	307	A_1
5	3	347	A_1
5	3	443	A_1
5	3	467	A_1
5	3	523	A_1
5	3	547	A_1
5	3	683	A_1
5	3	787	A_1

Table 3.5: X_∞ for second case with $\left(\frac{p}{q_1}\right) = \left(\frac{p}{q_2}\right) = -1$ where $\sqrt{\varepsilon_D \varepsilon_{2D}} \notin K_1$

As we can see, there is a clear pattern that we will explore in the next section for this case.

Examples where $\sqrt{\varepsilon_D \varepsilon_{2D}} \in K_1$:

p	q_1	q_2	$\lvert A_1 \rvert$	$\lvert A_2 \rvert$	$\lvert A_3 \rvert$
5	3	83	8	16	32
5	3	107	8	16	32
5	3	163	8	8	8
5	3	347	8	8	8
5	3	563	16	32	32
5	3	587	8	8	8
5	3	643	8	16	16

Table 3.6: X_∞ for second case with $\left(\frac{p}{q_1}\right) = \left(\frac{p}{q_2}\right) = -1$ where $\sqrt{\varepsilon_D \varepsilon_{2D}} \in K_1$

In this case, the behavior seems to be more complicated. We also mention that the discrepancy in $|A_1|$ for $q_2 = 563$ is because $A_0' \cong C_8 \times C_2$ for that particular prime.

Similar results can be obtained for the case $q_2 \equiv 7 \mod 8$. In fact, in [14] the authors prove that for the case where $\left(\frac{p}{q_2}\right) = 1$ and $\left(\frac{p}{q_1}\right) = -1$ we have $K_1(\sqrt{\varepsilon_D}) = K_1(\sqrt{\varepsilon_{2D}})$,

whilst for $\left(\frac{p}{q_2}\right) = -1$ this only happens when the ideal over q_1 in K is principal, which is again equivalent to $\sqrt{\varepsilon_D \varepsilon_{2D}} \in K_1$. It is harder to determine the sign of norms of $\sqrt{\varepsilon_D \varepsilon_{2D}}$ in this case.

3.2.1 Class group of K_2

Throughout this section, we will analyze the intermediate subfields of $K_2/\mathbb{Q}_1$ to get a new example of Greenberg's conjecture. To this end, we have the following result:

Lemma 3.2.7. *Let $K = \mathbb{Q}(\sqrt{D})$ where $D = pq_1q_2$ with $p \equiv 5 \mod 8$, $q_1 \equiv 3 \mod 8$ and $q_2 \equiv 3 \mod 4$. Then the 2-class group of $K_1' = \mathbb{Q}\left(\sqrt{(2+\sqrt{2})D}\right)$ is isomorphic to $C_2 \times C_2$.*

Proof. We first show that the 2-rank of A_1' is 2. Consider the extension $K_1/\mathbb{Q}_1$. From ([1], Theorem 1), we see that $\pm\varepsilon_2$ is not a norm from K_1. Indeed, from ([2], Theorem 2.5), if $\mathcal{Q}$ is the ideal over q_1 in $\mathbb{Q}_1$ (there is only one), then

$$\left(\frac{\varepsilon_2, D}{\mathcal{Q}}\right) = \left(\frac{N_{\mathbb{Q}_1/\mathbb{Q}}(\varepsilon_2), D}{q_1}\right) = \left(\frac{-1, D}{q_1}\right) = -1,$$

which implies that ε_2 is not a norm, since $K_1 = \mathbb{Q}_1(\sqrt{D})$ (Remark 2.3.7).

Following ([25],Lemma 3.5), if $\mathcal{L}$ is not a 2-adic prime of $\mathbb{Q}_1$, then the extension $\mathbb{Q}_2/\mathbb{Q}_1$ is unramified at $\mathcal{L}$. Since $\mathbb{Q}_2 = \mathbb{Q}_1(\varepsilon_2\sqrt{2})$, the Hilbert symbol satisfies:

$$\left(\frac{\varepsilon_2, \varepsilon_2\sqrt{2}}{\mathcal{L}}\right) = 1.$$

Multiplying the symbols we obtain

$$\left(\frac{\varepsilon_2, D\varepsilon_2\sqrt{2}}{\mathcal{Q}}\right) = -1.$$

Thus, we know that ε_2 is not a norm from $K_1' = \mathbb{Q}_1(\sqrt{D\varepsilon_2\sqrt{2}})$ in both cases. Using a similar argument, one can conclude that -1 is not a norm if $q_2 \equiv 7 \mod 8$, since for a prime $\mathcal{Q}$ over q_2 satisfying $\left(\frac{2}{q_2}\right) = 1$, Azizi ([1]) showed that

$$\left(\frac{-1, D}{\mathcal{Q}}\right) = \left(\frac{-1}{q_2}\right) = -1,$$

whereas for $q_2 \equiv 3 \mod 8$, this symbol is always one.

Next, we apply the genus formula to the extension $K_1'/\mathbb{Q}_1$. If $q_2 \equiv 3 \mod 8$, there are 4 ramifying primes in this extension: the 3 primes from the divisors of D and one prime over 2. Hence,

$$r_2(A_0') = 3 - e,$$

where e is the norm unit index (Equation (2.2)). Thus, the 2-rank is at most 2. Since the extension $K_1'(\sqrt{p}, \sqrt{q_1 q_2})$ is unramified and biquadratic over K_1', it follows that the 2-rank of the class group is exactly 2.

Conversely, when $q_2 \equiv 7 \mod 8$, there are 5 primes that ramify, as q_2 splits in $\mathbb{Q}_1$. Then, since -1 and ε_2 are not norms, we must have

$$r_2(A_0') = 4 - e = 4 - 2 = 2.$$

In any case, the class group of K_1' is of the form $C_{2^m} \times C_{2^n}$ for some $m, n \geq 1$.

The cyclicity of the groups A_n plays a significant role in the following argument. Consider

the intermediate fields of the extension $M = K_1'(\sqrt{p}, \sqrt{q_1 q_2})$ over K_1'; i.e, the fields

$$M_1 = \mathbb{Q}\left(\sqrt{2+\sqrt{2}}, \sqrt{pq_1q_2}\right) = K_2\ ;$$
$$M_2 = \mathbb{Q}\left(\sqrt{(2+\sqrt{2})p}, \sqrt{q_1q_2}\right);$$
$$M_3 = \mathbb{Q}\left(\sqrt{(2+\sqrt{2})q_1q_2}, \sqrt{p}\right).$$

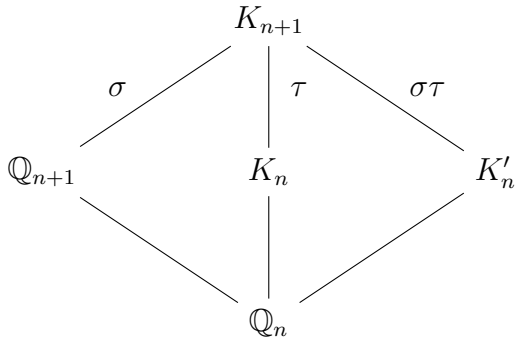
Suppose H is the 2-class field of K_1' with Galois group $C_{2^m} \times C_{2^n}$.

If $m, n \geq 2$, the extension M/K_1' is unramified and its Galois group $\mathrm{Gal}(M/K_1') \cong C_2 \times C_2$ is contained in both $C_{2^2} \times C_2$ and $C_2 \times C_{2^2}$, which are proper subgroups of $\mathrm{Gal}(H/K_1')$. It follows that the two unramified extensions corresponding to these subgroups contain both M and $M_1 = K_2$, which is impossible, since K_2 cannot have two different unramified extensions of the same order, as its class group is cyclic.

Therefore, $A_1' \cong C_2 \times C_{2^n}$ for some $n \geq 1$. The extension H/K_2 is unramified and abelian, hence it must be cyclic. It follows that $Gal(H/M)$ is also cyclic, and it is contained in $Gal(H/M_i)$ for $i = 1, 2, 3$, which are the 3 different subgroups of index two of A_1'.

Let $A_1' \cong \langle a \rangle \times \langle b \rangle$, where a has order 2 and b has order 2^n. The subgroups of index 2 correspond to $\langle b \rangle$, $\langle a \cdot b \rangle$, and $\langle a \rangle \times \langle b^2 \rangle$. These groups have trivial intersection, thus $Gal(H/M)$ is trivial, and $H = M$. The result then follows, since $Gal(M/K_1') \cong C_2 \times C_2$. $\square$

The following result is derived from ([20], Lemma 2.1) and is proved in [14]. Even though the authors prove it for the current case, it holds with more generality. Consider the following diagram



where both σ and τ are generators of the corresponding Galois groups.

Lemma 3.2.8. *Let $K = \mathbb{Q}(\sqrt{D})$ with $D \equiv 5 \pmod 8$. Then*

$$|A_{n+1}| \leq \frac{|A'_n| \cdot |A_n|}{2 \cdot \left[E(K_n) : N_{K_{n+1}/K_n}(E(K_{n+1}))\right]} \leq \frac{1}{2} \cdot |A_n| \cdot |A'_n|$$

Proof. The proof is analogous to ([14], Lemma 5.1), since the prime 2 is inert in the extension $K/\mathbb{Q}$, the same steps can be taken whenever this happens. We write it down for completion.

By ([24],Remark 2.6), σ acts as -1 on A_{n+1}, since the class group of $\mathbb{Q}_n$ is always trivial. This implies that $A_{n+1}^{\sigma\tau-1} = A_{n+1}^{\tau+1}$, where $A_{n+1}^{\tau+1} = \{[\mathfrak{a}]^\tau \cdot [\mathfrak{a}] : [\mathfrak{a}] \in A_{n+1}\}$.

From the long exact sequence:

$$1 \longrightarrow A_{n+1}^{\langle\sigma\tau\rangle} \longrightarrow A_{n+1} \longrightarrow A_{n+1}^{\sigma\tau-1} \longrightarrow 1.$$

It follows that $|A_{n+1}| = \left|A_{n+1}^{\langle\sigma\tau\rangle}\right| \cdot \left|A_{n+1}^{\tau+1}\right|$. By the genus formula on the quadratic extension K_{n+1}/K'_n (Theorem 2.3.6), we have

$$\left|A_{n+1}^{\langle\sigma\tau\rangle}\right| = \frac{|A'_n| \cdot 2^{t-1}}{e(K_{n+1}/K'_n)}$$

where t is the number of prime ideals ramified on K_{n+1}/K'_n and $e(K_{n+1}/K'_n)$ is the norm unit index. It is easy to see that the extension K_{n+1}/K'_n is always unramified, since

$K_{n+1} = K'_n(\sqrt{D})$. Therefore, $|A_{n+1}| \leq \frac{1}{2} \cdot |A'_n| \cdot \left|A_{n+1}^{\tau+1}\right|$.

Since $A_{n+1}^{\tau+1}$ is contained in the group $B(K_{n+1})^{\langle\tau\rangle}$ of classes containing an ideal fixed by the action of τ (Theorem 2.3.6), and the extension K_{n+1}/K_n is totally ramified, the following inequality holds:

$$\left|A_{n+1}^{\tau+1}\right| \leq \left|B(K_{n+1})^{\langle\tau\rangle}\right| = \frac{|A_n|}{\left[E(K_n) : N_{K_{n+1}/K_n}(E(K_{n+1}))\right]}$$

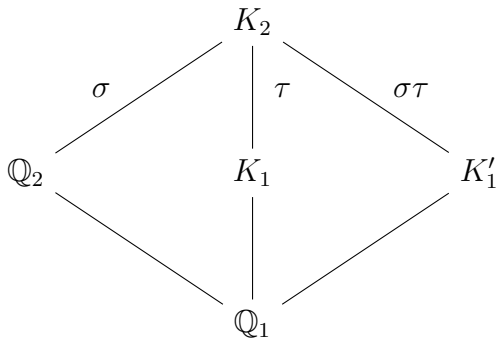
Piecing everything together, the result follows. □

Remark. As mentioned in [14], if $D \equiv 1 \mod 8$, we obtain

$$|A_{n+1}| \leq \frac{|A'_n| \cdot |A_n|}{\cdot \left[E(K_n) : N_{K_{n+1}/K_n}(E(K_{n+1}))\right]} \leq |A_n| \cdot |A'_n|$$

instead, since 2 splits in K. The inclusion of the index $\left[E(K_n) : N_{K_{n+1}/K_n}(E(K_{n+1}))\right]$ is important to our study since we will prove that there are units in K_n that are not norms from $E(K_{n+1})$, even if they are norms from K_{n+1}^*.

We will try to determine an F.S.U of the field $K_2 = \mathbb{Q}\left(\sqrt{2+\sqrt{2}}, \sqrt{D}\right)$ by analyzing the units of the intermediate fields in the following diagram:



By Dirichlet's unit theorem, the $\mathbb{Z}$-rank of the units of the intermediate fields is 3, and the $\mathbb{Z}$-rank of $E(K_2)$ is 7. We also note that they all share ε_2 , hence $E(K_1) \cdot E(K_1') \cdot E(\mathbb{Q}_2)$ has $\mathbb{Z}$-rank equal to 7 and it has finite index in $E(K_2)$. This is also apparent from Lemmermeyer's formula (Theorem 2.2.2).

First, we notice that if x is K_1, the norm from K_2 to any of the other subfields is equal to $N_{K_1/\mathbb{Q}_1}(x)$, since the other automorphisms change $\sqrt{D}$. The same argument works as well if x is in the other fields. From Wada's analysis [30], the units of $E(K_2)$ are generated by the units of the intermediate fields and the elements of $E(K_1) \cdot E(K_1') \cdot E(\mathbb{Q}_2)$ that are squares in K_2. To see this, if $u \in E(K_2)$, then

$$N_{K_2/K_1}(u) \cdot N_{K_1/K_1'}(u) \cdot N_{K_2/\mathbb{Q}_2}(u) = u^2 \cdot N_{K_2/\mathbb{Q}_1}(u).$$

The units of $\mathbb{Q}_2$ are determined by the cyclotomic units [31],

$$\xi_a = \frac{\sin \pi a/16}{\sin \pi/16},\ a \in \{3, 5, 7\}$$

Then $\xi_5 = 1 + \sqrt{2} + \sqrt{2 + \sqrt{2}}$ has norm ε_2 in $\mathbb{Q}_1$ and $\xi_7 = 1 + \sqrt{2} + \sqrt{2}\sqrt{2 + \sqrt{2}}$ has norm -1. Since $\xi_3 \cdot \xi_5 \cdot \xi_7^{-1} = \varepsilon_2$, we can choose a F.S.U. $\{w_1, w_2, \varepsilon_2\}$ of $\mathbb{Q}_2$, such that $N_{\mathbb{Q}_2/\mathbb{Q}_1}(w_1) = \varepsilon_2$ and $N_{\mathbb{Q}_2/\mathbb{Q}_1}(w_2) = -1$.

In the extension $K_1'/\mathbb{Q}_1$, as seen in Lemma 3.2.7, ε_2 is not a norm. In particular, if v is a unit with $N_{K_1'/\mathbb{Q}_1}(v) = \pm\varepsilon_2^n$, then n has to be even, otherwise $v \cdot \varepsilon_2^{-(n-1)/2}$ has norm ε_2. Since ε_2 forms part of the fundamental system of $E(K_1')$, as $\sqrt{\varepsilon_2} \notin K_1'$, the unit v can be replaced by $v \cdot \varepsilon_2^{-n/2}$, so that its norm is ± 1. In particular, we can choose a F.S.U. of $E(K_1')$ of the form $\{v_1, v_2, \varepsilon_2\}$, where $N_{K_1'/\mathbb{Q}_1}(v_1) = 1$, and $N_{K_1'/\mathbb{Q}_1}(v_2) = \pm 1$, depending on whether -1 is a norm or not.

In view of Example 3.2.6, we prove the following result about one of the cases discussed in Lemma 3.2.5:

Theorem 3.2.9. *Let $K = \mathbb{Q}(\sqrt{D})$ where $D = pq_1q_2$, such that $p \equiv 5 \mod 8$, $q_1, q_2 \equiv 3 \mod 8$, and $\left(\frac{p}{q_1}\right) = \left(\frac{p}{q_2}\right) = -1$. Furthermore, suppose that $\sqrt{\varepsilon_D \varepsilon_{2D}} \notin K_1$. Then $X_\infty \cong A_1$.*

Proof. We will show that $|A_2| = |A_1|$. From Lemma 3.2.7, we must have $|A_1'| = 4$. Thus, from Lemma 3.2.8 we have

$$|A_2| \leq \frac{2 \cdot |A_1|}{\left[E(K_1) : N_{K_2/K_1}(E(K_2))\right]} \leq 2 \cdot |A_1| \,.$$

From Lemmermeyer's formula (Theorem 2.2.2 and Equation (2.1)),

$$|A_2| = \frac{1}{8} \cdot q(K_2) \cdot |A_1| \cdot |A_1'| = \frac{q(K_2)}{2} \cdot |A_1| \,,$$

which implies that $q(K_2)$ is at most 4; i.e., at most two independent elements of $E(K_1) \cdot E(K_1') \cdot E(\mathbb{Q}_2)$ are squares in K_2.

Since $\sqrt{\varepsilon_D \varepsilon_{2D}} \notin K_1$, the fundamental system of K_1 is $\{\varepsilon_D, \varepsilon_{2D}, \varepsilon_2\}$. The F.S.U. of $E(K_1')$ is of the form $\{v_1, v_2, \varepsilon_2\}$, where $N_{K_1'/\mathbb{Q}_1}(v_1) = 1$, and $N_{K_1'/\mathbb{Q}_1}(v_2) = -1$. The one for $E(\mathbb{Q}_2)$ is $\{w_1, w_2, \varepsilon_2\}$, where $N_{\mathbb{Q}_2/\mathbb{Q}_1}(w_1) = \varepsilon_2$, and $N_{\mathbb{Q}_2/\mathbb{Q}_1}(w_2) = -1$.

Suppose $u \in E(K_2)$ satisfies

$$u^2 = \varepsilon_D^a \, \varepsilon_{2D}^b \, \varepsilon_2^c \, v_1^d \, v_2^e \, w_1^f \, w_2^g.$$

Applying the norm to K_1 on both sides of the equation, we have

$$N_{K_2/K_1}(u)^2 = \varepsilon_D^{2a} \, \varepsilon_{2D}^{2b} \, \varepsilon_2^{2c} \, (-1)^e \, \varepsilon_2^f \, (-1)^g.$$

Since ε_2 is not a square in K_1, it follows that $e \equiv g \mod 2$, and $f \equiv 0 \mod 2$. Hence,

$$u^2 = \varepsilon_D^a \, \varepsilon_{2D}^b \, \varepsilon_2^c \, v_1^d \, v_2^e \, w_2^e \, t^2, \text{ for some } t.$$

For now, we omit t, since it can be included inside u, with the idea in mind that the norm to K_1 of any square we leave out of the equations always lies in $\mathbb{Q}_1$. By taking the norm to $\mathbb{Q}_2$, we can see that

$$N_{K_2/\mathbb{Q}_2}(u)^2 = \varepsilon_2^{2c} \, (-1)^e \, w_2^{2e},$$

which implies $e \equiv 0 \mod 2$. Hence,

$$u^2 = \varepsilon_D^a \, \varepsilon_{2D}^b \, \varepsilon_2^c \, v_1^d$$

modulo squares. Suppose $N_{K_2/K_1}(E(K_2)) = E(K_1)$, so that both ε_D and ε_{2D} are norms from K_2. If $N_{K_2/K_1}(u) = \varepsilon_{2D}$, then we can write

$$u^2 = \varepsilon_D^a \, \varepsilon_{2D}^b \, \varepsilon_2^c \, v_1^d \, t^2,$$

where the norm of t is some element w in $\mathbb{Q}_1$. By applying the norm to K_1 on both sides,

we have

$$\varepsilon_D^2 = \varepsilon_D^{2a}\ \varepsilon_{2D}^{2b}\ \varepsilon_2^{2c}\ w^2,$$

from where we conclude that $b = 0$ and $a = 1$. Consequently, $u^2 = \varepsilon_D\ \varepsilon_2^c\ v_1^d$ for some $c, d \in \{0, 1\}$. Similarly, if $N_{K_2/K_1}(v) = \varepsilon_{2D}$, then $v^2 = \varepsilon_D\ \varepsilon_2^m\ v_1^n$ for some $m, n \in \{0, 1\}$.

First, we notice that we cannot have mixed terms inside the square root since this would give us 3 independent square roots by taking the product. For example, $\sqrt{\varepsilon_D v_1}$ and $\sqrt{\varepsilon_{2D} v_1}$ being in K_2 implies that $\sqrt{\varepsilon_D \varepsilon_{2D}} \in K_2$. We also notice that $K_2(\sqrt{\varepsilon_D}) = K_2(\sqrt{d_1})$ for some proper divisor d_1 of D, as seen in Lemma 3.2.5, so that we cannot have $\sqrt{\varepsilon_D} \in K_2$. Similarly, both $\sqrt{\varepsilon_{2D}}$ and $\sqrt{\varepsilon_D \varepsilon_{2D}}$ are not in K_2.

Therefore, either $\sqrt{\varepsilon_D \varepsilon_2} \in K_2$ or $\sqrt{\varepsilon_{2D} \varepsilon_2} \in K_2$. Consider the map θ in $\mathrm{Gal}(K_2/\mathbb{Q})$ defined by

$$\theta\left(\sqrt{2+\sqrt{2}}\right) = \sqrt{2-\sqrt{2}}\ ,\ \theta(\sqrt{D}) = \sqrt{D}.$$

Suppose $\sqrt{\varepsilon_{2D} \varepsilon_2} = u \in K_2$. Since $\theta(\sqrt{2}) = -\sqrt{2}$, then $\theta(\varepsilon_{2D})$ is its conjugate over $\mathbb{Q}$. Thus,

$$(u \cdot \theta(u))^2 = N_{K'/\mathbb{Q}}(\varepsilon_{2D}) \cdot N_{\mathbb{Q}_1/\mathbb{Q}}(\varepsilon_2) = -1,$$

which is impossible. Similarly, if $\sqrt{\varepsilon_D \varepsilon_2} = u \in K_2$, then

$$(u \cdot \theta(u))^2 = -(\varepsilon_D)^2 < 0.$$

Therefore, at most one of these elements is a norm and $\left[E(K_1) : N_{K_2/K_1}(E(K_2))\right] > 1$,

which implies that $|A_2| \leq |A_1|$, by Lemma 3.2.8 and the result follows for this case using Theorem 2.3.3. $\square$

We end this section with an analysis of the cases that are left. For $q_2 \equiv 3 \mod 8$, the λ-invariant is equal to 0, except maybe in the cases where $\eta = \sqrt{\varepsilon_D \varepsilon_{2D}} \in K_1$. As seen in Example 3.2.6, some extra conditions are needed to have $X_\infty \cong A_1$. From our observations, $N_{K_1/\mathbb{Q}_1}(\eta) = -1$ whenever this happens. In particular, doing the same analysis as in the previous result, any square in K_2 is of the form

$$u^2 = (\eta v_2 w_2)^a \cdot \varepsilon_D^b \cdot \varepsilon_2^c \cdot v_1^d$$

It is clear that if one of $(\eta v_2 w_2) \cdot \varepsilon_2^c$ or $\varepsilon_D \cdot v_1 \cdot \varepsilon_2^c$ is not a square in K_2, then $|A_2| = |A_1|$, following the same ideas from the previous theorem. One could take a naive approach and try to analyze when $\varepsilon_D \cdot v_1$ is not a square, which is equivalent to $K_2(\sqrt{v_1}) \neq K_2(\sqrt{p})$. This condition seems rather complicated, as the units of K_1' are difficult to determine [20].

Moreover, if $v_1 = a + b\sqrt{2+\sqrt{2}}\sqrt{D}$ with $a, b \in \mathbb{Z}[\sqrt{2}]$, then $(a-1)(a+1) = (2+\sqrt{2})Db^2$. One could try to take a similar approach to that of the previous section, but the unit ε_2 complicates this idea in terms of factorization. Furthermore, if we take the quadratic symbol in the extension $\mathbb{Q}_1$ [23], the symbol $\left(\frac{2+\sqrt{2}}{p\mathcal{O}_{\mathbb{Q}_1}}\right)$ is equal to -1 ([23]), which makes it hard to determine if there is a contradiction regarding the quadratic symbols.

The case $q_2 \equiv 7 \mod 8$ appears to be even more complex, as it is not obvious whether η has norm 1 or -1. In this case, -1 is not a norm in the extension $K_1'/\mathbb{Q}_1$, so the units of this field K_1' could potentially appear in the square root of either element. To add to the complexity, the prime q_2 splits in $\mathbb{Z}[\sqrt{2}]$, so that the factorization problem depends on which prime above q_2 is chosen. Some parallels can be drawn with what will be presented in the next chapter, but there seems to be no real approach using the techniques at our disposal.

3.3 Third Case

Throughout this section, we assume $K = \mathbb{Q}(\sqrt{D})$, where $D = pq$ with $p \equiv 5 \pmod 8$, $q \equiv 1 \pmod 8$, and $\left(\frac{2}{q}\right)_4 \neq (-1)^{\frac{q-1}{8}}$. We provide new examples of infinite families of real quadratic fields in Theorem 2.3.9 satisfying Greenberg's conjecture. Following ([25], Theorem 4.1), we prove the following result:

Lemma 3.3.1. *The following statements hold:*

(i) Assume that the ideal Q above the prime q in K is not principal. Then the λ-invariant of the cyclotomic extension of K is 0 and $X_\infty \cong A_0$.

(ii) Assume that the ideal Q' above the prime q in K' is not principal, and $q \equiv 1 \mod 16$. Then the λ-invariant of the cyclotomic extension K is 0 and $X_\infty \cong A_1$.

Proof. Since $n_0 = 0$ for K, $n_0 = 1$ for K', and all the 2-groups involved are non-trivial, we can apply Proposition 2.3.1 and Corollary 2.3.2 with $N = 0$ or $N = 1$, once we prove that a non-trivial ideal capitulates in the next level.

Let Q denote the prime of K above q, and assume that it is not principal. Since $q \equiv 1 \mod 8$, it splits in $\mathbb{Q}_1 = \mathbb{Q}(\sqrt{2})/\mathbb{Q}$ and ramifies in $K/\mathbb{Q}$. Thus, Q splits into two primes Q_1, Q_2 in K_1. These primes cannot be principal, because they are conjugate by the non-trivial automorphism of $\mathrm{Gal}(K_1/K)$, so if $Q_1 = \langle \alpha \rangle$, it follows that $Q = \langle N_{K_1/K}(\alpha) \rangle$ in K, which is a contradiction by our assumption. Since all q-adic primes ramify in K_1/Q_1, it follows that Q_i^2 comes from an ideal of $\mathbb{Q}_1$ for $i = 1, 2$. Since the class group of $\mathbb{Q}_1$ is trivial, it follows that Q_i^2 is principal in K_1. Any cyclic group has a unique element of order 2, therefore Q_1 and Q_2 lie within the same class of A_1. Hence, $Q = Q_1 Q_2$ is principal in K_1 and Q capitulates in K_1. By Proposition 2.3.1 and corollary 2.3.2, the result follows for the first statement.

Let Q' be the prime above q in K'. Assume Q' is not principal and $q \equiv 1 \mod 16$. Since q splits in $\mathbb{Q}_1$, it follows that Q' splits into two non-principal prime ideals $Q'_1,\ Q'_2$ of K_1. The field $\mathbb{Q}_2 = \mathbb{Q}(\sqrt{2+\sqrt{2}})$ is contained in $\mathbb{Q}(\zeta_{16})$ (it is the maximal real subfield). Since $q \equiv 1 \mod 16$, it splits completely in the extension $\mathbb{Q}(\zeta_{16})/\mathbb{Q}$ [31]. Therefore, both primes Q'_1 and Q'_2 are non-trivial and split in K_2. Since the q-adic primes are ramified in $K_2/\mathbb{Q}_2$ and the group A_2 is cyclic, both primes capitulate in K_2 due to a similar argument. Once again, we can conclude by Proposition 2.3.1 and Corollary 2.3.2 that $X_\infty \cong A_1$. □

Remark. The case $q \equiv 9 \mod 16$ turns out to be more complex: the inertia degree in $\mathbb{Q}(\zeta_{16})/\mathbb{Q}$ is equal to the order modulo 16, which in this case is 2. The primes over q in $\mathbb{Q}_1$ become inert in $\mathbb{Q}_2$, therefore the primes Q'_1 and Q'_2 are inert in the extension K_2/K_1, and one cannot draw the same conclusion. Some work has been done with similar cases using circular units ([20]) to analyze the units of the field K'_1 or using Iwasawa theory [11]. Still, the modular conditions make it hard to get similar results. We will refer to this case in the next chapter, as its complexity requires some degree of explanation.

Proposition 3.3.2. *Let N denote the norm map of the corresponding field to $\mathbb{Q}$. Then the following hold:*

(i) If $N(\varepsilon_D) = -1$, then the ideal above q in K is not principal.

(ii) If $N(\varepsilon_{2D}) = -1$, then the ideal above q in K' is not principal.

Proof. First, assume that $N(\varepsilon_D) = -1$. Let Q denote the prime of K above q. Assume by contradiction that Q is principal. Then there exists a fractional ideal $\langle x \rangle$ in K such that $Q = \langle x \rangle$. By squaring, we get $q = x^2 \cdot \varepsilon_D^n$ for some n. Applying the norm map on both sides, it follows that $q^2 = N_{K/\mathbb{Q}}(x)^2(-1)^n$. Hence, n is even and

$$q = (|N_{K/\mathbb{Q}}(x)| \cdot \varepsilon_D^{\frac{n}{2}})^2.$$

Therefore, $\sqrt{q} \in K$, which is a contradiction. It follows that Q is not principal in K. The second case is analogous. □

We also get the following corollary:

Corollary 3.3.3. *Suppose $K = \mathbb{Q}(\sqrt{pq})$ with the same conditions as before. Then the following hold:*

(i) Assume $\left(\frac{p}{q}\right) = -1$. Then $\lambda = 0$, and $X_\infty \cong A_0 \cong C_2$.

(ii) Assume $\left(\frac{p}{q}\right) = 1$ and $\left(\frac{p}{q}\right)_4 = \left(\frac{q}{p}\right)_4 = -1$. Then $\lambda = 0$, and $X_\infty \cong A_0 \cong C_4$.

(iii) Assume $\left(\frac{p}{q}\right) = 1$ and $\left(\frac{p}{q}\right)_4 = \left(\frac{q}{p}\right)_4 = 1$. If the ideal above q in K is not principal, then $\lambda = 0$, and $X_\infty \cong A_0$. In particular, the result holds if $N(\varepsilon_{2D}) = -1$.

(iv) Assume $\left(\frac{p}{q}\right) = 1$, $\left(\frac{p}{q}\right)_4 = -\left(\frac{q}{p}\right)_4$ and $q \equiv 1 \mod 16$. If the ideal above q in K' is not principal, then $\lambda = 0$ and $X_\infty \cong A_1$. In particular, the result holds if $N(\varepsilon_{2D}) = -1$.

Proof. This follows from Lemma 3.3.1, Proposition 3.3.2, and Theorem 1.2.6. □

Since these conditions are rather complicated, we will present some examples at the end of this chapter. One of the cases from Theorem 1.2.6 in the previous corollary was excluded due to the following:

Proposition 3.3.4. *Assume $\left(\frac{p}{q}\right) = 1$ and $\left(\frac{p}{q}\right)_4 = \left(\frac{q}{p}\right)_4 = 1$. Then $N(\varepsilon_{2D}) = 1$ and the ideal above q is principal in K'.*

Proof. By Kaplan ([18], §4, Proposition B2), since $\left(\frac{2p}{q}\right)_4 \neq \left(\frac{q}{2p}\right)_4$, either q or $-q$ is a norm from K' to $\mathbb{Q}$. The principal genus contains both $[q, 0, -2p]$ and $[-q, 0, 2p]$, so exactly one of them is equivalent to the unit, by Kaplan's criterion on the 8-rank.

We conclude as before that the ideal over q in K' is principal. Thus $q = x^2 \cdot \varepsilon_{2D}^n$ for some n. Since $\sqrt{q} \notin K_1$, n must be odd, $K_1(\sqrt{\varepsilon_{2D}}) = K_1(\sqrt{q})$, and $N(\varepsilon_{2D}) = 1$. □

We mention some results and consequences in terms of fundamental units and class groups, as we did for the second case.

Corollary 3.3.5. *Suppose* $\left(\frac{p}{q}\right) = -1$. *Then the 2-class group* A_0' *of* K' *is isomorphic to* $C_2 \times C_2$. *Furthermore,* $\{\varepsilon_D, \varepsilon_{2D}, \varepsilon_2\}$ *is a fundamental system of units F.S.U. of* K_1.

Proof. By Kaplan ([18], §4, Proposition A_2), we have $N(\varepsilon_{2D}) = -1$, as only the unit and its inverse are in the principal genus. Thus, the 4-rank is 0 and $A_0' \cong C_2 \times C_2$, since it must be equal to its narrow class group.

From Theorem 2.2.1 and Corollary 3.3.3, we have $|A_1| = |A_0| = q(K_1) \cdot |A_0|$. Therefore, $q(K_1) = 1$, and the fundamental system is the one indicated. □

Remark. In particular, since the norm of every unit is -1, we must have $\sqrt{\varepsilon_D \varepsilon_{2D} \varepsilon_2} \notin K_1$, and the traces mentioned in Example 3.1.3 are not squares in K_1.

Corollary 3.3.6. *Assume* $\left(\frac{p}{q}\right) = 1$. *Suppose we are in one of the following cases:*

(i) $\left(\frac{p}{q}\right)_4 = \left(\frac{q}{p}\right)_4 = -1$.

(ii) $\left(\frac{p}{q}\right)_4 = \left(\frac{q}{p}\right)_4 = 1$, *and the ideal above* q *in* K *is not principal.*

Then the 2-class group A_0' *of* K' *is isomorphic to* $C_2 \times C_2$ *and the norm of the fundamental unit* ε_{2D} *is* 1. *Furthermore,* $\{\varepsilon_D, \varepsilon_{2D}, \varepsilon_2\}$ *is a F.S.U. of* K_1. *In the second case, if the ideal above* q *in* K *is principal, then* $\{\sqrt{\varepsilon_D \varepsilon_{2D}}, \varepsilon_{2D}, \varepsilon_2\}$ *is a F.S.U. of* K_1.

Proof. From the Kubota-Kuroda formula we have

$$|A_1| = \frac{q(K_1) \cdot |A_0| \cdot |A_0'|}{4}.$$

From Corollary 3.3.3, $|A_1| = |A_0|$, and we have $q(K_1) \cdot |A_0'| = 4$. Thus, $|A_0'| \leq 4$. Furthermore, the 2-rank of this group is 2, from where it follows that $A_0' \cong C_2 \times C_2$, $q(K_1) = 1$, and the fundamental system is the one stated.

The Rèdei-Reichardt matrix for K' is

$$\begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Hence, the 4-rank of the narrow class group of K' is $3-1-1=1$. Since the narrow class number differs from the strict class number, the fundamental unit must have norm equal to 1.

Finally, if the ideal above q is principal in K, it follows that $K_1(\sqrt{\varepsilon_D}) = K_1(\sqrt{q}) = K_1(\sqrt{\varepsilon_{2D}})$ (proposition 3.3.4), and $\sqrt{\varepsilon_D\varepsilon_{2D}} \in K_1$. □

For the last case in Lemma 3.3.1, we have the following:

Proposition 3.3.7. *Suppose* $\left(\frac{p}{q}\right) = 1$ *and* $\left(\frac{p}{q}\right)_4 = -\left(\frac{q}{p}\right)_4$. *Then the ideal over* q *is not principal in* K' *if and only if* $N(\varepsilon_{2D}) = -1$.

Proof. One of the implications was already discussed in proposition 3.3.2. Assume that the ideal over q is not principal in K'. From Kaplan ([18], Proposition B_2), the forms in the principal genus are $f = [1, 0, -pq]$, $\overline{f} = [-1, 0, pq]$, $h = [q, 0, -2p]$ and $\overline{h} = [-q, 0, 2p]$. We cannot have f equivalent to h or $\overline{h}$, otherwise q would be principal in K'. Therefore, f is equivalent to $\overline{f}$ and f represents -1, which completes the result. □

Lemma 3.3.8. *Suppose* $\left(\frac{p}{q}\right) = 1$ *and* $\left(\frac{p}{q}\right)_4 = -\left(\frac{q}{p}\right)_4$. *If* $q \equiv 1 \mod 16$, *then the following statements hold:*

(i) If $N(\varepsilon_{2D}) = -1$*, the fundamental system of units of* K_1 *is* $\{\varepsilon_D, \varepsilon_{2D}, \varepsilon_2\}$ *and we get* $|A_1| = \frac{1}{2} \cdot |A_0'|$*. Moreover, if* $\left(\frac{2p}{q}\right)_4 = -1$*, then* $N(\varepsilon_{2D}) = -1$ *and* $|A_1| = 4$*.*

(ii) If $N(\varepsilon_{2D}) = 1$*, then* $\{\sqrt{\varepsilon_D \varepsilon_{2D}}, \varepsilon_D, \varepsilon_2\}$ *is a F.S.U. of* K_1*. Hence,* $q(K_1) = 2$ *in this case.*

Proof. For the field K, the norm of ε_D is 1 and one of the ideals above p or q in K is principal ([29],[17]). Thus, we have $K_1(\sqrt{p}) = K_1(\sqrt{q}) = K(\sqrt{\varepsilon_D})$. In particular, $\sqrt{\varepsilon_D} \notin K_1$.

If $N(\varepsilon_{2D}) = -1$, the only possible system is $\{\varepsilon_D, \varepsilon_{2D}, \varepsilon_2\}$.. Therefore $q(K_1) = 1$, and since $|A_0| = 2$, we get

$$|A_1| = \frac{1}{2} \cdot |A_0'|.$$

In the case when $\left(\frac{2p}{q}\right)_4 = -1$, due to ([18], §4, Proposition A_2), the 8-rank of the narrow class group of K' is 0 and $N(\varepsilon_{2D}) = -1$. Since the 4-rank of the narrow class group is 1 and the 2-rank is 2, we have $A_0' \cong C_4 \times C_2$.

Finally, if $N(\varepsilon_{2D}) = 1$ we must have $K_1(\sqrt{\varepsilon_{2D}}) = K_1(\sqrt{q}) = K_1(\sqrt{\varepsilon_D})$ due to Proposition 3.3.7. □

The complexity of the cases that are left is similar to what was discussed during the second case. We prove a result similar to Lemma 3.2.7, that doesn't need any extra conditions on the quadratic or biquadratic symbols, as it will be helpful for our analysis in the next chapter:

Lemma 3.3.9. *Suppose* $p \equiv 5 \mod 8$ *and* $q \equiv 1 \mod 8$ *with* $\left(\frac{2}{q}\right)_4 \neq (-1)^{\frac{q-1}{8}}$*. Then the 2-class group of* $K_1' = \mathbb{Q}\left(\sqrt{(2+\sqrt{2})pq}\right)$ *is isomorphic to* $C_2 \times C_2$*. In particular,* $|A_1'| = 4$*.*

Proof. We first show that the 2-rank of A_1' is 2. Consider the extension $K_1'/\mathbb{Q}_1$. Since there

are 4 ramifying primes in this extension (2 over q, 1 over p and 1 over 2), we have:

$$r_2(A_1') = 3 - e(K_1'/\mathbb{Q}_1)$$

where $e(K_1'/\mathbb{Q}_1)$ is the unit index, as expressed in Theorem 2.3.6.

Since the extension $K_1'(\sqrt{p}, \sqrt{q})$ is unramified and biquadratic over K_1', it follows that the 2-rank of the class group is at least 2.

If $\mathcal{L}$ is not a 2-adic prime of $\mathbb{Q}_1$, then the extension $\mathbb{Q}_2/\mathbb{Q}_1$ is unramified at $\mathcal{L}$. Since $\mathbb{Q}_2 = \mathbb{Q}_1(\varepsilon_2\sqrt{2})$, we have

$$\left(\frac{\varepsilon_2, \varepsilon_2\sqrt{2}}{L}\right) = 1.$$

Let $\mathcal{Q}$ be an ideal over q in Q_2. Then as discussed in [3],

$$\left(\frac{\varepsilon_2, q}{\mathcal{Q}}\right) = -1,$$

since

$$\left(\frac{\varepsilon_2, q}{\mathcal{Q}}\right) = \left(\frac{2}{q}\right)_4 \cdot \left(\frac{q}{2}\right)_4.$$

In particular

$$\left(\frac{\varepsilon_2, pq\varepsilon_2\sqrt{2}}{\mathcal{Q}}\right) = -1$$

Thus, we know that ε_2 is not a norm from K_1'. It follows that $e(K_1'/\mathbb{Q}_1) = 1$ and the 2-rank of A_1' is exactly 2.

From here the proof is the same as in Lemma 3.2.7, by simply considering the intermediate

fields of the extension $M = K_1'(\sqrt{p}, \sqrt{q}) = Q(\sqrt{2+\sqrt{2}}, \sqrt{p}, \sqrt{q})$ over K_1'.

$$M_1 = \mathbb{Q}(\sqrt{2+\sqrt{2}}, \sqrt{pq}) = K_2$$
$$M_2 = \mathbb{Q}(\sqrt{(2+\sqrt{2})p}, \sqrt{q})$$
$$M_3 = \mathbb{Q}(\sqrt{(2+\sqrt{2})q}, \sqrt{p})$$

Repeating the same argument, M is the $2-$class field of K_1' and $A_1' \cong C_2 \times C_2$. □

We end this section with some examples:

Example 3.3.10. These lists were obtained by using the software Mathematica and transforming the biquadratic conditions into modular conditions. Since it will be enough to illustrate the different cases, we assume that $p = 5$ and provide some lists of the first primes q satisfying one of the conditions in Corollary 3.3.3. We also give examples of the behavior in the fourth case when $p \equiv 9 \mod 16$ in the next section.

p	q	Modulo 16
5	17	1
5	97	1
5	433	1
5	673	1
5	73	9
5	233	9
5	617	9
5	937	9

Table 3.7: Examples of third case with $\left(\frac{p}{q}\right) = -1$

p	q	Modulo 16
5	769	1
5	1009	1
5	1409	1
5	3169	1
5	89	9
5	1049	9
5	2089	9
5	3049	9

Table 3.8: Condition: $\left(\frac{p}{q}\right)_4 = \left(\frac{q}{p}\right)_4 = -1$

p	q	Modulo 16
5	2081	1
5	4561	1
5	6961	1
5	12401	1
5	11161	9
5	17801	9
5	17881	9
5	18121	9

Table 3.9: Condition: $\left(\frac{p}{q}\right)_4 = \left(\frac{q}{p}\right)_4 = 1$, with $N(\varepsilon_D) = -1$

p	q
5	449
5	929
5	1489
5	2609

Table 3.10: Condition: $\left(\frac{p}{q}\right)_4 = -\left(\frac{q}{p}\right)_4 = -1$, $N(\varepsilon_{2D}) = -1$, and $q \equiv 1 \mod 16$

Chapter 4

Future explorations

We start this chapter with an analysis of the second and third cases of Proposition 3.1.2, whenever $N(\varepsilon_D) = -1$, as it will give us some new ideas on how to deal with the cases from Theorem 2.3.9 that are left.

4.1 Trace condition [15], [32], [23], [4]

Let $D = pq$ with $p \equiv q \equiv 5 \mod 8$. Let $\varepsilon_D = x + y\sqrt{D}$, where x is even and y is odd. Since $x^2 + 1 = Dy^2$, we have a factorization $(x+i)(x-i) = Dy^2$ in the unique factorization domain $\mathbb{Z}[i]$. Both primes split in $\mathbb{Q}(i)$, therefore there exists primes π_1, π_2 of $\mathbb{Z}[i]$ such that $p = \pi_1\overline{\pi_1}$, $q = \pi_2\overline{\pi_2}$, where $\overline{\pi_j}$ denotes the complex conjugate.

The primes can be chosen to be primary, which means $\pi_1 \equiv \pi_2 \equiv 1 \mod (1+i)^3$, so that they are relatively prime to 2. Every element of $E(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$ is unique modulo π_j. Then for α not divisible by π_j, there is a unique unit $\left(\frac{a}{\pi_j}\right)_4$ such that

$$a^{(N(\pi_j)-1)/4} \equiv \left(\frac{a}{\pi_j}\right)_4 \mod \pi_j.$$

This is known as the biquadratic symbol for $\mathbb{Z}[i]$, and its square $\left(\frac{a}{\pi_j}\right)_2$ is the quadratic symbol. Most of the properties we will use are taken from ([23], Chapters 5 and 6).

The following calculations are taken from ([32],Theorem 1), and specifically from [4], where the authors study the case $\left(\frac{p}{q}\right) = -1$. They give a necessary and sufficient condition for whether $\sqrt{\varepsilon_D \varepsilon_{2D} \varepsilon_2} \in K_1$ or not.

Since $g.c.d.(x+i, x-i) \mid 2i$ and $\pi_j \mid (x+i)(x-i)$, it follows that π_j divides one of $x \pm i$. We could replace π_j by its conjugate if necessary and assume that π_j divides $x+i$. This choice turns out to be significant when $\left(\frac{p}{q}\right) = 1$. In any case, by unique factorization, we must have

$$x + i = u\pi_1\pi_2 y_1^2$$

for some unit $u \in E(\mathbb{Z}[i])$, and $y_1 \in \mathbb{Z}[i]$ such that $y_1\overline{y_1} = y$. Since x is even and y is odd, taking the equation modulo 2, it follows that $u \equiv i \mod 2$. Replacing y_1 by iy_1 if necessary, we can assume that $u = i$ and

$$\begin{cases} x + i = \ i \cdot \pi_1 \cdot \pi_2 \cdot y_1^2, \\ x - i = -i \cdot \overline{\pi_1} \cdot \overline{\pi_2} \cdot \overline{y_1}^2. \end{cases}$$

Let $z = (1+i)y_1\sqrt{\pi_1 \cdot \pi_2} + (1-i)\overline{y_1}\sqrt{\overline{\pi_1} \cdot \overline{\pi_2}}$. Then

$$z^2 = 2\varepsilon_D,$$

which implies

$$\sqrt{2\varepsilon_D \cdot \pi_1 \cdot \pi_2} \in \mathbb{Z}\left[i, \sqrt{D}\right].$$

We also have

$$\sqrt{2\varepsilon_2} = \sqrt{1+i} + \sqrt{1-i},$$

from where it follows that $\sqrt{2\varepsilon_2 \cdot (1+i)} \in \mathbb{Z}\left[i, \sqrt{2}\right]$.

Let $\varepsilon_{2D} = r + s\sqrt{\varepsilon_{2D}}$. Then $(r+1)(r-1) = 2Ds^2$. Since $(1+i)(1-i) = 2$, one of the following equations holds:

1. $$\begin{cases} r \pm i = u \cdot (1-i) \cdot \pi_1 \cdot \pi_2 \cdot s_1^2, \\ r \mp i = \overline{u} \cdot (1+i) \cdot \overline{\pi_1} \cdot \overline{\pi_2} \cdot \overline{s_1}^2. \end{cases}$$

2. $$\begin{cases} r \pm i = u \cdot (1-i) \cdot \pi_1 \cdot \overline{\pi_2} \cdot s_1^2, \\ r \mp i = \overline{u} \cdot (1+i) \cdot \overline{\pi_1} \cdot \pi_2 \cdot \overline{s_1}^2. \end{cases}$$

where $u \in E(\mathbb{Z}[i])$ and $s = s_1\overline{s_1}$.

In the first case,

$$\sqrt{2^k \varepsilon_{2D} \cdot (1+i) \cdot \pi_1 \cdot \pi_2} \in \mathbb{Z}\left[i, \sqrt{2D}\right],$$

whereas in the second case, we have

$$\sqrt{2^k \varepsilon_{2D} \cdot (1+i) \cdot \pi_1 \cdot \overline{\pi_2}} \in \mathbb{Z}\left[i, \sqrt{2D}\right].$$

Multiplying the equalities for $\varepsilon_D, \varepsilon_{2D}, \varepsilon_2$, we can see that $\sqrt{\varepsilon_D \varepsilon_{2D} \varepsilon_2} \in K_1(i)$ only in the first equation, since $\sqrt{\pi_2 \overline{\pi_2}} = \sqrt{p} \notin K_1(i)$.

The following necessary and sufficient condition is given without proof in [4]:

$$\left(\frac{\pi_2}{\pi_1}\right)_2 \left(\frac{1+i}{\pi_1\pi_2}\right)_2 = -1.$$

We derive it in a similar way as before. First, from [23], we have

$$\left(\frac{i}{\pi_1}\right)_2 = (-1)^{(p-1)/2} = -1,$$

since $p \equiv 5 \mod 8$. The same result follows for π_2. Following [32], the equation $x + i = i \cdot \pi_1 \cdot \pi_2 \cdot y_1^2$ implies that

$$2 = \pi_1 \cdot \pi_2 \cdot y_1^2 + \overline{\pi_1} \cdot \overline{\pi_2} \cdot \overline{y_1}^2.$$

Therefore,

$$\left(\frac{2}{\pi_1}\right)_2 = \left(\frac{\overline{\pi_1} \cdot \overline{\pi_2}}{\pi_1}\right)_2.$$

Suppose first that $u = 1$, we have

$$\begin{cases} r \pm i = (1-i) \cdot \pi_1 \cdot \pi_2 \cdot y_1^2, \\ r \mp i = (1+i) \cdot \overline{\pi_1} \cdot \overline{\pi_2} \cdot \overline{y_1}^2, \end{cases}$$

Then

$$\left(\frac{(1+i) \cdot \overline{\pi_1} \cdot \overline{\pi_2}}{\pi_1}\right)_2 = \left(\frac{\pm 2i}{\pi_1}\right)_2,$$

which implies

$$\left(\frac{1+i}{\pi_1}\right)_2 = \left(\frac{i}{\pi_1}\right)_2 = -1.$$

Similarly, we get

$$\left(\frac{1+i}{\pi_2}\right)_2 = \left(\frac{i}{\pi_1}\right)_2 = -1.$$

In the second case, with $u = i$, we have

$$\begin{cases} r \pm i = i(1-i) \cdot \pi_1 \cdot \pi_2 \cdot y_1^2, \\ r \mp i = -i(1+i) \cdot \overline{\pi_1} \cdot \overline{\pi_2} \cdot \overline{y_1}^2, \end{cases}$$

then

$$\left(\frac{-i \cdot (1+i) \cdot \overline{\pi_1} \cdot \overline{\pi_2}}{\pi_1}\right)_2 = \left(\frac{\pm 2i}{\pi_1}\right)_2,$$

which implies

$$\left(\frac{1+i}{\pi_1}\right)_2 = 1.$$

Again, we also have

$$\left(\frac{1+i}{\pi_2}\right)_2 = 1.$$

In both cases,

$$\left(\frac{1+i}{\pi_1}\right)_2 = \left(\frac{1+i}{\pi_2}\right)_2.$$

In the case

$$\begin{cases} r \pm i = u \cdot (1-i) \cdot \pi_1 \cdot \overline{\pi_2} \cdot y_1^2, \\ r \mp i = \overline{u} \cdot (1+i) \cdot \overline{\pi_1} \cdot \pi_2 \cdot \overline{y_1}^2, \end{cases}$$

we have

$$\left(\frac{1+i}{\pi_1}\right)_2 = \left(\frac{1+i}{\overline{\pi_2}}\right)_2$$

instead. Following ([23], Proposition 6.8), we have the equation

$$\left(\frac{1+i}{\pi_2}\right)_2 \cdot \left(\frac{1+i}{\overline{\pi_2}}\right)_2 = \left(\frac{i}{\pi_2}\right)_2 = -1,$$

which implies

$$\left(\frac{1+i}{\pi_1}\right)_2 \neq \left(\frac{i+1}{\pi_2}\right)_2.$$

Therefore, a necessary and sufficient condition for $\sqrt{\varepsilon_D \varepsilon_{2D} \varepsilon_2} \in K_1$ is

$$\left(\frac{1+i}{\pi_1}\right)_2 = \left(\frac{i+1}{\pi_2}\right)_2.$$

In [4], the authors prove that if $\left(\frac{p}{q}\right) = -1$, the following equation is independent of the choice of the factorization:

$$\left(\frac{pq}{2}\right)_4 \left(\frac{2p}{q}\right)_4 \left(\frac{2q}{p}\right)_4 = \left(\frac{\pi_2}{\pi_1}\right)_2 \left(\frac{1+i}{\pi_1}\right)_2 \left(\frac{i+1}{\pi_2}\right)_2.$$

Also worth mentioning, the following equality holds:

$$\left(\frac{2}{\pi_1\pi_2}\right)_4 \cdot \left(\frac{\pi_2}{\pi_1}\right)_2 = \left(\frac{2p}{q}\right)_4 \cdot \left(\frac{2q}{p}\right)_4.$$

From ([32], Corollary 2), the symbol $\left(\frac{\pi_2}{\pi_1}\right)_2$ is equal to -1 whenever $\left(\frac{p}{q}\right) = -1$, Then

$$\sqrt{\varepsilon_D \varepsilon_{2D} \varepsilon_2} \in K_1 \iff \left(\frac{pq}{2}\right)_4 \left(\frac{2p}{q}\right)_4 \left(\frac{2q}{p}\right)_4 = -1.$$

for this case. This is proved in [4]. This condition appears for the first time in ([17], Proposition B_1'), and it is equivalent to the 2-part of $Cl^+(\mathbb{Q}(\sqrt{-pq}))$ being equal to $C_2 \times C_4$.

We now assume that $\left(\frac{p}{q}\right) = 1$ with $\left(\frac{p}{q}\right)_4 = \left(\frac{q}{p}\right)_4 = -1$. We need to understand when the condition $\left(\frac{1+i}{\pi_1}\right)_2 \left(\frac{i+1}{\pi_2}\right)_2 = 1$ happens. The symbols are dependent on the choice of factorization in this case, since

$$\left(\frac{1+i}{\pi_1}\right)_2 = \left(\frac{2}{a+b}\right),$$

$$\left(\frac{1+i}{\pi_2}\right)_2 = \left(\frac{2}{c+d}\right),$$

where $\pi_1 = a + bi$, $\pi_2 = c + di$.

Since $2 = i^3 \cdot (1+i)^2$, it follows that

$$\left(\frac{2}{\pi_1\pi_2}\right)_4 = \left(\frac{i}{\pi_1\pi_2}\right)_4 \cdot \left(\frac{1+i}{\pi_1\pi_2}\right)_2.$$

It is easy to see that

$$\left(\frac{i}{\pi_1\pi_2}\right)_4 = \left(\frac{pq}{2}\right)_4 = (-1)^{\frac{pq-1}{8}},$$

so that the condition transforms into

$$\left(\frac{2}{\pi_1\pi_2}\right)_4 \cdot (-1)^{\frac{pq-1}{8}} = 1.$$

Likewise, if $\left(\frac{p}{q}\right) = 1$ with $\left(\frac{p}{q}\right)_4 = \left(\frac{q}{p}\right)_4 = 1$ and $N(\varepsilon_D) = 1$, we have the same conditions. It is worth noting that the condition $\left(\frac{p}{q}\right)_4 = \left(\frac{q}{p}\right)_4$ appears in ([18], Proposition B_4'), and it is equivalent again the 2-part of $Cl^+(\mathbb{Q}(\sqrt{-pq}))$ being equal to $C_2 \times C_4$.

In these cases, we could not find a way to express $\left(\frac{2}{\pi_1\pi_2}\right)_4$ in terms of p and q, since both symbols $\left(\frac{2p}{q}\right)_4, \left(\frac{2q}{p}\right)_4$ are not well defined. Still, we show how to calculate this condition using this equivalence:

Example 4.1.1. Let $p = 5 = (-1+2i)(-1-2i)$ and $q = 29 = (-5+2i)(-5-2i)$, where all the elements $(-1 \pm 2i), (-5 \pm 2i)$ are primary. In this case, $\varepsilon_D = 12 + \sqrt{D}$. Only one of

$$\frac{12+i}{(-1 \pm 2i) \cdot (-5 \pm 2i))}$$

is an element of $\mathbb{Z}[i]$. In this case, $\pi_1 = -1+2i$ and $\pi_2 = -5+2i$, so that

$$1 = \left(\frac{1+i}{\pi_1}\right)_2 \neq \left(\frac{1+i}{\pi_2}\right)_2 = \left(\frac{2}{-3}\right) = -1$$

and $\sqrt{\varepsilon_D \varepsilon_{2D} \varepsilon_2} \notin K_1$, which is the case since $|A_1| = |A_0|$ according to PARI. We provide a list of the first examples with the corresponding symbols and primes in $\mathbb{Z}[i]$:

p	q	π_1	π_2	$\left(\frac{1+i}{\pi_1}\right)_2$	$\left(\frac{1+i}{\pi_2}\right)_2$	Is $\sqrt{\varepsilon_D \varepsilon_{2D} \varepsilon_2} \in K_1$?
5	29	$-1+2i$	$-5+2i$	1	-1	No
5	229	$-1+2i$	$15-2i$	1	-1	No
5	349	$-1+2i$	$-5+18i$	1	-1	No
5	509	$-1+2i$	$-5+22i$	1	1	Yes
5	709	$-1+2i$	$15-2i$	1	1	Yes
5	1109	$-1+2i$	$-25+22i$	1	-1	No
5	1229	$-1+2i$	$35-2i$	1	1	No
5	1549	$-1-2i$	$35+18i$	-1	-1	Yes
5	1669	$-1-2i$	$15+38i$	-1	-1	Yes
5	1709	$-1+2i$	$35+22i$	1	1	Yes
5	1789	$-1+2i$	$-5-42i$	1	1	Yes
5	2029	$-1+2i$	$-45+2i$	1	-1	No

Table 4.1: Trace condition for $\left(\frac{p}{q}\right)_4 = \left(\frac{q}{p}\right)_4 = -1$.

Since we need to calculate the fundamental unit to determine the correct primes, this

condition is as complex as the trace condition in the previous chapter. The one obtained in [4] for the case $\left(\frac{p}{q}\right) = -1$ is a lot easier, since it depends only on p and q:

p	q	$\left(\frac{pq}{2}\right)_4$	$\left(\frac{2p}{q}\right)_4$	$\left(\frac{2q}{p}\right)_4$	Is $\sqrt{\varepsilon_D \varepsilon_{2D} \varepsilon_2} \in K_1$?
5	29	1	−1	1	Yes
5	37	−1	1	−1	No
5	53	−1	1	1	Yes
5	157	1	−1	−1	No
5	173	1	1	1	No
5	197	1	−1	−1	No
5	277	−1	1	−1	No
5	293	−1	−1	1	No
5	317	1	1	−1	Yes

Table 4.2: Trace condition for $\left(\frac{p}{q}\right) = -1$.

4.2 Case $q \equiv 9 \mod 16$

Out of all the possible cases from Theorem 2.3.9 that are left, the one from the second case where $\left(\frac{p}{q}\right) = 1$, $\left(\frac{p}{q}\right)_4 = -\left(\frac{q}{p}\right)_4$, $q \equiv 9 \pmod{16}$, and $N(\varepsilon_{2D}) = -1$ seems to be the one within reach with the techniques used in this dissertation. We were not able to find an example where $X_\infty \ncong A_1$.

p	q	X_∞
5	6569	A_1
5	7129	A_1
5	15289	A_1
5	16249	A_1
5	19289	A_1
5	25609	A_1
5	26249	A_1
5	28409	A_1
5	32089	A_1
5	48649	A_1
5	57689	A_1
5	64489	A_1
5	65929	A_1
5	77689	A_1

Table 4.3: Condition: $\left(\frac{p}{q}\right)_4 = -\left(\frac{q}{p}\right)_4 = -1$, $N(\varepsilon_{2D}) = -1$, and $q \equiv 9 \mod 16$

We conjecture that the following statement is true:

Conjecture 4.2.1. *Let $K = \mathbb{Q}(\sqrt{D})$, where $D = pq$ with $p \equiv 5 \pmod 8$, $q \equiv 1 \pmod 8$, and $\left(\frac{2}{q}\right)_4 \neq (-1)^{\frac{q-1}{8}}$. Assume that $\left(\frac{p}{q}\right) = 1$, $\left(\frac{p}{q}\right)_4 = -\left(\frac{q}{p}\right)_4$, $q \equiv 9 \mod 16$, and $N(\varepsilon_{2D}) = -1$. Then $X_\infty \cong A_1$.*

A similar case is treated in [11] and [20], with different modular conditions over the prime p. The same techniques cannot be applied to get a concrete answer in our case, but some properties about the prime q might be useful. We expand on some of the ideas in these papers and explain the main differences with the current case.

The prime q splits in $\mathbb{Q}_1$ as $q = q_1 q_2$, where $q_1 \equiv r + s\sqrt{2}$ and $q_1 \equiv r + s\sqrt{2}$ for some positive integers r, s. From ([20], Lemma 2.4), we have

$$q_1 \equiv q_2 \equiv 3 \text{ or } (1 + 2\sqrt{2}) \mod 4\sqrt{2}.$$

The main difference is that

$$pq_i \equiv -1 \text{ or } -(3+2\sqrt{2}) = -(1+\sqrt{2})^2 \mod 4\sqrt{2},$$

and the extension $K_1(\sqrt{q_i})$ is ramified at the primes above 2 ([31], Exercise 9.3). This can also be drawn from A_1 being cyclic, but we wanted to emphasize why the same ideas fail within this context.

Following the notation in Theorem 2.1.1, let B_n' denote the subgroup of $B_n = A_n^{\mathrm{Gal}(K_n/K)}$ consisting of ideal classes containing an ideal invariant under the action of $\mathrm{Gal}(K_n/K)$. From Theorem 2.3.4 and Remark 2.3.5,

$$|B_n'| = \frac{|A(K)|}{\left[E(K) : N_{K_n/K}(E(K_n)\right]} = \frac{2}{\left[E(K) : N_{K_n/K}(E(K_n))\right]}.$$

The F.S.U. of K_1 is $\{\varepsilon_D, \varepsilon_{2D}, \varepsilon_2\}$, due to a similar argument as in Lemma 3.3.8. In particular, $\varepsilon_D \notin N_{K_1/K}(E(K_1))$. Moreover, since $N_{K_n/K}(u) = N_{K_1/K}(N_{K_n/K_1}(u))$, it follows that $\varepsilon_D \notin N_{K_n/K}(E(K_n))$ and $|B_n'| = 1$ for every n.

If $\mathcal{L}_n$ is the ideal in K_n above 2, since the class of $\mathcal{L}_n$ is in B_n' if follows that this ideal is always principal, similar to what is concluded in ([20], Lemma 2.4). The author calculates A_1 and uses circular units to estimate the order of the groups A_1' and A_2. Even though we know that $|A_1'| = 4$ in our case (Lemma 3.3.9), the complicated nature of A_0' makes it difficult to arrive to the same conclusions since all that is known is that this group is of the form $C_{2^m} \times C_2$ with $m \geq 3$ ([18], Proposition B_2).

We want to take a similar approach to Theorem 3.2.9, given that both Lemma 3.2.8 and Lemma 3.3.9 hold for this case. Similar to what we did in the previous section with the field $\mathbb{Q}(i)$, we would like to use the factorization in $\mathbb{Z}\left[\sqrt{2}\right]$ and the quadratic symbol of $\mathbb{Q}_1$ ([23],

Chapter 4) to draw some conclusions.

There is a F.S.U. of K_1' of the form $\{v_1, v_2, \varepsilon_2\}$, where v_1 has norm 1 in $\mathbb{Q}_1$ and v_2 has norm -1. The F.S.U. of $\mathbb{Q}_2$ is the system $\{w_1, w_2, \varepsilon_2\}$ mentioned before, and the one for K_1 is $\{\varepsilon_D, \varepsilon_{2D}, \varepsilon_2\}$. Then any square in $E(K_2)$ is necessarily of the form

$$u^2 = (\varepsilon_{2D} v_2 w_2)^a \cdot \varepsilon_D^b \cdot \varepsilon_2^c \cdot v_1^d,$$

since ε_D has norm 1 and ε_{2D} has norm -1. As before, it is enough to show that either ε_D or ε_{2D} is not a norm from K_2. If ε_D is a norm, then either $\varepsilon_D v_1$ or $\varepsilon_D v_1 \varepsilon_2$ is a square in K_2.

Suppose we can write $v_1 = r + s\sqrt{2+\sqrt{2}} \cdot \sqrt{D}$, where $r, s \in \mathbb{Z}\left[\sqrt{2}\right]$. Then

$$(r+1)(r-1) = p \cdot q \cdot (2+\sqrt{2}) \cdot s^2.$$

If $\varepsilon_D v_1$ is a square, since $K_2(\sqrt{\varepsilon_D}) = K_2(\sqrt{p})$, by unique factorization we must have

$$\begin{cases} r \pm 1 = u_1 \cdot d_1 \cdot s_1^2 \\ r \mp 1 = u_1^{-1} \cdot (2+\sqrt{2}) \cdot d_2 \cdot s_2^2 \end{cases}$$

where $d_1 = p$ or $d_1 = q$, $s_1 s_2 = s$, and $u_1 \in E(\mathbb{Q}_1)$.

This is a rather promising path. For instance, if $d_1 = p$ and $u_1 = 1$, then

$$\left(\frac{(2+\sqrt{2})q}{p\mathbb{Z}[\sqrt{2}]}\right) = \left(\frac{\pm 2}{p\mathbb{Z}[\sqrt{2}}\right) = 1,$$

but

$$\left(\frac{2+\sqrt{2}}{p\mathbb{Z}[\sqrt{2}]}\right) = -1,$$

giving us a contradiction, since $\left(\frac{q}{p}\right) = 1$.

The main issue is that the prime q splits in $\mathbb{Q}_1$ and the symbol depends on the choice of the divisor, as seen in the previous chapter. If $q = q_1 q_2$ in $\mathbb{Q}_1$, we believe that $K_2(\sqrt{v_1}) = K_2(\sqrt{q_j})$ for some $j \in \{1, 2\}$, but certain problems arise in the argument. For instance, what happens if $u_1 = \varepsilon_2$, or why is it not possible for $\varepsilon_D v_1 \varepsilon_2$ to be a square in K_2? If one of these elements is a square, is it possible for $\varepsilon_{2D} v_2 w_2$ to be a square? If we have to deal with this, it becomes more complicated, since we would have to work on $\mathbb{Z}[\sqrt{2}, i]$ instead, where the quadratic symbols are more difficult to manage.

It might be possible to use these ideas to formulate a valid argument using the quadratic symbols, by proving that the extension $K_2(\sqrt{v_1})$ is ramified, or using the conditions on the prime q discussed at the beginning of this section, but at the moment we have not been able to do so. We hope in the future to be able to use the quadratic symbols and their properties to conclude the result, and that the study of the biquadratic extensions K_{n+2}/K_n and its intermediate subfields will bring forth a better understanding of the cyclotomic $\mathbb{Z}_p$-extension and towers of p-groups in general.

Bibliography

[1] Abdelmalek Azizi, *Sur la capitulation des 2-classes d'idéaux de* $\mathbb{Q}(\sqrt{2pq}, i)$ *où* $p \equiv -q \equiv 1 \mod 4$, Acta Arith. **94** (2000), no. 4, 383–399.

[2] Abdelmalek Azizi and Ali Mouhib, *Le 2-rang du groupe de classes de certains corps biquadratiques et applications*, Int. J. Math. **15** (2004), no. 2, 169–182.

[3] Abdelmalek Azizi and Ali Mouhib, *Sur le rang du 2-groupe de classes de* $\mathbb{Q}(\sqrt{m}, \sqrt{d})$ *où* $m = 2$ *ou un premier* $p \equiv 1 \pmod 4$, Trans. Amer. Math. Soc. **353** (2001), 2741–2752.

[4] Abdelmalek Azizi, Abdelkader Zekhnini, and Mohammed Taous, *Sur l'équation* $X^2 - \varepsilon_2 \varepsilon_{p_1p_2} \varepsilon_{2p_1p_2} = 0$. Conference: Rencontre des Algébristes à Rabat (RAR'2013), arXiv preprint arXiv:1504.04892 (2015).

[5] Elliot Benjamin, *On the 2-class field tower conjecture for imaginary quadratic number fields with 2-class group of rank 4*, J. of Number Theory **154** (2015), 118–143.

[6] J. W. S. Cassels and Albrecht Fröhlich, *Algebraic number theory*, Academic Press, London; Thompson Book Co., Inc., Washington, D.C, 1967.

[7] Claude Chevalley, *Sur la théorie du corps de classes dans les corps finis et les corps locaux (Thése)*, J. Fac. Sci. Tokyo. **2** (1933), 365–476.

[8] David A. Cox, *Primes of the form* $x^2 + ny^2$, 2nd ed., John Wiley & Sons,Inc., New York, 1989.

[9] Bruce Ferrero and Lawrence C. Washington, *The Iwasawa invariant* μ_p *vanishes for abelian number fields*, Ann. of Math. **109** (1979), 377–395.

[10] Takashi Fukuda, *Remarks on* $\mathbb{Z}_p$*-extensions of number fields*, Proc. Japan Acad. Ser. A, Math. Sci **70** (1994), no. 8, 264–266.

[11] Takashi Fukuda and Keiichi Komatsu, *On the Iwasawa lambda-Invariant of the Cyclotomic* $\mathbb{Z}_2$*-Extension of a Real Quadratic Field*, Tokyo J. Math. **28** (2005), no. 1, 259–264.

[12] Carl Gauss, *Disquisitiones Arithmeticae*, 1801.

[13] Ralph Greenberg, *On the Iwasawa invariants of totally real number fields*, Am. J. Math. **98** (1976), no. 1, 263–284.

[14] Laxmi Hariharan and Anupam Saikia, $\mathbb{Z}_2$*-extension of real quadratic fields with* $\mathbb{Z}/2\mathbb{Z}$ *as 2-class group at each layer*, (2024), arXiv: 2310.03543.

[15] Kenneth Ireland and Michael Rosen, *A classical introduction to modern number theory*, 2nd ed., Graduate Texts In Mathematics., 84, Springer, New York, 1990.

[16] Kenkichi Iwasawa, *On $\mathbb{Z}_l$-extensions of algebraic number fields*, Ann. of Math. **98** (1973), 246–326.

[17] Pierre Kaplan, *Divisibilité par 8 du nombre des classes des corps quadratiques dont le 2-groupe des classes est cyclique, et réciprocité biquadratique*, J. Math. Soc. Japan **25** (1973), 596–608.

[18] Pierre Kaplan, *Sur le 2-groupe des classes d'idéaux des corps quadratiques.* J. Reine Angew. Math. **283-284** (1976), 313–363.

[19] Tomio Kubota, *Über den bizyklischen biquadratischen Zahlkörper*, Nagoya Math. J. **10** (1956), 65–85.

[20] Naoki Kumakawa, *On the Iwasawa λ-invariant of the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}(\sqrt{pq})$ and the 2-part of the class number of $\mathbb{Q}(\sqrt{pq}, \sqrt{2+\sqrt{2}})$*, Int. J. Number Theory **17** (2021), no. 4, 931–958.

[21] Sigekatu Kuroda, *Über den Dirichletschen Körper*, J. Fac. Sci. Imp. Univ. Tokyo. **4** (1943), 383–406.

[22] Franz Lemmermeyer, *Kuroda's class number formula*, Acta Arith. **66** (1994), no. 3, 245–260.

[23] Franz Lemmermeyer, *Reciprocity laws: from Euler to Eisenstein*, Springer Monographs in Mathematics, Springer, Berlin, 2000.

[24] Yasushi Mizusawa, *A Study of Iwasawa Theory on Class Field Towers*, PhD thesis, Waseda University, (2004).

[25] Ali Mouhib and Abbas Movahhedi, *Cyclicity of the unramified Iwasawa module*, Manuscr. Math. **135** (2011), 91–106.

[26] Jürgen Neukirch, *Algebraic number theory*, Grundlehren der mathematischen Wissenschaften, Springer Berlin, 1999.

[27] Manabu Ozaki and Hisao Taya, *On the Iwasawa λ_2-invariants of certain families of real quadratic fields*, Manuscr. Math. **94** (1997), no. 4, 437–444.

[28] László Rédei and Hans Reichardt, *Die Anzahl der durch vier teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers.* J. Reine Angew. Math. **170** (1934), 69–74.

[29] Arnold Scholz, *Über die Lösbarkeit der Gleichung $t^2 - Du^2 = -4$*, Math. Z. **39** (1935), 95–111.

[30] Hideo Wada, *On the class number and the unit group of certain algebraic number fields*, J. Fac. Sci. Univ. Tokyo **13** (1966), 201–209.

[31] Lawrence C. Washington, *Introduction to cyclotomic fields*, 2nd ed., Graduate Texts In Mathematics., vol. 83, Springer-Verlag, New York, 1997.

[32] Kenneth S. Williams, *On the evaluation of $(\varepsilon_{q_1q_2}/p)$*, Rocky Mountain J. Math. **10** (1980), no. 3, 559–573.