A STUDY OF CLASS GROUPS OF NUMBER FIELDS IN CONNECTION WITH GREENBERG'S CONJECTURES

by

H LAXMI

DEPARTMENT OF MATHEMATICS
INDIAN INSTITUTE OF TECHNOLOGY GUWAHATI
GUWAHATI - 781039, INDIA

MARCH 2025

A study of class groups of number fields in connection with Greenberg's conjectures

by

H LAXMI

Roll No. 206123010

Department of Mathematics

under the supervision of

Dr. ANUPAM SAIKIA

Professor,

Department of Mathematics

submitted in fulfillment of the requirements of the degree of Doctor of Philosophy to the

Indian Institute of Technology Guwahati
Guwahati - 781039, India

March 2025

This work is dedicated

to

The pillars of my life:

Amma and Appa,

Chitha and Chithi

Certificate

This is to certify that the thesis entitled **"A study of class groups of number fields in connection with Greenberg's conjectures"** submitted by **Ms. H Laxmi** to the **Indian Institute of Technology Guwahati**, for the award of the Degree of **Doctor of Philosophy**, is a record of the original bona fide research work carried out by her under my guidance and supervision. The thesis has reached the standards fulfilling the requirements of the regulations relating to the degree.

The results contained in this thesis have not been submitted in part or full to any other university or institute for the award of any degree or diploma.

Date: 28 March, 2025

Guwahati, India

Dr. Anupam Saikia

Professor

Department of Mathematics

Indian Institute of Technology Guwahati

Acknowledgements

First and foremost, I would like to express sincere gratitude towards my supervisor, Prof. Anupam Saikia. I deeply appreciate his unwavering support in moments of both progress and setbacks throughout my Master's and doctoral journey. His enthusiasm, openness to discussions, and constant encouragement paved the way for me to express my ideas and thoughts with confidence. His eye for precision and perfection in mathematics has always inspired me to improve myself. His deep knowledge, with the aptitude for connecting multiple concepts, helped me gain new perspectives on the subject. I owe him a great deal for his patience and graciousness. I cannot thank him enough for making time to diligently review all my work and enhancing its quality with his valuable insights and feedback. He has exemplified a holistic approach towards academics and life, and I feel highly fortunate to have had such a supervisor.

I am grateful to the members of my doctoral committee – Prof. Rupam Barman, Prof. K. V. Krishna, and Dr. Vinay Wagh for their timely assessment of my work and constructive suggestions. I am thankful for the atmosphere of warmth and ease they provided in the entire course of PhD which helped me focus well on my research. From the bottom of my heart, I would also like to thank Dr. Sriparna Bandopadhyay, Dr. Anjan K. Chakrabarty, Prof. Sukanta Pati, Prof. Jiten C. Kalita, Dr. Sweta Tiwari, and Dr. Pratyoosh Kumar for boosting me to make more efforts to uplift myself as a student in mathematics. It's not just their unforgettable lessons, but also their welcoming nature with which they treated me.

I profoundly acknowledge the Indian Institute of Technology Guwahati for providing excellent facilities and resources for my research. The serenity of the institute campus will forever hold a special place in my heart. I sincerely thank the Ministry of Human Resources

and Development, Government of India for the financial assistance. I am grateful to all the technical and non-teaching staff of the Department of Mathematics of IITG, especially Mr. Jayanta Kalita, Mr. Pranpratim Borgohain, and Ms. Trishna Choudhury for their kindness and support in various ways.

It was a great experience working with my collaborator, Dr. Jaitra Chattopadhyay. His explanation skills and effective questioning taught me a lot as a new entrant into research. Next, my heartfelt appreciation goes to all my dear friends and research group members – Dr. Ajit Singh, Dr. Anwita Bhowmik, Deepa Antony, Sulakashna, Gurinder Singh, Ansh Agrawal, Alapan Ghosh, Sipra Maity, Manisha Bansal, Mandeep Singh, Jaspreet Kaur, Digvijay Singh Bisht, Vivek Sahu, Gaurav Kumar, Saurabh Bansal, Manali Sajjan, Sunil Kundu, Archita Sharma, and Sonakshi Aggarwal. They have played a major role in creating a healthy research environment and have backed me up numerous times. They have stood beside me through thick and thin and each of them has taught me something with their distinctive nature. I will always cherish and carry this spirit of camaraderie with me.

Most importantly, I am forever indebted to my family that has made me who I am today. No words can measure my gratitude and love towards my parents Mr. S. Hariharan and Mrs. S. Rajalakshmi, my uncle Mr. S. Ramakrishnan, my aunt Mrs. N. Vijayalakshmi, and my grandparents Late Shri. H. Subramoniam and Late Smt. S. Lakshmy for nurturing me. They are my greatest strength, who believed in me and helped me chase my dreams. They are the first ones who taught me - “Try and try till you succeed”. They have always been there to show me that the sky is the limit and have consistently motivated me to be a better person. I would also like to thank my family members Mrs S. Sankari, Mr. H. S. Gopalakrishnan, and my cousin S. Lakshmi for their constant support and wishes. My family members are my cheerleaders and well-wishers who have been nothing but loving and encouraging, and I could have never asked for more. I am eternally thankful for the life they have blessed me with.

Abstract

The class group is one of the most intriguing aspects of a number field. Although the finiteness of the class group is known, it is seldom trivial to precisely identify the structure of the class group. Instead of being dealt with altogether, it is fairly common to study the class group and the class number with respect to individual prime numbers. This inspires the question on the p-primary part of the class group for a prime p, and this thesis revolves around the same question asked for various families of number fields.

Firstly, we look into p-rational fields, a concept first introduced by Movaheddi. For a prime number p and a number field K, the p-rationality of K is based on a characteristic of the maximal p-ramified pro-p-extension of K. Greenberg proved that if K is a quadratic field, then the p-rationality for K boils down to non-divisibility of the class number of K by p and to the fundamental unit of K (if K is real). For any natural number m we discuss the existence of m-consecutive imaginary, and two consecutive real quadratic p-rational fields for infinitely many primes p. The motivation behind "consecutiveness" arises from Iizuka's conjecture. Given a prime number ℓ, Iizuka's conjecture asserts the existence of some $m+1$ number fields of the form $\mathbb{Q}(\sqrt{d}), \mathbb{Q}(\sqrt{d+1}), \ldots, \mathbb{Q}(\sqrt{d+m})$ whose class numbers are divisible by ℓ. On the similar lines, our work deals with non-divisibility of class numbers. We essentially construct quadratic fields whose class numbers are lesser than p, and use Serre's result to deal with the fundamental units of certain families of real quadratic fields.

Greenberg conjectured the vanishing of the Iwasawa invariants λ and μ for the cyclotomic $\mathbb{Z}_\ell$-extension of totally real number fields. The vanishing of μ and λ is equivalent to rank and order stability, respectively, of the ℓ-class groups of the intermediate fields present in a $\mathbb{Z}_\ell$-extension of a number field. The second topic that we address in this thesis

is broadly based on the Iwasawa module corresponding to the cyclotomic $\mathbb{Z}_2$-extension of real quadratic and biquadratic fields. The influence of the field extension on aspects like ideal factorization and units, in turn have an effect on the class groups. Such effects are best illustrated in genus formulae, Hilbert's theorem 94, and various kinds of class number formula, to name a few. We utilize all these theories to understand more about 2-class groups. In case of quadratic fields, the rank of the 2-class group is completely known, owing to genus theory. We also proceed a few steps further by studying rank of the 2-class groups of fields of degree 4 and even 8, mainly via genus formula and by examining the relative norms of units. Calculation of the order of the 2-class groups is a slightly more complex task and we accomplish this by identifying the action of Galois groups on the class groups by considering suitable extensions. We also closely observe the units of quadratic and biquadratic extensions to be able to apply results like Kuroda-Kubota's class number formula. We frequently appeal to key results from class field theory, Galois theory, and group theory to draw our conclusions.

Contents

Certificate i

Acknowledgements iii

Abstract v

Introduction 1

1 Preliminaries 9

1.1 Results from algebra and number theory 9

1.1.1 Profinite groups 10

1.1.2 Congruence and quadratic residues 12

1.2 Number fields 14

1.2.1 The class group 15

1.2.2 Ramification theory 16

1.3 Unramified extensions of number fields 20

1.3.1 The Hilbert and narrow Hilbert class fields 20

1.3.2 Genus field and the p-rank of class group 21

1.4 Class group as a Galois module 23

1.5 Homomorphisms between class groups 25

1.6 Reciprocity laws in number fields and the Hilbert symbol 27

1.7 Density 29
1.7.1 Analytic class number formula 31
1.7.2 Kuroda-Kubota's class number formula 31
1.8 $\mathbb{Z}_\ell$-extension 32
1.8.1 Cyclotomic $\mathbb{Z}_\ell$-extension 34
1.8.2 Nakayama's lemma and Fukuda's result on stability 34
1.9 Class field tower and Burnside's basis theorem 35

2 On the p-rationality of consecutive quadratic fields 37
2.1 Introduction 37
2.2 Criteria for p-rationality 39
2.3 Consecutive imaginary quadratic p-rational fields 40
2.3.1 Proof of Theorem 2.1.4 42
2.4 Consecutive real quadratic p-rational fields 43
2.4.1 Proof of Theorem 2.1.5 43
2.5 Square-free values of integral polynomials 45
2.6 Biquadratic and triquadratic p-rational fields 47

3 Structure of 2-class groups in the $\mathbb{Z}_2$-extensions of certain real quadratic fields 51
3.1 Introduction 51
3.2 Ramified primes and the 2-rank 54
3.2.1 Proof of Theorem 3.1.2 58
3.2.2 Proof of Theorem 3.1.4 60

4 Stability of 2-class groups in the $\mathbb{Z}_2$-extension of certain real quadratic fields 65
4.1 Introduction 65
4.2 The 2-class group of $\mathbb{Q}(\sqrt{p_1q_1q_2})$ and $\mathbb{Q}(\sqrt{2p_1q_1q_2})$ 67

4.3 2-class groups of the sub-extensions of K_∞/K . . . 70
4.4 The case of (5,3,3) . . . 72
4.4.1 Proof of Theorem 4.1.1 . . . 72
4.4.2 Proof of Theorem 4.1.3 . . . 73
4.5 The case of (5,7,3) . . . 77
4.5.1 Proof of Theorem 4.1.5 . . . 77

5 Study of Iwasawa module via a bounded quotient 79

5.1 Introduction . . . 79
5.2 Boundedness of $A'_\ell(F_n)$ and $A_\ell(F_n)^{\langle\tau_n\rangle}$ . . . 81
5.3 Extensions of $\mathbb{Q}_1$ based on factors of p in $\mathbb{Q}_1$ . . . 82
5.4 Structure of $A(K_n)$ . . . 83
5.5 Structure of $A'(K_n)$ . . . 87
5.5.1 Proof of Theorem 5.1.1 . . . 87
5.5.2 Proof of Theorem 5.1.3 . . . 89

6 Stability of 2-class groups in the $\mathbb{Z}_2$-extension of certain real biquadratic fields 91

6.1 Introduction . . . 91
6.2 Fields with 2-class group $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ . . . 93
6.2.1 Groups of order 16 . . . 96
6.3 Capitulation and norm maps in cyclic extensions . . . 97
6.4 The rank of $A(K_n)$ . . . 98
6.4.1 Proof of Theorem 6.1.1 . . . 101
6.5 An equivalent criteria for $\#A(K_n) = \#A(\mathbb{Q}_n(\sqrt{p}))$ . . . 103
6.5.1 Proof of Theorem 6.1.4 . . . 105
6.6 Order of $A(K_1)$ . . . 106
6.6.1 Proof of Theorem 6.1.6 . . . 109

6.6.2 An alternate condition for $\#A(K_1) = 2$ 113

Scope of future work **117**

Bibliography **117**

Publications **124**

Introduction

In 1600s, Fermat quoted his last "theorem" which states that for $n \geq 3$, there do not exist nonzero integers that satisfy $x^n + y^n = z^n$, although he did not provide a proof. Assuming that such integers exist, the left hand side of equation can be factorized as $x^n + y^n = (x + y)(x + \zeta_n y) \cdots (x + \zeta_n^{n-1} y)$, where ζ_n is a primitive n-th root of unity. Each factor $x + \zeta_n^i y$ is a complex number belonging to the ring $\mathbb{Z}[\zeta_n]$. Consequently, it was thought that studying the ring $\mathbb{Z}[\zeta_n]$ could provide an answer to Fermat's last theorem. It turned out that this ring is not a PID, but is a Dedekind Domain, and therefore, it is a PID if and only if it is a UFD. Kummer was able to show that for $p = 23$, $\mathbb{Z}[\zeta_p]$ is not a PID, and currently it is known that $\mathbb{Z}[\zeta_n]$ is a PID for only finitely many values of n. These key observations led to the realization that many rings with enough algebraic structures were still not completely understood. The study of such rings can be attributed towards the development of algebraic number theory, even though this area did not have a unified structure back then.

Algebraic number theory can be perceived as the study of algebraic numbers (the numbers that satisfy a polynomial with coefficient in $\mathbb{Q}$). From field theory, we know that finite extensions of $\mathbb{Q}$ are algebraic, and such fields are known as number fields. Every number field F contains a special ring known as the ring of integers $\mathcal{O}_F$, which contains all the elements of F that are integral over $\mathbb{Z}$. The containment $\mathcal{O}_F \subset F$ is analogous to $\mathbb{Z} \subset \mathbb{Q}$, but with a significant difference that $\mathcal{O}_F$ may not be a PID like $\mathbb{Z}$. As a result, the ideals of such rings became topics of interest. Keeping $\mathbb{Z}[\zeta_p]$ as an instance, we can prove that $\mathcal{O}_F$ is a Dedekind Domain, a property which ensures unique prime factorization of ideals of $\mathcal{O}_F$, even though it does not guarantee unique factorization of elements. The ideal class group emerged as a measure of the deviation of the ring of integers from being a

PID. More precisely, the ideal class group (or simply, class group) of a number field F is a finite abelian group $\mathcal{C}l_F$ whose order (known as the class number and denoted by h_F) is 1 if and only if $\mathcal{O}_F$ is a PID. The concept of class groups had previously come up in Gauss's work on quadratic forms. Later, it was used by Kummer in his quest to prove Fermat's last theorem. Kummer noticed that the size of the class group proved to be an obstruction in the proof. Nevertheless, he ended up proving Fermat's last theorem for $n = p$, where p is a regular prime, that is, a prime that does not divide the class number of $\mathbb{Q}(\zeta_p)$. Dedekind then introduced ideas like ideal factorization, and the area of algebraic number theory later got a more definite form. Finally, as one of the biggest achievements in the 20th century, Fermat's last theorem was proved by Andrew Wiles who used a variety of other concepts including elliptic curves and modular forms along with algebraic number theory to give a concrete proof.

The class group reflects the complexity of F, and is influenced by a number of factors including the discriminant of F, number of embeddings of F, units in $\mathcal{O}_F$, and so on. Although Minkowski's theorem provides a hands on method to calculate the class number, it is mostly feasible only when the class number is small. Therefore, class group always generates curiosity, and is an object of frequent consideration in research. In this thesis, we deal with problems involving the structure of class groups of various families of number fields. The topics covered can be broadly classified into two categories. The first one is about p-rationality of quadratic fields, and the second one is about Greenberg's conjecture on Iwasawa modules formed by ℓ-class groups.

Both finite and infinite field extensions play an important role in the characterization of class groups due to the Galois module structure of the class groups. A widely known conjecture on infinite Galois extensions which has appeared in numerous works in number theory is Leopoldt's conjecture ([54]). Certain versions of this conjecture can be found in [35]. For a prime number ℓ, an extension F_∞/F is said to be a $\mathbb{Z}_\ell$-extension if $\mathrm{Gal}(F_\infty/F)$ is topologically isomorphic to $\mathbb{Z}_\ell$, the additive group of ℓ-adic integers. Suppose $\mathcal{F}_\infty$ is the compositum of all the $\mathbb{Z}_\ell$-extensions of F. Then, as a consequence of Leopoldt's conjecture, as $\mathbb{Z}_\ell$-modules, $\mathrm{Gal}(\mathcal{F}_\infty/F) \cong \mathbb{Z}_\ell^{1+s}$, where s is the number of pairs of complex conjugate embeddings of F. In [12], Brumer validated Leopoldt's conjecture for abelian extensions of $\mathbb{Q}$ and for the abelian extensions of imaginary quadratic extensions of $\mathbb{Q}$.

While trying to produce infinitely many nonabelian number fields that satisfy Leopoldt's

conjecture at a prime p, Movaheddi introduced p-rational fields (cf. [67], [68], [69]). Let F be a number field and M be the maximal pro-p-extension of F unramified outside p. Then, F is said to be p-rational if $\Gamma = \mathrm{Gal}(M/F)$ is a free pro-p-group. Suppose Γ^{ab} is the largest abelian quotient of Γ. Then, Γ^{ab} is also a $\mathbb{Z}_p$-module, and F is p-rational if and only if the following conditions are satisfied (cf. [8], [36]):

1. The field F satisfies Leopoldt's conjecture at p, i.e., $\mathrm{rank}_{\mathbb{Z}_p}(\Gamma^{ab}) = 1 + s$.
2. As a $\mathbb{Z}_p$-module, Γ^{ab} is torsion free.

Let F be a totally really number field with fundamental units $\varepsilon_1, \ldots, \varepsilon_{r-1}$. Then, the p-adic regulator $R_{p,F}$ of F is the determinant of the matrix formed by the p-adic logarithms of $\varepsilon_1, \ldots, \varepsilon_{r-1}$. An equivalent version of Leopoldt's conjecture asserts that $R_{p,F}$ is nonzero. For a prime p, let $T_F = Tor_{\mathbb{Z}_p}(\Gamma^{ab})$. Let μ_p and μ_{p^∞} be the groups of all p-th and p-powered roots of unity, respectively. Suppose $x \sim y$ denotes that x and y have the same p-adic valuation. If F is a totally real number field with discriminant D_F for which Leopoldt's conjecture is true at p, then Coates proved the following result (cf. [8, Equation 2.1]):

$$\#T_F \sim \#(\mu_{p^\infty} \cap F(\mu_p)) \frac{h_f R_{p,F}}{\sqrt{|D_F|}} \prod_{\mathfrak{p}|p} \left(1 - (N_{F/\mathbb{Q}}(\mathfrak{p}))^{-1}\right).$$

Here, $N_{F/\mathbb{Q}}(\mathfrak{p})$ denotes the absolute norm of a prime ideal $\mathfrak{p}$ that lies above p in F. This result allows us to find explicit criteria for p-rationality in terms of p-adic valuations of various invariants associated with F. A number of results relating p-rationality with p-adic valuations can be found in [8]. Gras gave a complete list of abelian fields F of degree $p = 2, 3$ over $\mathbb{Q}$ that are p-rational (cf. [28]). Further details on this topic can be found in [2], [8], [29], [30], [32], [43], [68], and [69]. In 2016, while working on Galois representations of the group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ to $GL_n(\mathbb{Z}_p)$, Greenberg [36] conjectured the existence of multi-quadratic p-rational number fields of degree 2^t for any odd prime number p and any integer $t \geq 1$. He further provided a criteria of determining the p-rationality of quadratic fields for odd primes p. The conditions are comparable with Coates' result, and involve the class number and the fundamental unit of F. The conjecture has been proven for all odd primes in case of $t = 1$ and 2 (cf. [6], [8], respectively), and for infinitely many primes when $t = 3$ (cf. [46]). We aim on finding new families of quadratic p-rational fields with emphasis on "consecutiveness", as we shall see shortly.

The central question in classical Iwasawa theory is to study the growth of arithmetic objects as Galois modules in infinite extensions of number fields. The driving force behind this idea was the theory of algebraic varieties over extensions of finite fields. We may obtain extensions of finite fields by adjoining roots of unity, as finite extensions of the same degree of finite fields are unique up to isomorphism. But when it comes to infinite fields, that is not the case. This led to a particular choice of infinite extensions of number fields, namely the $\mathbb{Z}_\ell$-extensions for a prime ℓ.

We are already aware of the definition of a $\mathbb{Z}_\ell$-extension. One of the most important aspects of such an extension is that for each n, there exists a unique intermediate extension $F \subset F_n \subset F_\infty$ such that $\Gamma_n := \mathrm{Gal}(F_n/F) \cong \mathbb{Z}/\ell^n\mathbb{Z}$. Such an F_n is known as the *n-th layer* of F. The theory was initially developed by Iwasawa, keeping the ℓ-class groups of F_n as the primary objects of study. One of the reasons behind this was the obstruction caused by the ℓ-class groups in Kummer's proof of Fermat's last theorem, making these groups interesting. Later on, more objects like Selmer groups of elliptic curves defined over number fields, graphs, general linear groups have also been considered in $\mathbb{Z}_\ell$-extensions. We shall first understand the *Iwasawa algebra* and then proceed to *Iwasawa module* constructed with ℓ-class groups. Detailed discussion on Iwasawa modules in general can be found in [40] and [41].

Definition 0.0.1. [80, Theorem 13.13] *Let F be a number field with a $\mathbb{Z}_\ell$-extension F_∞, n-th layers F_n, and $\Gamma_n = \mathrm{Gal}(F_n/F)$. With respect to the projection maps from Γ_n to Γ_m for $n \geq m$, the Iwasawa algebra is defined as*

$$\Lambda := \varprojlim_n \mathbb{Z}_\ell[\Gamma_n] = \mathbb{Z}_\ell[\![\Gamma]\!].$$

Let $A_\ell(F_n)$ be the ℓ-class group of F_n. The standard action of Γ_n on $A_\ell(F_n)$ can be naturally extended to an action of $\mathbb{Z}_\ell[\Gamma_n]$ on $A_\ell(F_n)$. Because of this, $A_\ell(F_n)$ becomes a module over the group ring $\mathbb{Z}_\ell[\Gamma_n]$ and a similar behaviour is followed by their inverse limits.

Definition 0.0.2. [80, Theorem 13.13] *Let F be a number field with a $\mathbb{Z}_\ell$-extension F_∞, n-th layers F_n, and $\Gamma_n = \mathrm{Gal}(F_n/F)$. With respect to the norm maps $N_{n,m} : A_\ell(F_n) \to A_\ell(F_m)$ for $n \geq m$, $\{A_\ell(F_n) : n \geq 0\}$ forms an inverse system. The corresponding inverse limit given by*

$$X(F_\infty) := \varprojlim_n A_\ell(F_n),$$

is known as the Iwasawa module.

Therefore, Λ acts canonically on $X(F_\infty)$. One of the biggest advantages of treating $X(F_\infty)$ as a Λ-module is that we can obtain information on $A_\ell(F_n)$'s by understanding $X(F_\infty)$, and this is substantiated in [80, Lemma 13.15]. It turns out that $X(F_\infty)$ is a finitely generated, and torsion Λ-module (cf. [76, Proposition 3.2.11], [80, Lemma 13.17]). Due to the structure theorem of finitely generated Λ-modules (cf. [80, Theorem 13.12]), Iwasawa was able to prove the celebrated *Iwasawa's class number formula*, which we state as follows.

Theorem 0.0.3. [40, Theorem 11] *Let ℓ be a prime number and F be a number field with $\mathbb{Z}_\ell$-extension F_∞. Suppose F_n is the n-th layer in the extension F_∞/F and ℓ^{e_n} is the largest power of ℓ dividing the class number of F_n. Then, for sufficiently large n, there exist constants $\lambda(F_\infty/F)$, $\mu(F_\infty/F)$, and $\nu(F_\infty/F)$ such that*

$$e_n = \lambda(F_\infty/F) \cdot n + \mu(F_\infty/F) \cdot \ell^n + \nu(F_\infty/F).$$

Iwasawa conjectured that $\mu(F_\infty/F)$ must vanish for the cyclotomic $\mathbb{Z}_\ell$-extension F_∞ over any number field F. In [35], Greenberg conjectured that both $\mu(F_\infty/F)$ and $\lambda(F_\infty/F)$ must vanish for the cyclotomic (see Section 1.8.1) $\mathbb{Z}_\ell$-extension F_∞/F when F is a totally real field. Following these conjectures, Ferrero and Washington [21] proved that $\mu(F_\infty/F) = 0$ for the cyclotomic $\mathbb{Z}_\ell$-extension of a number field F when $F/\mathbb{Q}$ is an abelian extension. Greenberg's conjecture is still open, with partial progress made by considering particular values of ℓ and specific families of number fields. Some of the works in this direction can be seen in [23], [34], [38], [47], [50], [57], [59], [60], [61], [62], [63], [65], [66], [70], [71], [81].

In this thesis, we stick to the case $\ell = 2$ due to the availability of rich theories based on 2-class groups, and the comprehensive structure of the cyclotomic $\mathbb{Z}_2$-extension of number fields. We simply use $A(F)$ to denote the 2-class group of F.

Organization of the Thesis

We present the entire work of this thesis in six chapters as described below.

- Chapter 1: Preliminaries
- Chapter 2: On the p-rationality of consecutive quadratic fields
- Chapter 3: Structure of 2-class groups in the $\mathbb{Z}_2$-extensions of certain real quadratic fields
- Chapter 4: Stability of 2-class groups in the $\mathbb{Z}_2$-extension of certain real quadratic fields
- Chapter 5: Study of Iwasawa module via a bounded quotient
- Chapter 6: Stability of 2-class groups in the $\mathbb{Z}_2$-extension of certain real biquadratic fields

We discuss all the necessary theories and pre-requisites in Chapter 1 that are required to understand our work carried out in subsequent chapters. We look into concepts like ramification, Hilbert class fields, genus theory, quadratic reciprocity, and class number formula, to name a few.

Using the criteria provided by Greenberg to check p-rationality for abelian number fields and driven by his conjecture, certain infinite families of quadratic, biquadratic and triquadratic p-rational fields have been shown to exist in recent years. In Chapter 2, for any integer $m \geq 1$, we prove the existence of infinitely many prime numbers p for which the imaginary quadratic fields $\mathbb{Q}(\sqrt{-(p-1)}), \ldots, \mathbb{Q}(\sqrt{-(p-m)})$ and $\mathbb{Q}(\sqrt{-p(p-1)}), \ldots, \mathbb{Q}(\sqrt{-p(p-m)})$ are all p-rational. This can be construed as analogous results in the spirit of Iizuka's conjecture on the divisibility of class numbers of consecutive quadratic fields. We also address a similar question of p-rationality for two consecutive real quadratic fields by proving the existence of infinitely many p-rational fields of the form $\mathbb{Q}(\sqrt{p^2+1})$ and $\mathbb{Q}(\sqrt{p^2+2})$. The result for imaginary quadratic fields is accomplished by producing infinitely many primes for which the corresponding consecutive discriminants have large square divisors. The same for real quadratic fields is proven using a result of Heath-Brown on the relative density of square-free values of polynomials at prime arguments.

Chapter 3 onwards, our primary focus shifts to $\mathbb{Z}_2$-extension of real quadratic and biquadratic extensions of $\mathbb{Q}$, and the 2-class groups of the associated intermediate extensions.

In Chapter 3, for $K = \mathbb{Q}(\sqrt{d}), d > 0$, we study the structure of the 2-class group $A(K_1)$ of the first layer $K_1 = \mathbb{Q}(\sqrt{2}, \sqrt{d})$ of the $\mathbb{Z}_2$-extension of K. With some simple assumptions, we characterize K for which the 2-class group $A(K)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. We infer that the 2-ranks of the class groups in each layer stabilizes by virtue of a result of Fukuda. In some cases, we also provide sufficient conditions on the constituent prime factors of D_K that imply $A(K) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, $A(K_1) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ and $A(K') \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, where $K' = \mathbb{Q}(\sqrt{2d})$. This extends some results obtained by Mizusawa. We achieve our results by utilizing genus theory and Kuroda-Kubota's class number formula.

In Chapter 4, we deal with real quadratic fields $K = \mathbb{Q}(\sqrt{d})$, where d has 3 distinct odd prime factors. We choose certain infinite families K from the fields obtained by Mouhib and Movaheddi in [66]. In [66], the authors classified all the real quadratic fields whose Iwasawa module corresponding to their $\mathbb{Z}_2$-extension is cyclic. We show that for our choice of K, the 2-class group of each layer in the $\mathbb{Z}_2$-extension of K is $\mathbb{Z}/2\mathbb{Z}$ under certain elementary assumptions on the prime factors of d. In particular, it validates Greenberg's conjecture on the vanishing of the Iwasawa λ-invariant for a new family of infinitely many real quadratic fields. We accomplish this by studying the possible action of Galois group on 2-class groups. We again appeal to Kuroda-Kubota's class number formula, but with variation in arguments to establish the equivalence of order stability of 2-class groups and the existence of solutions to certain Diophantine equations. In the end, we also furnish an infinite family of real quadratic fields K such that the 2-class group of each layer of the $\mathbb{Z}_2$-extension of K is $\mathbb{Z}/2^m\mathbb{Z}$ for some $m \geq 2$.

In Chapter 5, we examine an infinite family of real quadratic fields $K = \mathbb{Q}(\sqrt{d})$ such that $d \equiv 1 \pmod 8$. This family is special because the prime $\langle 2 \rangle$ splits in K, in contrast to its behaviour in the previous chapter. We make use of the Hilbert symbol and prove that the Iwasawa module $X(K_\infty)$ of the $\mathbb{Z}_2$-extension of K has rank 2. More importantly, we study a quotient $X'(K_\infty)$ of $X(K_\infty)$, and prove the boundedness of its order. This helps us in verifying Greenberg's conjecture for K and also allows us to prove that the 4-rank of $X(K_\infty)$ is at most 1. The factorization of certain primes $p \equiv 1 \pmod 8$ in $\mathbb{Q}(\sqrt{2})$ becomes handy in this work.

Greenberg's conjecture on the stability of 2-class groups in the cyclotomic $\mathbb{Z}_2$-extension of a real field has been proven for various infinite families of real quadratic fields. But

the developments are not just limited to quadratic fields. In Chapter 6, we consider an infinite family of real biquadratic fields K. With some extensive use of elementary group theoretic and class field theoretic arguments, we find the structure of $A(K_1)$. We use the information about the $\mathbb{Z}_2$-extensions of the subfields of K to prove Greenberg's conjecture for K. We also relate capitulation of ideal classes of certain sub-extensions of K_n to the relative sizes of the 2-class groups. Kisilevsky's result on number fields with terminating 2-class field towers and classification of groups of order 16 are some of the essential tools used in this work.

1

Preliminaries

1.1 Results from algebra and number theory

By the *Fundamental theorem of finite abelian groups*, any finite abelian group G is isomorphic to the direct sum $\mathbb{Z}/p_1^{n_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_r^{n_r}\mathbb{Z}$ where p_i's are prime numbers and $n_i \geq 1$ for all $i = 1, \ldots, r$. If G is a finite abelian 2-group, then it must be isomorphic to $\mathbb{Z}/2^{n_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/2^{n_r}\mathbb{Z}$. Our focus will be mostly on finite 2-groups. It is known that there are exactly 5 distinct groups of order 8 upto isomorphism. The abelian ones are $\mathbb{Z}/8\mathbb{Z}, \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, and $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. The non-abelian groups of order 8 are $D_8 = \{r^m s^n : r^4 = s^2 = id,\ rs = sr^{-1}\}$ and $Q_8 = \{x^m y^n : x^2 = y^2, x^4 = y^4 = id,\ xy = yx^{-1}\}$. Proceeding to order 16, there are 5 abelian and 9 non-abelian groups of order 16. These groups are discussed in great detail in [15] and [16].

1.1.1 Profinite groups

We begin with inverse system and inverse limits of a set of groups indexed by a directed set. Inverse limit is an important concept and has been used in many areas of algebra and number theory. One of its applications is in the construction of completions of topological groups. Let I be a directed set with partial order $\leq$. Let $S = \{G_i : i \in I\}$ be a set of groups G_i indexed by I. Suppose for each $j, i \in I$ with $i \leq j$, there exists a homomorphism $\phi_{ji} : G_j \to G_i$ such that the following properties are satisfied:

1. For each i, $\phi_{ii} : G_i \to G_i$ is the identity map on G_i.
2. For all $i \leq j \leq k$, $\phi_{ki} = \phi_{ji} \circ \phi_{kj}$.

Then, the set S with the maps $\{\phi_{ji} : i, j \in I, i \leq j\}$ is known as an *inverse system*. Now we proceed to inverse limit:

Definition 1.1.1. [80, Appendix, Section 1] *Let* $\mathcal{G} = \prod_{i \in I} G_i$. *Then the inverse limit of* $\{G_i : i \in I\}$ *with respect to the maps* ϕ_{ji} *is given by*

$$\varprojlim_i G_i = \{(\ldots, g_i, \ldots) \in \mathcal{G} : \phi_{ji}(g_j) = g_i \text{ whenever } i \leq j\}.$$

There is a way to traverse from the inverse limit to individual components via projection maps. For each $i \in I$, there exists a map $\phi_i : \varprojlim_i G_i \to G_i$ which is induced by the usual projection map from $\mathcal{G}$ to G_i. In addition, $\phi_{ji} \circ \phi_j = \phi_i$ for all $i \leq j$. A well known example of inverse limits is the additive group of p-adic integers $\mathbb{Z}_p$ for any prime p. Let $I = \mathbb{N}$, $G_i = \mathbb{Z}/p^i\mathbb{Z}$, and $\phi_{ji}(a \pmod{p^j}) = a \pmod{p^i}$. Then $\varprojlim_i \mathbb{Z}/p^i\mathbb{Z} = \mathbb{Z}_p$. The group $\mathbb{Z}_p$ can also be interpreted as the completion of $\mathbb{Z}$ under the p-adic topology. We shall look at other inverse limits as we progress.

Suppose $\{G_i : i \in I\}$ is an inverse system of abelian groups. Then, the system is said to satisfy *Mittag-Leffler* condition if for every i, there exists a $j \geq i$ such that for all $k \geq j$, $\phi_{ki}(G_k) = \phi_{ji}(G_j)$. An inverse system of finite abelian groups always satisfies this condition. We now state a special consequence for such systems:

Lemma 1.1.2. *Let* $\{A_n : n \in \mathbb{N}\}$, $\{B_n : n \in \mathbb{N}\}$, *and* $\{C_n : n \in \mathbb{N}\}$, *be inverse systems of abelian groups. Assume that* $\{A_n : n \in \mathbb{N}\}$ *satisfies the Mittag-Leffler condition. Then,*

if the sequence $0 \to A_n \to B_n \to C_n \to 0$ *is exact, then the sequnce of inverse limits* $0 \to \varprojlim_n A_n \to \varprojlim_n B_n \to \varprojlim_n C_n \to 0$ *is also exact.*

In an infinite Galois extension of number fields, the Galois group is often expressed as the inverse limit of Galois groups of the finite intermediate extensions. This motivates one to study profinite groups, which we define as follows.

Definition 1.1.3. *A group G is said to be profinite if it is an inverse limit of finite groups. If each group in the inverse system is a finite p-group, then G is said to be a pro-p-group. If each group in the inverse system is cyclic, then G is said to be procyclic.*

If G is a topological group, then we say that a subset $S \subset G$ *topologically generates* G if the topological closure of the subgroup generated by S is equal to G, i.e., $\overline{\langle S \rangle} = G$. Let G be a p-group with its commutator subgroup G' and the subgroup G^p which is generated by all p-th powers in G. Then, it is known that G' and G^p are contained in every maximal subgroup of G. Therefore, $G', G^p \subset \phi(G)$ the *Frattini subgroup*, which is the intersection of all maximal subgroups of G. The subgroup $\phi(G)$ is normal (cf. [18, Theorem 1, Chapter 6]) and consequently, $G/\phi(G)$ is the largest p-elementary abelian quotient of G, and can be viewed as a vector space over $\mathbb{Z}/p\mathbb{Z}$ (cf. [18, Page 199]). *Burnside's basis theorem* is a result that relates the generators of G with the generators of $G/\phi(G)$.

Theorem 1.1.4. (Burnside's basis theorem) *Suppose G is a p-group with its Frattini subgroup $\phi(G)$. Then the following hold:*

1. *A subset S of G is a generating set of G if and only if the image of S in $G/\phi(G)$ generates it as a vector space over $\mathbb{Z}/p\mathbb{Z}$.*
2. *A subset S of G is a minimal generating set of G if and only if the image of S in $G/\phi(G)$ is a basis of $G/\phi(G)$ as a vector space over $\mathbb{Z}/p\mathbb{Z}$.*
3. *(Profinite version) Let G be a pro-p-group. Any lift of the generators of $G/\phi(G)$ to G will topologically generate G.*

Burnside's basis theorem is frequently used in understanding class field towers, which we shall see in the later sections.

1.1.2 Congruence and quadratic residues

Given integers x, y, and $m \neq 0$, we say x and y are *congruent modulo* m and denote by $x \equiv y \pmod{m}$, if m divides $x - y$. It is a routine question on whether there exists an integer x which satisfies a given system of congruences. This is tackled by the *Chinese remainder theorem*.

Theorem 1.1.5. (Chinese remainder theorem) *Let $n_1, \ldots, n_k$ be pairwise coprime positive integers, i.e., $\gcd(n_i, n_j) = 1$ for all $i \neq j$. Let $a_1, \ldots, a_k$ be integers such that $0 \leq a_i < n_i$. Consider the system of congruences:*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

Then, there exists an α unique modulo $N = n_1 \cdots n_k$ that satisfies the above system of congruences.

Given any odd prime p, a non-zero integer a is said to be a *quadratic residue modulo* p if there exists another integer b such that $b^2 \equiv a \pmod{p}$. The *Legendre symbol* $\left(\frac{a}{p}\right)$ is defined as the following:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p, \\ 0 & \text{if } p \text{ divides } a, \\ -1 & \text{if } a \text{ is not a quadratic residue modulo } p. \end{cases}$$

Fermat's little theorem states that any nonzero integer a which is coprime to a prime number p satisfies $a^{p-1} \equiv 1 \pmod{p}$. Keeping this in mind, the Legendre symbol is also defined to be the value that satisfies the congruence

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

We now look at some of the important characteristics of the Legendre symbol:

- If $a \equiv b \pmod{p}$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

- Completely Multiplicative: For every $a, b \in \mathbb{Z}$, $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$.
- Quadratic reciprocity: For distinct odd primes p and q, $\left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$.
- Special values: $\left(\frac{-1}{p}\right) = \begin{cases} -1 & \text{if } p \equiv 3 \pmod 4, \\ 1 & \text{if } p \equiv 1 \pmod 4 \end{cases}$ and

  $\left(\frac{2}{p}\right) = \begin{cases} -1 & \text{if } p \equiv 3, 5 \pmod 8, \\ 1 & \text{if } p \equiv 1, 7 \pmod 8. \end{cases}$
- For any odd p, there are exactly $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ non-residues modulo p.

The Legendre symbol was then generalized to *Jacobi symbol*, which allows the parameter at the bottom to be a positive odd number n instead of just odd prime numbers. Let n be an odd positive number with the prime factorization $n = {p_1}^{a_1} \cdots {p_r}^{a_r}$, where $a_i \geq 1$, p_i's are odd primes, and let $a \in \mathbb{Z}$ be any integer. Then, the Jacobi symbol $\left(\frac{a}{n}\right)$ is given by $\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{a_1} \cdots \left(\frac{a}{p_r}\right)^{a_r}$, where each $\left(\frac{a}{p_i}\right)$ is the Legendre symbol.

The next level of generalization of the Legendre symbol is the Kronecker symbol, where the parameter at the bottom, say n, can be any integer. Let $n \in \mathbb{Z}$, with prime factorization $n = up_1^{a_1} \cdots p_r^{a_r}$, where $u \in \{1, -1\}$, $a_i \geq 1$ and p_i's are prime numbers for $i = 1, \ldots, r$. Then, for any $m \in \mathbb{Z}$, the Kronecker symbol with upper parameter m, and lower parameter n is defined as $\left(\frac{m}{n}\right) = \left(\frac{m}{u}\right) \prod_{i=1}^{r} \left(\frac{m}{p_i}\right)^{a_i}$, where $\left(\frac{m}{p_i}\right)$ is the usual Legendre symbol if p_i is odd. For $p = 2$, the Kronecker symbol is defined as $\left(\frac{m}{2}\right) = \begin{cases} 1 & \text{if } m \equiv 1, 7 \pmod 8, \\ 0 & \text{if } m \text{ is even}, \\ -1 & \text{if } m \equiv 3, 5 \pmod 8 \end{cases}$.

For $u = 1$, $\left(\frac{m}{1}\right) = 1$ for all $m \in \mathbb{Z}$, and for $u = -1$, $\left(\frac{m}{-1}\right) = \begin{cases} 1 & \text{if } m \geq 0, \\ -1 & \text{if } m < 0 \end{cases}$. Finally, for $n = 0$, $\left(\frac{m}{0}\right) = \begin{cases} 1 & \text{if } m = 1, -1, \\ 0 & \text{otherwise} \end{cases}$.

Definition 1.1.6. *Let $p \equiv 1 \pmod 4$ be a prime number. Then, an integer m is said to be a quartic residue modulo p if m is congruent to a fourth power modulo p. The quartic residue symbol is denoted by $\left(\frac{\bullet}{p}\right)_4$.*

Remark 1.1.7. *If m is quartic residue modulo p, then obviously, it has to be a quadratic residue modulo p. Therefore, quartic symbols are only considered for integers that are quadratic residues. If a quadratic residue m is a quartic residue, then $\left(\frac{m}{p}\right)_4 = 1$, and otherwise $\left(\frac{m}{p}\right)_4 = -1$.*

We are all well aware that there are infinitely many prime numbers in $\mathbb{Z}$. One of the remarkable proofs of the infinitude of primes is the Dirichlet's theorem on primes in arithmetic progression. We state it as follows (cf. [14, Chapter 2, Theorem 4.1]).

Theorem 1.1.8. *Let $m > 0$ and a be relatively prime integers. Then, there are infinitely many primes of the form $a + mk$, where $k \in \mathbb{N}$. Equivalently, there are infinitely many primes p satisfying $p \equiv a \pmod m$.*

1.2 Number fields

A *number field* F is a finite field extension of $\mathbb{Q}$. The set of all elements of F that are roots of monic polynomials in $\mathbb{Z}$ form a ring. The ring is usually denoted by $\mathcal{O}_F$ and is known as the *ring of integers* of F. If $F/\mathbb{Q}$ is an extension of degree n, then there exist $\alpha_1, \ldots, \alpha_n$ in $\mathcal{O}_F$ such that $\{\alpha_1, \ldots, \alpha_n\}$ forms a basis of F as a vector space over $\mathbb{Q}$. Also, due to the existence of such a basis, $\mathcal{O}_F$ is a free module over $\mathbb{Z}$. Let $\sigma_1, \ldots, \sigma_n$ be the n-embeddings of F to $\mathbb{C}$ and $\{\beta_1, \ldots, \beta_n\}$ be a $\mathbb{Z}$-basis of $\mathcal{O}_F$ (also known as integral basis of F). The quantity $D_F := det([\sigma_i(\beta_j)])^2$ is a nonzero rational integer known as the *discriminant* of F, and it is independent of the choice of the integral basis. The discriminant is of great significance as it reflects many properties of the field F.

Suppose K/F is a Galois extension of number fields with $G = \mathrm{Gal}(K/F)$. If $\alpha \in K$ is arbitrary, then the trace and norm of α with respect to the extension K/F is given by:

$$Tr_{K/F}(\alpha) = \sum_{\sigma \in G} \sigma(\alpha),$$

$$N_{K/F}(\alpha) = \prod_{\sigma \in G} \sigma(\alpha).$$

It is a proven fact that both norm and trace of α belong to F, and if $\alpha \in \mathcal{O}_K$, then these quantities belong to $\mathcal{O}_F$. It is also to be noted that the norm and trace of an element are dependent on the extension in which they are being calculated.

The set of all multiplicative units in the ring $\mathcal{O}_F$ forms a group under multiplication. It is known as the *unit group* and is denoted by $E(F)$ or $\mathcal{O}_F^\times$. The units are crucial as they appear in various identities related to number fields. The *Dirichlet's unit theorem* characterizes the unit group $E(F)$ to a large extent. Let r be the number of real embeddings and s be the number of pairs of complex conjugate embeddings of F into $\mathbb{C}$. We now state the theorem as follows:

Theorem 1.2.1. (Dirichlet's unit theorem) *The unit group $E(F)$ of $\mathcal{O}_F$ is isomorphic to $W \oplus \left(\bigoplus_{r+s-1} \mathbb{Z} \right)$, where W is the group of roots of unity contained in $\mathcal{O}_F$.*

We infer that the non-torsion part of $E(F)$ has $r+s-1$ generators over $\mathbb{Z}$. A set $\{\varepsilon_1, \ldots, \varepsilon_{r+s-1}\}$ containing $r+s-1$ generators is known as a fundamental system of units. A generator ε_i is called a fundamental unit. Any unit u in $\mathcal{O}_F$ can be expressed as $u = u_1 \cdot \varepsilon_1^{n_1} \cdots \varepsilon_{r+s-1}^{n_{r+s-1}}$ where $u_1 \in W$ and $n_i \in \mathbb{Z}$.

1.2.1 The class group

For any number field F, $\mathcal{O}_F$ is a *Dedekind domain*, i.e., it is an integrally closed, Noetherian domain of dimension 1. By virtue of these properties, every ideal I of $\mathcal{O}_F$ can be uniquely expressed as a product of positive powers of finitely many prime ideals. In addition $\mathcal{O}_F$ is a PID if and only if it is a UFD. Suppose I and J are two ideals in $\mathcal{O}_F$. Then, from the definition of multiplication of ideals, it is clear that $IJ \subseteq I \cap J$. This means that the resultant ideal will be smaller than the factors. So the question arises on whether there are structures contained in F which upon multiplying with the ideals of $\mathcal{O}_F$ produce $\mathcal{O}_F$. This question was addressed with the introduction of *fractional ideals*.

Definition 1.2.2. *An $\mathcal{O}_F$-submodule $\mathfrak{a} \subset F$ is said to be a fractional ideal of F if there exists a nonzero element c in $\mathcal{O}_F$ such that $c\mathfrak{a} \subset \mathcal{O}_F$. Correspondingly, the set $\mathfrak{b} = c\mathfrak{a}$ is an ideal in $\mathcal{O}_F$.*

Every ideal contained in $\mathcal{O}_F$ is also a fractional ideal. The product of two fractional ideals is defined in the same way as that of two ideals. If $\mathfrak{a}$ is a fractional ideal, then we

define $\mathfrak{a}^{-1} := \{x \in F : x\mathfrak{a} \subseteq \mathcal{O}_F\}$. This set is a fractional ideal and we can prove that $\mathfrak{a}\mathfrak{a}^{-1}$ is equal to $\mathcal{O}_F$. Also, every fractional ideal can be uniquely factorised into a product of prime ideals raised to integral powers (negative powers are allowed). The set $\mathfrak{a}^{-1}$ is treated as the inverse of $\mathfrak{a}$ under multiplication, and we obtain the following theorem:

Theorem 1.2.3. *Let F be a number field and I_F be the set of all fractional ideals of F. Then I_F forms a group under multiplication.*

The set of principal fractional ideals $\mathcal{P}_F$, i.e., the ideals of the form $c^{-1}\langle a\rangle$, where $c \in \mathcal{O}_F \setminus \{0\}$ and $a \in \mathcal{O}_F$ forms a subgroup of I_F. Since $\mathcal{O}_F$ is a commutative ring, I_F is an abelian group and we can consider the quotient group $I_F/\mathcal{P}_F$. This group is known as the *class group* of F and is denoted by $\mathcal{C}l_F$. The quotient is associated with the equivalence relation on I_F where two fractional ideals $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent if and only if there exists a principal fractional ideal $\langle c\rangle$ such that $\mathfrak{a} = \langle c\rangle\mathfrak{b}$. Using Minowski's bound, we can prove the following theorem:

Theorem 1.2.4. *Let F be a number field and $\mathcal{C}l_F$ be its class group. Then $\mathcal{C}l_F$ is a finite abelian group and its order h_F is known as the class number of F.*

The ring $\mathcal{O}_F$ is a principal ideal domain if and only if every ideal of $\mathcal{O}_F$ is principal, i.e., $I_F = \mathcal{P}_F$. With the definition of class number, $\mathcal{O}_F$ is a PID if and only if $h_F = 1$. Therefore, class number measures how far the ring of integers is from being a PID. Higher the class number, higher the complexity in the ring of integers. This is one of the most significant aspects of the class group as it acts as a tool to assess $\mathcal{O}_F$.

1.2.2 Ramification theory

Suppose K/F is a finite extension of number fields. If $\mathfrak{p}$ is a prime ideal in $\mathcal{O}_F$, then $\mathfrak{p}\mathcal{O}_K$ is an ideal in $\mathcal{O}_K$ which can be factorized as

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

where $\mathfrak{P}_i$'s are prime ideals in $\mathcal{O}_K$ and r is a positive integer. Any $\mathfrak{P}_i$ that divides $\mathfrak{p}\mathcal{O}_K$ is said to *lie above* $\mathfrak{p}$. For each $i \in \{1, \ldots, r\}$, e_i is a positive integer, and is known as the *ramification index* for $\mathfrak{P}_i/\mathfrak{p}$.

Since the ring of integers is a Dedekind domain, every prime ideal is maximal, that too with finite index over the ring of integers. Suppose $\mathfrak{P}$ is a prime above $\mathfrak{p}$ in K. Since $\mathfrak{p}$ is a prime ideal, there exists a unique prime $p \in \mathbb{Z}$ such that $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$. Then, $\mathbb{F}_\mathfrak{p} := \mathcal{O}_F/\mathfrak{p}$ and $\mathbb{F}_\mathfrak{P} := \mathcal{O}_K/\mathfrak{P}$ are finite fields of characteristic p. Further, $\mathbb{F}_\mathfrak{P}$ can be viewed as an extension of $F_\mathfrak{p}$. Let f_i denote the degree of this extension. Then f_i is known as the *residual degree* or the *degree of residue* of $\mathfrak{P}_i/\mathfrak{p}$. Now, we quote a well known result that connects the ramification indices, residual degrees and the degree of the given extension of number fields:

Theorem 1.2.5. *Let K/F be a finite extension of number fields of degree n. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_F$ that factorizes as $\mathfrak{p}\mathcal{O}_F = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ in $\mathcal{O}_K$. Then we have $\sum_{i=1}^{r} e_i f_i = n$, where e_i is the ramification index and f_i is the residual degree of $\mathfrak{P}_i/\mathfrak{p}$ for each i.*

If $\sigma \in \mathrm{Aut}(K/F)$, and $\mathfrak{a}$ is an ideal of $\mathcal{O}_K$, then σ acts on $\mathfrak{a}$ by $\sigma(\mathfrak{a}) = \{\sigma(x) : x \in \mathfrak{a}\}$. In this way, if K/F is a Galois extension with Galois group G, then G acts transitively on the set of all prime ideals in $\mathcal{O}_K$ lying above a given prime ideal of $\mathcal{O}_F$.

Remark 1.2.6. *Suppose K/F is a Galois extension of degree n, $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_F$ that factorizes as $\mathfrak{p}\mathcal{O}_F = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ in $\mathcal{O}_K$. Then, $e_1 = \cdots = e_r = e$, $f_1 = \cdots = f_r = f$, and $efr = n$.*

If there exists at least one index $e_i > 1$, then $\mathfrak{p}$ is said to be *ramified* in K. Otherwise, $\mathfrak{p}$ is said to be *unramified* in K. The prime $\mathfrak{p}$ is said to be *totally ramified* if there exists some e_i such that $e_i = n$. In that case $p\mathcal{O}_K = \mathfrak{P}^n$ for some prime ideal $\mathfrak{P}$ in $\mathcal{O}_K$. If $r = 1$ and $e_1 = 1$, then $\mathfrak{p}$ is said to be *inert* in K. Consequently, $\mathfrak{p}\mathcal{O}_K$ is a prime ideal. Finally, if $e_i = f_i = 1$ for all i, then $\mathfrak{p}$ is said to *split completely* or *totally* in K. *Dedekind-Kummer* theorem provides us with a method of factorizing $\mathfrak{p}$ in extensions of number fields. We state it as follows:

Theorem 1.2.7. *Let K/F be an extension of number fields with $\mathcal{O}_K = \mathcal{O}_F[\alpha]$ for some $\alpha \in K$. Let f be the monic irreducible polynomial of α over F, and let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_F$ with $\mathbb{F}_\mathfrak{p} = \mathcal{O}_F/\mathfrak{p}$. Suppose $f(x)$ factorizes as $\overline{f(x)} = \overline{f_1(x)}^{e_1} \cdots \overline{f_r(x)}^{e_r}$ in $\mathbb{F}_\mathfrak{p}[x]$, where, $\overline{f_i(x)}$'s are distinct monic irreducible polynomials in $\mathbb{F}_\mathfrak{p}[x]$. For each i, let $f_i(x)$ be a lift of $\overline{f_i(x)}$ for each i to $\mathcal{O}_F[x]$. If $\mathfrak{P}_i$ denotes the ideal generated by $\mathfrak{p}$ and $f_i(\alpha)$ in $\mathcal{O}_K$, then, each $\mathfrak{P}_i$ is a prime ideal in $\mathcal{O}_K$ and $\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$.*

In case of quadratic fields $F = \mathbb{Q}(\sqrt{d})$ where d is square-free, ramification of primes of $\mathbb{Q}$ can be easily determined by the discriminant of the field. Let D_F be the discriminant of F and let p be an odd prime number in $\mathbb{Z}$. Then, $p\mathbb{Z}$ is inert in F if $\left(\frac{D_K}{p}\right) = -1$, ramified if p divides D_F, and splits completely if $\left(\frac{D_K}{p}\right) = 1$. The ideal $2\mathbb{Z}$ is inert if $d \equiv 5 \pmod 8$, ramified if $d \equiv 2, 3 \pmod 4$, and decomposed if $d \equiv 1 \pmod 8$. The converse also holds.

An important property of the ramification index and the residue degree is that they are multiplicative over a finite tower of number fields. If $F \subset K \subset L$ is a finite tower of number fields, and $\mathfrak{p}_F$ is a prime ideal of F with prime factors $\mathfrak{p}_K$ and $\mathfrak{p}_L$ in K and L, respectively, then,

$$e(\mathfrak{p}_L/\mathfrak{p}_F) = e(\mathfrak{p}_K/\mathfrak{p}_F) \cdot e(\mathfrak{p}_L/\mathfrak{p}_K),$$
$$f(\mathfrak{p}_L/\mathfrak{p}_F) = f(\mathfrak{p}_K/\mathfrak{p}_F) \cdot f(\mathfrak{p}_L/\mathfrak{p}_K).$$

Suppose K/F is a Galois extension with Galois group G and $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_F$ with a prime factor $\mathfrak{P}$ in $\mathcal{O}_K$. The *decomposition group* of $\mathfrak{P}$ is given by:

$$Z(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in G : \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

Due to the action of G on the set of prime ideals of K lying above $\mathfrak{p}$, $Z(\mathfrak{P}/\mathfrak{p})$ can be considered as the stabilizer of $\mathfrak{P}$. If $\mathfrak{P}$ and $\mathfrak{P}'$ are two prime factors of $\mathfrak{p}\mathcal{O}_K$, then $Z(\mathfrak{P}/\mathfrak{p})$ and $Z(\mathfrak{P}'/\mathfrak{p})$ are G-conjugate. The group $Z(\mathfrak{P}/\mathfrak{p})$ acts on the finite field $\mathbb{F}_\mathfrak{P} = \mathcal{O}_K/\mathfrak{P}$ and fixes $\mathbb{F}_\mathfrak{p} = \mathcal{O}_F/\mathfrak{p}$. Therefore, there exits a homomorphism ψ from $Z(\mathfrak{P}/\mathfrak{p})$ to $\mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})$ given by $\sigma \overset{\psi}{\mapsto} \bar{\sigma}$ where $\bar{\sigma}(x + \mathfrak{P}) = \sigma(x) + \mathfrak{P}$. This is a surjective homomorphism with kernel $T(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in Z(\mathfrak{P}/\mathfrak{p}) : x - \sigma(x) \in \mathfrak{P} \text{ for all } x \in \mathcal{O}_K\}$, known as the *inertia group* of $\mathfrak{P}$. The orbit-stabilizer theorem yields that $\#Z(\mathfrak{P}/\mathfrak{p}) = ef$ where e is the ramification index and f is the residual degree of $\mathfrak{P}/\mathfrak{p}$. Thus, $\#T(\mathfrak{P}/\mathfrak{p}) = e$.

The *norm of an ideal* in F is defined as its index as a subgroup of $\mathcal{O}_F$. If $\mathfrak{p}$ is a prime ideal in $\mathcal{O}_F$ and $N(\mathfrak{p})$ is its norm, then $N(\mathfrak{p}) = \#\mathbb{F}_\mathfrak{p}$. Let $\mathfrak{P} \subset \mathcal{O}_K$ be a prime above $\mathfrak{p}$. Then, the extension $\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p}$ is finite and cyclic, and its Galois group is generated by the *Frobenius element* given by $\phi_\mathfrak{p}(x+\mathfrak{P}) = x^{N(\mathfrak{p})}+\mathfrak{P}$. The pre-image of $\phi_\mathfrak{p}$ in $Z(\mathfrak{P}/\mathfrak{p})$ is called the *Frobenius element at* $\mathfrak{P}$. If $\mathfrak{P}$ and $\mathfrak{P}'$ are two primes above $\mathfrak{p}$, then the corresponding Frobenius elements must be conjugates. Suppose $\mathfrak{p}\mathcal{O}_F$ is unramified in K. Then, for any $\mathfrak{P}$ above $\mathfrak{p}$ in $\mathcal{O}_K$, $T(\mathfrak{P}/\mathfrak{p})$ must be trivial and $Z(\mathfrak{P}/\mathfrak{p}) \cong \mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})$. In that case, $\phi_\mathfrak{p}$ has a unique pre-image, i.e., the Frobenius element at $\mathfrak{P}$ must be an automorphism of K/F.

This pre-image is denoted by $\left(\frac{K/F}{\mathfrak{P}}\right)$.

Remark 1.2.8. *Let K/F be a Galois extension and $\mathfrak{p}$ be an unramified prime in K/F. Then, $\mathfrak{p}$ splits completely in K if and only if the Frobenius element at every prime divisor of $\mathfrak{p}$ is trivial.*

If K/F is an abelian extension, then the decomposition group for any prime factor of a given prime ideal of $\mathcal{O}_F$ will be the same, and hence, can be viewed independent of the prime factor. Thus, when K/F is an abelian extension, we say *decomposition group of* $\mathfrak{p}$ and denote it by $Z(\mathfrak{p})$. The Forbenius element corresponding to any prime divisor of $\mathfrak{p}$ will also be the same, and is denoted by $\left(\frac{K/F}{\mathfrak{p}}\right)$. Let K^Z and K^T be subfields of K fixed by $Z(\mathfrak{P}/\mathfrak{p})$ and $T(\mathfrak{P}/\mathfrak{p})$, respectively. Then we have the *Layer theorem* which gives a nice characterization of the decomposition of $\mathfrak{p}$ in K, K^T, and K^Z.

Theorem 1.2.9. [14, Chapter 1, Theorem 1.3] *Let K/F be an abelian extension and $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_F$. Then, $\mathfrak{p}$ splits completely in K^Z/F. The primes above $\mathfrak{p}$ remain inert in K^T/K^Z, and ramify totally in K/K^T.*

Finally, we state the following result which characterizes the splitting of primes in a compositum of Galois extensions:

Proposition 1.2.10. [42, Chapter 3, Corollary 2.7] *Let K_1 and K_2 be Galois extensions of F, and $L = K_1K_2$. Then, a prime $\mathfrak{p}$ of F splits completely in L if and only if $\mathfrak{p}$ splits completely in both K_1 and K_2.*

Artin map

Let K/F be an abelian extension with Galois group G. Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_F$ unramified in K/F. Then, $Z(\mathfrak{p})$ must be cyclic with one of its generators being the Frobenius element $\left(\frac{K/F}{\mathfrak{p}}\right)$. Let $\mathfrak{m}$ be the product of all primes that ramify in K/F, and let $\mathcal{I}_F(\mathfrak{m})$ be the group generated by all ideals of $\mathcal{O}_F$ that are relatively prime to $\mathfrak{m}$. Any ideal $\mathfrak{a} \in \mathcal{I}_F(\mathfrak{m})$ can be factorized as $\mathfrak{a} = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}$ where $a_i \in \mathbb{Z}$ and $\mathfrak{p}_i$'s are prime ideals unramified in K/F. The *Artin map* $\mathcal{A}$ from $\mathcal{I}_F(\mathfrak{m})$ to G is defined as $\mathfrak{a} \overset{\mathcal{A}}{\mapsto} \left(\frac{K/F}{\mathfrak{a}}\right) := \prod_{i=1}^{r} \left(\frac{K/F}{\mathfrak{p}_i}\right)^{a_i}$, where $\left(\frac{K/F}{\mathfrak{p}_i}\right)$ is the Frobenius element at $\mathfrak{p}_i$. The symbol $\left(\frac{K/F}{\mathfrak{a}}\right)$ is

known as the *Artin symbol*. We now state one of the important statements of the *Artin Reciprocity law*.

Theorem 1.2.11. [14, Chapter 5, Theorem 2.1(i)] *Let K/F be an abelian extension of number fields, and let $\mathfrak{m}$ be an ideal of $\mathcal{O}_F$ divisible by all the primes that ramify in K/F. Let $G = \mathrm{Gal}(K/F)$. Then, the Artin map $\mathcal{A} : \mathcal{I}_F(\mathfrak{m}) \to G$ is surjective.*

1.3 Unramified extensions of number fields

Let F be a number field and σ be an embedding of F into $\mathbb{C}$. We associate a formal object $\mathfrak{p}_\sigma$ to σ, which is called an *infinite prime* (real or imaginary) of F. If σ is an imaginary embedding, then $\mathfrak{p}_\sigma$ is associated with the conjugate pairs σ and $\bar{\sigma}$. Let K/F be an extension. If σ is a real embedding of F, then we say that $\mathfrak{p}_\sigma$ (or σ) ramifies in K/F if the extension of σ in K is such that $\sigma(K) \not\subseteq \mathbb{R}$. An extension K/F is said to be *unramified* if every prime (prime ideals of $\mathcal{O}_F$ and infinite primes) of F is unramified in K.

1.3.1 The Hilbert and narrow Hilbert class fields

The main philosophy behind class field theory is that one can study ideals and the class group of a number field F by studying abelian extensions of F. For any number field F, the maximal unramified abelian extension of F is known as the *Hilbert class field* of F. It is generally denoted by H_F and class field theory asserts its existence. Such an extension is Galois and finite over F with $\mathrm{Gal}(H_F/F) \cong \mathcal{C}l_F$, implying that $[H_F : F] = h_F$ (cf. [42, Theorem 13.1]). In fact, the Artin maps induces the isomorphism between the class group of a number field with its Hilbert class field (cf. [14, Chapter 3, Section 3]). For a prime number ℓ, the maximal ℓ-extension $L(F)$ of F contained in H_F is known as the ℓ-Hilbert class field of F. The Galois group of $L(F)/F$ is isomorphic to the ℓ-Sylow subgroup of $\mathcal{C}l_F$ (also known as the ℓ-class group of F). Therefore, $L(F)$ is the maximal unramified abelian ℓ-extension of F. Some of the most significant properties of the Hilbert class field of a number field F includes the following (cf. [42]).

1. A prime ideal $\mathfrak{p}$ in $\mathcal{O}_F$ splits into r prime ideals of inertia degree f, where $fr = [H_F : F] = h_F$ and f is the order of the ideal class $[\mathfrak{p}]$ in $\mathcal{C}l_F$. Therefore, an ideal is principal in F if and only if splits completely in H_F.

2. (Principal ideal theorem) Every ideal in F becomes principal in H_F.

3. If K is a finite extension of F such that $K \cap H_F = F$, then h_F divides h_K. Consequently, if some prime of F is totally ramified in a finite extension K/F, then h_F must divide h_K.

By definition, the Hilbert class field H_F obeys a stricter condition in the sense of ramification, that both the finite and infinite primes of F must remain unramified in H_F. It is possible to have a field extension where only the infinite primes are ramified. For example, $\mathbb{Q}(\sqrt{-1}, \sqrt{3})/\mathbb{Q}(\sqrt{3})$. Such extensions act as tools to understand the Hilbert class field better. First, we consider the following set up. An element $\alpha \in F$ is said to be *totally positive* if $\sigma(\alpha) > 0$ for all real embeddings of F. Let $\mathcal{P}_F^+$ be the set of all principal ideals of F generated by the totally positive elements of F. Then, the quotient group $\mathcal{C}l_F^+ = I_F/\mathcal{P}_F^+$ is known as the *narrow class group* of F (cf. [14, Chapter 3]). Again by class field theory, there exists an abelian extension H_F^+ of F such that $\mathrm{Gal}(H_F^+/F) = \mathcal{C}l_F^+$. This field is called the *narrow Hilbert class field* of F with $\#\mathcal{C}l_F^+$ known as the *narrow class number* of F, and it is ramified at only the infinite primes of F. It is automatic that $H_F \subset H_F^+$ as $P_F^+ \subset P_F$. In fact, if r is the number of real embeddings of F, and $E(F)^+ \subset E(F)$ is the subgroup of all totally positive units of $\mathcal{O}_F$, then from [42, Chapter 6, Theorem 3.1], $[H_F^+ : H_F] = 2^r/[E(F) : E(F)^+]$. In particular, if $F = \mathbb{Q}(\sqrt{d})$, then we have the following result:

Theorem 1.3.1. [42, Chapter 6, Theorem 3.2] *Let $F = \mathbb{Q}(\sqrt{d})$ where d is square-free, and u be the fundamental unit of F if $d > 0$. Then, $H_F^+ = H_F$ if either $d < 0$ or $d > 0$ with $N_{F/\mathbb{Q}}(u) = -1$. If $d > 0$ with $N_{F/\mathbb{Q}}(u) = 1$, then $[H_F^+ : H_F] = 2$.*

1.3.2 Genus field and the p-rank of class group

If $F/\mathbb{Q}$ is an abelian extension, then by maximality, H_F and H_F^+ are Galois (but not necessarily abelian) extensions of $\mathbb{Q}$. The largest abelian extension of $\mathbb{Q}$ contained in H_F can help in knowing more about the class group of F.

Definition 1.3.2. *Let $F/\mathbb{Q}$ be an abelian extension. The genus field (narrow genus field) of F over $\mathbb{Q}$ is the largest abelian extension of $\mathbb{Q}$ contained in H_F (H_F^+, respectively).*

We use F_G (F_G^+) to denote the genus field (narrow genus field, respectively) of F over $\mathbb{Q}$. It turns out that if $F = \mathbb{Q}(\sqrt{d})$, then F_G can be easily determined with the help of H_F^+ via Theorem 1.3.1.

Theorem 1.3.3. [42, Chapter 6, Theorems 3.10] *Let $F = \mathbb{Q}(\sqrt{d})$ where d is square-free. Suppose $|D_F|$ can be factorized as $2^e \cdot p_1 \cdots p_t$, where $e = 0, 2$, or 3, and p_i's are odd primes. With p_i^* defined as*

$$p_i^* = \begin{cases} p_i & \text{if } p_i \equiv 1 \pmod 4, \\ -p_i & \text{if } p_i \equiv 3 \pmod 4, \end{cases}$$

the narrow genus field F_G^+ is the field $\mathbb{Q}(\sqrt{d}, \sqrt{p_1^*}, \ldots, \sqrt{p_t^*})$. The genus field F_G is equal to F_G^+ if $d < 0$, and it is equal to the maximal real subextension of F_G^+ if $d > 0$.

In addition, when $F = \mathbb{Q}(\sqrt{d})$, the Artin map provides a relation between F_G and $\mathcal{C}l_F$ in the following way:

Theorem 1.3.4. [42, Chapter 6, Theorem 3.3] *Let $F = \mathbb{Q}(\sqrt{d})$ where d is square-free. Then, $\mathrm{Gal}(H_F/F_G) \cong \mathcal{C}l_F^2$. Therefore, $\mathrm{Gal}(F_G/F) \cong \mathcal{C}l_F/\mathcal{C}l_F^2$.*

For a finite abelian group G, G/G^2 is provides the number of components of even order present in the direct sum decomposition of G. We first define *rank* of a p-group and see how the rank of class group is it related with its genus field in some cases.

Definition 1.3.5. *Let G be a finite abelian p-group. By p-rank of G or $\mathrm{rank}_p G$, we mean the dimension of G/G^p as a vector space over $\mathbb{Z}/p\mathbb{Z}$.*

Since $\mathrm{Gal}(F_G/F) \cong \mathcal{C}l_F/\mathcal{C}l_F^2$ when F is a quadratic field, $\mathrm{Gal}(F_G/F)$ is an elementary-2 group (groups of the form $\mathbb{Z}/2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/2\mathbb{Z}$) isomorphic to the subgroup of $\mathcal{C}l_F$ of elements of order 2. Thus, F_G can aide in finding the 2-rank of $\mathcal{C}l_F$. In fact, F_G is the maximal unramified 2-elementary extension of F.

Remark 1.3.6. *Let F be a quadratic field with genus field F_G. Then, $\mathrm{rank}_2\mathrm{Gal}(F_G/F) = \mathrm{rank}_2\mathcal{C}l_F$.*

Genus fields can also be defined for arbirary extension of number fields. We use F_G to denote the genus field of F over $\mathbb{Q}$. For an arbitrary extension K/F, we use K_F^* to denote the genus field of K over F.

Definition 1.3.7. *Let K/F be a finite extension of number fields. Then, the genus field K_F^* of K over F is the maximal extension of the type Kk such that k/F is abelian and Kk/K is unramified.*

We note from [53, Theorem 1.3.4] that for an arbitrary quadratic extension K/F, the genus field K_F^* can be found in a similar way as given in Theorem 1.3.3, provided the narrow class number h_F^+ is equal to 1. Also, from [53, Section 1.3.2], we learn that if $F/\mathbb{Q}$ is a cyclic extension of odd degree p with number of ramified primes equal to t, then $[F_G : F] = p^{t-1}$. In addition, $\text{rank}_p \mathcal{C}l_F = r$, where $t-1 \leq r \leq (p-1)(t-1)$. This indicates that the p-ranks of $\mathcal{C}l_F$ and $\text{Gal}(F_G/F)$ need not be equal if $F/\mathbb{Q}$ is a cyclic extension of odd prime degree. Using arguments that mainly involve ramification theory, Xianke [82] found a method of finding genus fields for $F/\mathbb{Q}$ where F is an abelian extension of degree p^s for any prime p. The result is resourceful as it allows us to explicitly find genus fields of multiquadratic number fields over $\mathbb{Q}$.

1.4 Class group as a Galois module

It can be observed from the rich literature available that one can investigate class groups by viewing them as Galois modules. Let K/F be a Galois extension of number fields with $G = \text{Gal}(K/F)$. We recall from Section 1.2.2 that $\sigma \in G$ acts on ideals of $\mathcal{O}_K$ by acting element-wise. This action can be naturally extended to fractional ideals and ideal classes. If $\mathfrak{a} \subset K$ is a fractional ideal with factorization $\mathfrak{a} = \prod_{i=1}^{t} \mathfrak{P}_i^{n_i}$ where $n_i \in \mathbb{Z} \setminus \{0\}$ and $\mathfrak{P}_i$'s are prime ideals, then for any $\sigma \in G$,

$$\sigma(\mathfrak{a}) = \prod_{i=1}^{t} \sigma(\mathfrak{P}_i)^{n_i} \text{ and } \sigma([\mathfrak{a}]) = [\sigma(\mathfrak{a})]. \tag{1.1}$$

As $\sigma \in G$ is an automorphism of F, it distributes not only over products of elements of F, but also over product of ideals and ideal classes of F. Therefore, we obtain that $\sigma([\mathfrak{a}] \cdot [\mathfrak{b}]) = \sigma([\mathfrak{a} \cdot \mathfrak{b}]) = [\sigma(\mathfrak{a} \cdot \mathfrak{b})] = [\sigma(\mathfrak{a}) \cdot \sigma(\mathfrak{b})] = [\sigma(\mathfrak{a})] \cdot [\sigma(\mathfrak{b})] = \sigma[\mathfrak{a}] \cdot \sigma[\mathfrak{b}]$. Thus, $\mathcal{C}l_F$ is a G-module. In the subsequent sections, we use $[\mathfrak{a}]^\sigma$ to denote $\sigma([\mathfrak{a}])$. Since $\mathcal{C}l_F$ is a G-module, for $m \geq 0, a_i \in \mathbb{Z}$ and $\sigma_i \in G$, $[\mathfrak{a}]^{a_1\sigma_1 + \cdots + a_m\sigma_m} = ([\mathfrak{a}]^{a_1})^{\sigma_1} \cdots ([\mathfrak{a}]^{a_m})^{\sigma_m}$.

An ideal class $[\mathfrak{a}]$ is said to be *ambiguous* if $[\mathfrak{a}]^\sigma = [\mathfrak{a}]$ for every $\sigma \in G$, and *strongly*

ambiguous if there exists an ideal $\mathfrak{b} \in [\mathfrak{a}]$ such that $\mathfrak{b}^\sigma = \mathfrak{b}$ for every $\sigma \in G$. We denote the set of all ambiguous ideal classes in a Galois extension K/F by $\mathcal{C}l_K^G$ where $G = \mathrm{Gal}(K/F)$. Cornell in [17] related the subgroup of ambiguous ideal classes in a cyclic extension of number fields with the relative genus field. We now state some of the important the results which can be seen as generalizations of Theorem 1.3.4.

Theorem 1.4.1. [17, Proposition 3] *Let K/F be a cyclic extension with Galois group $G = \langle\sigma\rangle$. If K_F^* is the genus field of K over F, then $\mathrm{Gal}(K_F^*/K) \cong \mathcal{C}l_K/\mathcal{C}l_K^{1-\sigma}$, where $\mathcal{C}l_K^{1-\sigma} = \{[x]^{1-\sigma} : [x] \in \mathcal{C}l_K\}$.*

Proposition 1.4.2. [17, Proposition 4] *Let K/F be a cyclic extension with Galois group $G = \langle\sigma\rangle$ and the ambiguous class group of K given by $\mathcal{C}l_K^G$. Then, $\#\mathcal{C}l_K^G = [K_F^* : K]$.*

Formulas regarding $\#\mathcal{C}l_F^G$ dates back to a number of mathematicians including Chevalley, Herbrand, Furtwangler, Furuta, Yokoi, and many more. We present a version of such a formula for cyclic extensions of prime degree even though we mainly require the formula for quadratic extensions over $\mathbb{Q}$ (cf. [13], [58], [59]).

Theorem 1.4.3. (Genus formulae) *Let K/F be a cyclic extension of prime degree p and Galois group $G = \langle\sigma\rangle$. Let $A_p(K)$ and $A_p(F)$ denote the p-class groups of K and F, respectively. If $A_p(K)^G$ is the subgroup of $A_p(K)$ fixed by the action of G, and $B_p(K)^G$ is the subgroup of $A_p(K)$ generated by the strongly ambiguous ideal classes, then we have the following:*

$$\#A_p(K)^G = \frac{\#A_p(F) \cdot \prod_v e_v}{\#G \cdot \left[E(F) : E(F) \cap N_{K/F}(K^\times)\right]}, \tag{1.2}$$

$$\#B_p(K)^G = \frac{\#A_p(F) \cdot \prod_v e_v}{\#G \cdot \left[E(F) : N_{K/F}(E(K))\right]}. \tag{1.3}$$

Here, v runs over all places of F and e_v is the corresponding ramification index in K/F. In particular, when K/F is a quadratic extension with 2-class groups $A(K)$ and $A(F)$ and t is the number of places ramified in K/F, we have:

$$\#A(K)^G = \#A(F) \times \frac{2^{t-1}}{\left[E(F) : E(F) \cap N_{K/F}(K^\times)\right]}, \tag{1.4}$$

$$\#B(K)^G = \#A(F) \times \frac{2^{t-1}}{\left[E(F) : N_{K/F}(E(K))\right]}. \tag{1.5}$$

1.5 Homomorphisms between class groups

Given an extension of number fields K/F, we understand from the definition of norm of an element that such a map is a way of coming down from a bigger field to a smaller one. Similarly, extension and contraction of ideals is a way of climbing up and down between extension of rings. Motivated by these concepts, one may ask if there is way to navigate through the class groups of number fields in an extension. Such a question can be answered with the help of lifting and norm maps between the class groups.

Definition 1.5.1. *Let K/F be an extension of number fields. The lifting map $j : \mathcal{C}l_F \to \mathcal{C}l_K$ is defined as $j([\mathfrak{a}]) = [\mathfrak{a}\mathcal{O}_K]$, where $\mathfrak{a}\mathcal{O}_K$ is the extension of the ideal $\mathfrak{a}$ of F.*

The notion of norm can also be introduced to ideals. For an ideal $\mathfrak{b}$ in K, its norm with respect to the extension K/F with $G = \mathrm{Gal}(K/F)$ is given by $\prod_{\sigma \in G} \sigma(\mathfrak{b})$. This type of norm is sometimes known as the *algebraic norm* of an ideal. It can be extended as a map from $\mathcal{C}l_K$ to itself and is sometimes denoted by ν. In order to define the norm map between $\mathcal{C}l_K$ to $\mathcal{C}l_F$, we require one more step as we need an ideal in F.

Definition 1.5.2. *Let K/F be a Galois extension of number fields with $G = \mathrm{Gal}(K/F)$. Then the norm map from $\mathcal{C}l_K$ to $\mathcal{C}l_F$ is given by $N_{K/F}([\mathfrak{b}]) = \left[\prod_{\sigma \in G} \sigma(\mathfrak{b}) \cap \mathcal{O}_F\right]$.*

An ideal of F is said to *capitulate* in K if its extension in $\mathcal{O}_K$ is principal. The corresponding ideal class thus belongs to the kernel of the lifting map j. It is not trivial in general to find the ideal classes that capitulate in an extension. One of the earliest results that provides some idea on the size of the kernel of the lifting map is *Hilbert's Theorem 94*. We state it as follows:

Theorem 1.5.3. [53, Theorem 1.8.1] *Let K/F be a cyclic unramified extension of prime degree p. Then, there is a non principal ideal $\mathfrak{a}$ in F which capitulates in K. In particular, the class number of F is divisible by p.*

Let $\kappa_{K/F}$ be the kernel of the lifting map from F to K where the extension K/F is unramified and cyclic of prime power degree. Applying cohomological arguments, Rosen proved the following result that establishes a connection between capitulation and the units

(cf. [53, Section 1.8], [74]).

$$\#\kappa_{K/F} = [K : F][E(F) : N_{K/F}(E(K))]. \tag{1.6}$$

The Principal Ideal Theorem of class field theory essentially says that each ideal of F capitulates in H_F. Terada generalized this result in the sense of capitulation in unramified cyclic extensions by proving the following result (cf. [79]):

Theorem 1.5.4. *If K/F is cyclic and unramified, then the ambiguous ideal classes of K capitulate in H_F.*

Now we proceed to the norm map of ideal classes. Hilbert's Theorem 90 states that in a cyclic extension K/F with $\mathrm{Gal}(K/F) = \langle\sigma\rangle$, if $N_{K/F}(a) = 1$ for some $a \in K$, then there exists $b \in K$ such that $a = b/\sigma(b)$. In [25], Furtwängler proved an analogous version for norm map between class groups in an unramified cyclic extension, and it is known as the *Hilbert's Theorem 90 for ideal classes*. More specifically, this result characterizes the kernel of norm map between ideal classes when the extension is unramified and cyclic.

Theorem 1.5.5. *Let K/F be a cyclic unramified extension with $\mathrm{Gal}(K/F) = \langle\sigma\rangle$. Then, an ideal class $[\mathfrak{a}] \in \mathcal{C}l_K$ has $N_{K/F}([\mathfrak{a}]) = id$ if and only if there exists $[\mathfrak{b}] \in \mathcal{C}l_K$ such that $[\mathfrak{a}] = [\mathfrak{b}]^{1-\sigma}$.*

If K/F is Galois, then the composition of j and $N_{K/F}$ has a compact form that can be expressed as the following:

$$(j \circ N_{K/F})([\mathfrak{a}]) = \nu([\mathfrak{a}]) \text{ for all } [\mathfrak{a}] \in \mathcal{C}l_K, \text{ and,} \tag{1.7}$$

$$(N_{K/F} \circ j)([\mathfrak{b}]) = [\mathfrak{b}]^{[K:F]} \text{ for all } [\mathfrak{b}] \in \mathcal{C}l_F. \tag{1.8}$$

It may be pointed out from [76, Lemma 1.3.7] that if K/F is a Galois extension, then $coker(N_{K/F}) \cong \mathrm{Gal}(H_F \cap K/F)$. A direct consequence of this isomorphism is the following result that is utilized frequently while working with class groups of number fields in an extension.

Theorem 1.5.6. [76, Corollary 1.3.8] *If K/F is a Galois extension totally ramified at some prime, then $N_{K/F} : \mathcal{C}l_K \to \mathcal{C}l_F$ is surjective.*

1.6 Reciprocity laws in number fields and the Hilbert symbol

It is possible to extend the notions of reciprocity to the ring of integers of a number field that contains the m-th roots of unity for some m. The Artin symbol enables us to generalise the concepts like power residues and reciprocity to arbitrary ring of integers. The first symbol to branch out of the Artin symbol is the *norm residue symbol*. In a finite abelian extension K/F, for $\alpha \in F$ and a prime ideal $\mathfrak{p}$ of F, the norm residue symbol of α with respect to $\mathfrak{p}$ is an element in $\mathrm{Gal}(K/F)$. Suppose $\mathfrak{p}$ is an unramified prime ideal in K/F, and $\langle \alpha \rangle = \mathfrak{p}^a$ for some integer a in the completion $F_{\mathfrak{p}}$. Then, the norm residue symbol of α with respect to $\mathfrak{p}$ is defined as

$$\left(\frac{\alpha, K/F}{\mathfrak{p}}\right) = \left(\frac{K/F}{\mathfrak{p}}\right)^a.$$

This symbol is also defined for ramified prime ideals via ideles in class field theory (for further details, we refer to [14], [24], [42]).

Suppose F contains the m-th roots of unity, and $K = F(\beta^{1/m})$ for some $\beta \in F^\times \setminus (F^\times)^m$. For any $\alpha \in F$ and a prime ideal $\mathfrak{p}$ in F, the action of the norm residue symbol on $\beta^{1/m}$ is given by $\left(\frac{\alpha, K/F}{\mathfrak{p}}\right) \cdot \beta^{1/m} = \zeta_m \cdot \beta^{1/m}$, where ζ_m is an m-th root of unity. This root of unity ζ_m is denoted by $\left(\frac{\alpha, \beta}{\mathfrak{p}}\right)$, and is known as the *Hilbert symbol*. We now list some of the properties of the Hilbert symbol that come in handy in our work.

Proposition 1.6.1. *Let F be a number field that contains the m-th roots of unity. Suppose $\alpha, \beta \in F$ such that β is not an m-th power in F. Let $\mathfrak{p}$ be a prime in F. Then, the Hilbert symbol $\left(\frac{\alpha, \beta}{\mathfrak{p}}\right)$ satisfies the following:*

1. *The element $\alpha \in F$ is a norm in the extension $F(\beta^{1/m})/F$ if and only if $\left(\frac{\alpha, \beta}{\mathfrak{p}}\right) = 1$ for all the prime ideals $\mathfrak{p}$ of F.*
2. $\left(\frac{\alpha, \beta\gamma}{\mathfrak{p}}\right) = \left(\frac{\alpha, \beta}{\mathfrak{p}}\right)\left(\frac{\alpha, \gamma}{\mathfrak{p}}\right)$ *and* $\left(\frac{\alpha\gamma, \beta}{\mathfrak{p}}\right) = \left(\frac{\alpha, \beta}{\mathfrak{p}}\right)\left(\frac{\gamma, \beta}{\mathfrak{p}}\right)$
3. $\left(\frac{\alpha, \beta}{\mathfrak{p}}\right) = \left(\frac{\beta, \alpha}{\mathfrak{p}}\right)^{-1}$.

Analogous to Fermat's little theorem, if $\mathfrak{p}$ is a prime ideal in a number field F, and $\alpha \in \mathcal{O}_F \setminus \mathfrak{p}$, then $\alpha^{N\mathfrak{p}-1} \equiv 1 \pmod{\mathfrak{p}}$. Suppose F contains the m-th roots of unity and $\mathfrak{p}$ is a prime ideal that does not divide m. Then, [24, Page 105, Chapter 10], m divides $N\mathfrak{p}-1$. If $\alpha \notin \mathfrak{p}$, then $\alpha^{\frac{N\mathfrak{p}-1}{m}} \pmod{\mathfrak{p}}$ is an m-th root of unity modulo $\mathfrak{p}$. Therefore, the Legendre symbol in F can be defined as follows:

Definition 1.6.2. *Let F be a number field containing the m-th roots of unity, $\mathfrak{p}$ be an ideal not dividing m, and let $\alpha \in \mathcal{O}_F \setminus \mathfrak{p}$. The Legendre symbol $\left(\frac{\alpha}{\mathfrak{p}}\right)$ is defined as the unique m-th root of unity which satisfies*

$$\alpha^{\frac{N\mathfrak{p}-1}{m}} \equiv \left(\frac{\alpha}{\mathfrak{p}}\right) \pmod{\mathfrak{p}}.$$

The way Legendre symbol of a quadratic residue modulo p is equal to 1, we have the following result for general number fields.

Proposition 1.6.3. *Let F be a number field containing the m-th roots of unity, and let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_F$. If $\alpha \in \mathcal{O}_F \setminus \mathfrak{p}$, then α is an m-th power modulo $\mathfrak{p}$ if and only if $\left(\frac{\alpha}{\mathfrak{p}}\right) = 1$.*

The Jacobi symbol in a number field F containing the m-th roots of unity can also be derived similarly. Let $\alpha, \beta \in F^*$ with $\langle\alpha\rangle = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}$ and $\langle\beta\rangle = \mathfrak{q}_1^{b_1} \cdots \mathfrak{q}_s^{b_s}$ such that $\langle\alpha\rangle$ and $\langle\beta\rangle$ are coprime. If $\langle\beta\rangle$ and $\langle m\rangle$ are also coprime, then the Jacobi symbol with parameters α and β is given by

$$\left(\frac{\alpha}{\beta}\right) = \prod_{j=1}^{s} \left(\frac{\alpha}{\mathfrak{q}_j}\right)^{b_j}. \tag{1.9}$$

We require reciprocity laws when F is a number field containing only the second roots of unity. Therefore, we now state the quadratic reciprocity law for general number fields.

Theorem 1.6.4. [24, Corollary 10.11, Corollary 10.13] *Let F be a number field with r distinct embeddings into $\mathbb{R}$. Suppose $\alpha, \beta \in F^*$ such that $\langle\alpha\rangle$ and $\langle\beta\rangle$ are mutually coprime, and are also respectively coprime to $\langle 2\rangle$. Let $\sigma_1, \ldots, \sigma_r$ be the real embeddings and define $\alpha_i = \sigma_i(\alpha)$ and $\beta_i = \sigma_i(\beta)$ for $i = 1, \ldots, r$. Then,*

$$\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right) = \prod_{\mathfrak{p}\mid\langle 2\rangle} \left(\frac{\alpha,\beta}{\mathfrak{p}}\right) \prod_{i=1}^{r} (-1)^{s(\alpha_i,\beta_i)} \text{ where, } s(\alpha_i,\beta_i) = \begin{cases} 1 & \text{if } \alpha_i < 0 \text{ and } \beta_i < 0, \\ 0 & \text{otherwise.} \end{cases}$$

Here, $\left(\frac{\alpha,\beta}{\mathfrak{p}}\right)$ *is taken with respect to the extension* $F(\sqrt{\beta})/F$*. If either of* α *or* β *is congruent to a square modulo* $\langle 4\rangle$ *in* F*, then we arrive at a special case, also known as Hecke's reciprocity, given by*

$$\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right) = \prod_{i=1}^{r}(-1)^{s(\alpha_i,\beta_i)}.$$

1.7 Density

The proof of Dirichlet's theorem on primes in arithmetic progression requires analytic methods, and certain steps of the proof lead to the notion of *density*. We discuss two types of density, namely, the *natural density* and the *Dirichlet density*.

Definition 1.7.1. *Let* $A \subset \mathbb{N}$*. Then,* A *is said to have natural density* α *if*

$$\lim_{n\to\infty} \frac{\#\{x \in A : x \leq n\}}{n} = \alpha.$$

Clearly, $0 \leq \alpha \leq 1$. In number theory, it is fairly common to consider the density of subsets of prime numbers relative to the set of all prime numbers. The set of all prime numbers less than or equal to n is denoted by $\pi(n)$. We now proceed to Dirichlet density, another take on density that can be expanded to arbitrary number fields.

Definition 1.7.2. [14, Section 5] *Let* F *be a number field and* S *be a subset of prime ideals of* $\mathcal{O}_F$*. Then,* S *is said to have Dirichlet density* $\delta(S) = \delta$ *if* $\lim_{s\to 1^+} \frac{\sum_{\mathfrak{p}\in S} N(\mathfrak{p})^{-s}}{\log(\frac{1}{s-1})}$ *exists, and equals* δ*.*

From all the definitions, it is straightforward that a finite set has density 0. Therefore, if a set has positive density, then it must be infinite. On the other hand, some infinite subsets of $\mathbb{N}$ may have density 0. For example, if $A = \{n^2 : n \in \mathbb{N}\}$, then A is infinite and it can be easily shown that its density in $\mathbb{N}$ is 0. Another example is that the set of all prime numbers have density 0 in $\mathbb{N}$. One of the well known theorems involving density is *Chebotarev's density theorem* (cf. [42, Chapter 5, Theorem 10.4]). We state it as follows:

Theorem 1.7.3. *Let* K/F *be a Galois extension with Galois group* G*. Let* $\sigma \in G$ *and* C_σ *be its conjugacy class. Let* $S = \{\mathfrak{p} \subset \mathcal{O}_F : \mathfrak{p}$ *is unramified in* K/F *and* $\left(\frac{K/F}{\mathfrak{P}}\right) \in C_\sigma$ *for every* $\mathfrak{P}|\mathfrak{p}$ *in* $\mathcal{O}_K\}$*. Then, the Dirichlet density* $\delta(S)$ *of* S *is equal to* $\#C_\sigma/\#G$*.*

If K/F is an abelian extension, then for any $\sigma \in G$, C_σ is singleton. Therefore, Theorem 1.7.3 can be rephrased in the following manner:

Corollary 1.7.4. *Let K/F be an abelian extension with Galois group G, and an element $\sigma \in G$. Then, the Dirichlet density of $S = \{\mathfrak{p} \subset \mathcal{O}_F : \left(\frac{K/F}{\mathfrak{p}}\right) = \sigma\}$ is equal to $1/\#G$.*

Integrating the Artin map and the Chebotarev density theorem on H_F/F, it is known that every ideal class in $\mathcal{C}l_F$ contains infinitely many prime ideals. Furthermore, applying arguments involving summation of norms of prime ideals, the following result can be concluded, which we use in our study of class groups.

Corollary 1.7.5. *Let K/F be a Galois extension of number fields with $[\mathfrak{a}] \in \mathcal{C}l_K$. Then, $[\mathfrak{a}]$ can be represented by a prime ideal $\mathfrak{P}$ that lies over a prime $\mathfrak{p}$ of F which splits completely in K/F.*

Employing genus formula for quadratic extensions and Corollary 1.7.5, we obtain the next proposition, which we frequently appeal to while studying the 2-rank of class groups. We outline its proof though it is well-known in the literature.

Proposition 1.7.6. *Let K/F be a quadratic extension of number fields with 2-class groups $A(K)$ and $A(F)$, respectively. If the image of the lifting map $j : A(F) \to A(K)$ is trivial, then the non-trivial element of $G = \mathrm{Gal}(K/F)$ acts as -1 on $A(K)$. In that case, $A(K)^G$ is the subgroup of elements of order 2. Consequently,*

$$\#A(K)^G = \#\left(A(K)/2A(K)\right) = 2^{\mathrm{rank}_2 A(K)}.$$

Proof. Let σ be the generator of $G = \mathrm{Gal}(K/F)$, and $[\mathfrak{P}]$ be an ideal class in $A(K)$ for a prime ideal $\mathfrak{P}$ of K. From Corollary 1.7.5, we may choose $\mathfrak{P}$ such that it lies above a split prime $\mathfrak{p}$ in F. Since the lifting map is trivial, we have

$$[\mathfrak{P}] \cdot [\mathfrak{P}]^\sigma = [\mathfrak{p}\mathcal{O}_K] = j([\mathfrak{p}]) = id.$$

Hence, σ acts as -1 on $A(K)$. Therefore, $A(K)^G = A(K)[2]$ and the result follows. □

1.7.1 Analytic class number formula

Dirichlet's theorem on primes in arithmetic progression also motivated the definition of the *Dedekind zeta function*. Let $\mathfrak{a}\mathcal{O}_F$ be a non-zero ideal with norm $N\mathfrak{a}$. Then, the Dedekind zeta function of F is defined as

$$\zeta_F(s) = \sum_{\mathfrak{a}} \frac{1}{N\mathfrak{a}^s}.$$

The Analytic class number formula relates $\zeta_F(s)$ with a number of important invariants of F. The formula is generally attributed to Dedekind, Dirichlet, Kummer and Landau. We now state the result.

Theorem 1.7.7. [14, Chapter 2, Theorem 4.2] *Let F be a number field and $\zeta_F(s)$ be it Dedekind zeta function. Then, $\zeta_F(s)$ can be analytically continued to $\mathbb{C}\setminus\{1\}$, with a simple pole at $s = 1$. Moreover,*

$$\lim_{s\to 1^+}(s-1)\zeta_F(s) = \frac{2^{r_1}(2\pi)^{r_2} h_F R_F}{w_F\sqrt{|D_{F/\mathbb{Q}}|}}.$$

Here, r_1 = number of real embeddings of F, r_2 = number of pairs of complex embeddings of F, h_F = the class number of F, R_F = the regulator of F, w_F = number of roots of unity in F, and $D_{F/\mathbb{Q}}$ = the discriminant of F over $\mathbb{Q}$.

Dirichlet proved a special case of this formula in case of quadratic extensions of $\mathbb{Q}$. For a square-free d, let $F = \mathbb{Q}(\sqrt{d})$ with discriminant D_F. Let $\chi(m) = \left(\frac{d_F}{m}\right)$ be a Dirichlet character with L-series $L(s,\chi) = \sum_m \frac{\chi(m)}{m^s}$. If $d < 0$, then we denote w to be the number of roots of unity in F. If $d > 0$ and ε is the fundamental unit of F, then $R_F = \ln(\varepsilon)$ is the regulator of F. With these notations, *Dirichlet's class number formula* is given by

$$h_F = \begin{cases} \dfrac{w\sqrt{|D_F|}L(1,\chi)}{2\pi} & \text{if } d < 0, \\ \dfrac{\sqrt{|D_F|}L(1,\chi)}{2R_F} & \text{if } d > 0. \end{cases} \tag{1.10}$$

1.7.2 Kuroda-Kubota's class number formula

Genus formula and the analytic class number formula emphasize that the group of units in the ring of integers is a crucial ingredient in the study of class groups. Although

Dirichlet's unit theorem gives the structure of unit groups, the behaviour of units in relative extensions is non-trivial to identify. As an exception, *Kuroda-Kubota's class number formula* gives an idea on the fundamental system of units and the class number of totally real biquadratic extensions of $\mathbb{Q}$.

Theorem 1.7.8. ([49], [51], cf. [7]) *Let $L/\mathbb{Q}$ be a totally real biquadratic extension, with unit group $E(L)$. 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*

$$\#A(L) = \frac{1}{4} \cdot Q(L) \cdot \#A(L_1) \cdot \#A(L_2) \cdot \#A(L_3). \tag{1.11}$$

Further, the following are the possible systems of fundamental units of L under some numbering of the fields L_i.

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 ε_i that appears under the square-root is assumed to have norm equal to 1, except for the 7th case, where all of ε_i ($i = 1, 2, 3$) must have the same norm, either all 1, or all -1.

1.8 $\mathbb{Z}_\ell$-extension

We have already discussed the prevalence of $\mathbb{Z}_\ell$-extensions in various problems in the Introduction section. In this section, we emphasize some important results on such extensions.

Definition 1.8.1. *Let ℓ be a prime number and F be a number field. Then, we say that F_∞/F is a $\mathbb{Z}_\ell$-extension if $\Gamma := \mathrm{Gal}(F_\infty/F)$ is topologically isomorphic to the additive group of ℓ-adic integers $\mathbb{Z}_\ell$.*

Proposition 1.8.2. [80, Proposition 13.1] *Let F_∞/F be a $\mathbb{Z}_\ell$-extension of the number field F. Then, for each $n \geq 0$, there exists a unique field $F_n \subset F_\infty$ of degree ℓ^n over F. The fields F_n and F_∞ are the only intermediate extensions of F_∞/F.*

For each n, we call F_n the *n-th layer* of F_∞/F. In fact, F_n is the field fixed by Γ^{ℓ^n} with $\mathrm{Gal}(F_n/F) \cong \mathbb{Z}/\ell^n\mathbb{Z}$. We set $\Gamma_n = \mathrm{Gal}(F_n/F)$. Suppose γ is the topological generator of Γ, i.e., Γ is the closure of the group generated by γ. Then, γ induces an automorphism τ_n on F_n such that $\mathrm{Gal}(F_n/F)$ is generated by τ_n. Moreover, the associated topology in $\mathbb{Z}_\ell$ and results from local class field theory provide an insight on ramification in the extension F_∞/F.

Proposition 1.8.3. [80, Proposition 13.2, Lemma 13.3] *Let F_∞/F be a $\mathbb{Z}_\ell$-extension of F, and let $\mathfrak{p}$ (possibly infinite) be a prime in F that does not lie above ℓ. Then $\mathfrak{p}$, and the primes above $\mathfrak{p}$ remain unramified in F_∞/F. Only the prime(s) above ℓ can ramify in F_∞/F, and there exists $n \geq 0$ such that every ramified prime is totally ramified in F_∞/F_n.*

As we have already seen that there are relations among class numbers of fields in an extension, the question on growth of the class numbers of F_n is genuine. Let $A_\ell(F_n)$ be the ℓ-class group of F_n. Then, $A_\ell(F_n)$ becomes a module over the group ring $\mathbb{Z}_\ell[\Gamma_n]$. With respect to the projection maps from Γ_n to Γ_m for $n \geq m$, the *Iwasawa algebra* is defined as the completed $\mathbb{Z}_\ell$-group ring of Γ given by $\Lambda := \varprojlim_n \mathbb{Z}_\ell[\Gamma_n] = \mathbb{Z}_\ell[\![\Gamma]\!]$.

The power series ring $\mathbb{Z}_\ell[\![T]\!]$ is also isomorphic to Λ via the isomorphism $T \mapsto \gamma - 1$. This sometimes makes the perception of Λ as a ring easier.

The set $\{A_\ell(F_n) : n \geq 0\}$ forms an inverse system with respect to the norm maps $N_{n,m} : A_\ell(F_n) \to A_\ell(F_m)$ for $n \geq m$. Thus, the inverse limit

$$X(F_\infty) := \varprojlim_n A_\ell(F_n),$$

has a Λ-module structure, and is known as the *Iwasawa module*.

Due to the Artin map, $A(F_n)$ is isomorphic to $\mathrm{Gal}(L(F_n)/F_n)$ where $L(F_n)$ is the maximal unramified abelian ℓ-extension of F_n. Therefore, $X(F_\infty)$ can be treated as $\varprojlim_n \mathrm{Gal}(L(F_n)/F_n)$, which in turn is isomorphic to $\mathrm{Gal}(L(F_\infty)/F_\infty)$ (cf. [76, Proposition 3.2.6]). Here, $L(F_\infty)$ is the maximal abelian unramified pro-ℓ-extension of F_∞. This point of view of the Iwasawa module involves the aspects of ℓ-Hilbert class field of F_n. It turns

out that $X(F_\infty)$ is a finitely generated, and torsion Λ-module (cf. [76, Proposition 3.2.11]). Due to the structure theorem of finitely generated Λ-modules (cf. [80, Theorem 13.12]), Iwasawa was able to prove what is known today as Iwasawa's class number formula (Theorem 0.0.3).

1.8.1 Cyclotomic $\mathbb{Z}_\ell$-extension

The cyclotomic $\mathbb{Z}_\ell$-extension of a number field is one of the most commonly studied $\mathbb{Z}_\ell$-extensions. For $F = \mathbb{Q}$, and $\ell \neq 2$, the n-th layer $\mathbb{Q}_n$ is the unique subfield of degree ℓ^n in $\mathbb{Q}(\zeta_{\ell^{n+1}})/\mathbb{Q}$. Let $\mathbb{Q}_0 = \mathbb{Q}$ and $\mathbb{Q}_\infty := \bigcup_{n\geq 0} \mathbb{Q}_n$. Then, $\mathbb{Q}_\infty/\mathbb{Q}$ is known as the cyclotomic $\mathbb{Z}_\ell$-extension of $\mathbb{Q}$. For $\ell = 2$, $\mathbb{Q}_n$ is the maximal real subfield of $\mathbb{Q}(\zeta_{2^{n+2}})$ and the other definitions follow similarly. For an arbitrary number field F, F_∞ is given by the compositum of F and $\mathbb{Q}_\infty$.

When $\ell = 2$, for the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}$, the base layer is given by $\mathbb{Q}_0 = \mathbb{Q}$, and if $\mathbb{Q}_n = \mathbb{Q}(\sqrt{a_n})$, then $a_n = 2\cos(2\pi/2^{n+2})$, and $\mathbb{Q}_{n+1} = \mathbb{Q}(\sqrt{2+a_n})$. For instance, $\mathbb{Q}_0 = \mathbb{Q}$, $\mathbb{Q}_1 = \mathbb{Q}(\sqrt{2})$, and $\mathbb{Q}_2 = \mathbb{Q}(\sqrt{2+\sqrt{2}})$. For any quadratic field $F = \mathbb{Q}(\sqrt{d})$ where d is square-free and $d \neq 2$, we have, $F_1 = \mathbb{Q}(\sqrt{d}, \sqrt{2})$, $F_2 = \mathbb{Q}(\sqrt{d}, \sqrt{2+\sqrt{2}})$, and so on.

1.8.2 Nakayama's lemma and Fukuda's result on stability

Nakayama's lemma is one of the essential tools in Iwasawa theory particularly used to connect the ℓ-class groups $A_\ell(F_n)$. We now look at some of its equivalent statements.

Lemma 1.8.4. (Nakayama's Lemma) *Let R be a commutative ring with unity, and let M be a finitely generated R-module with group operation denoted by $+$. If $J(R)$ is the Jacobson radical of R and N is an R-submodule of M, then,*

$$M = N + J(R)M \text{ implies that } M = N.$$

We recall that $\Lambda \cong \mathbb{Z}_\ell[\![T]\!]$. Then, a version of Nakayama's lemma for modules over $\mathbb{Z}_\ell[\![T]\!]$ is given by:

1. *Let X be a compact $\mathbb{Z}_\ell[\![T]\!]$-module. Then, X is finitely generated over $\Lambda = \mathbb{Z}_\ell[\![T]\!]$ if and only if $X/\langle \ell, T\rangle$ is finite.*

2. *If $x_1, \ldots, x_r$ generate $X/\langle \ell, T\rangle$ over $\mathbb{Z}$, then their lifts in X generate X over Λ. In particular, $X/\langle \ell, T\rangle = 0$ if and only if $X = 0$.*

As an application of Nakayama's lemma, Fukuda derived a theorem on the stability of rank and order of ℓ-class groups in $\mathbb{Z}_\ell$-extension of number fields. By stability, we mean the eventual termination of growth of the order and rank of ℓ-class groups. Fukuda's result has been a key ingredient in many works that involves Greenberg's conjecture.

Theorem 1.8.5. [22, Theorem 1] *Let ℓ be a prime number. Let F be a number field and let F_∞/F be a $\mathbb{Z}_\ell$-extension of F. Let $n_0 \geq 0$ be an integer such that any prime of F_∞ which is ramified in F_∞/F is totally ramified in F_∞/F_{n_0}. Denote the n-th layer of F_∞/F by F_n and the ℓ-class group of F_n by $A_\ell(F_n)$. Then the following hold.*

1. *If there exists an integer $n \geq n_0$ such that $\#A_\ell(F_{n+1}) = \#A_\ell(F_n)$, then $\#A_\ell(F_m) = \#A_\ell(F_n)$ for all $m \geq n$. In particular, both the Iwasawa invariants $\mu(F_\infty/F)$ and $\lambda(F_\infty/F)$-invariants vanish.*

2. *If there exists an integer $n \geq n_0$ such that $\mathrm{rank}_\ell A_\ell(F_{n+1}) = \mathrm{rank}_\ell A_\ell(F_n)$, then $\mathrm{rank}_\ell A_\ell(F_m) = \mathrm{rank}_\ell A_\ell(F_n)$ for all $m \geq n$. In particular, the Iwasawa $\mu(F_\infty/F)$-invariant vanishes.*

1.9 Class field tower and Burnside's basis theorem

Apart from a $\mathbb{Z}_\ell$-extension, another interesting tower of number fields is formed by taking the chain of ℓ-Hilbert class fields. For a number field K and a prime ℓ, we set $K^{(0)} = K$ and define $K^{(i+1)}$ as the ℓ-Hilbert class field of the field $K^{(i)}$, for $i \geq 0$. This extension is known as the *ℓ-class field tower* of K. For each n, $K^{(n+1)}/K^{(n)}$ is an unramified abelian ℓ-extension. If $K^{(n+1)} = K^{(n)}$ for some n, then the tower is said to be finite, otherwise, it is infinite.

For a number field K, although its $\mathbb{Z}_\ell$-extension and its ℓ-class field tower are different, the Iwasawa module with respect to the $\mathbb{Z}_\ell$-extension is somewhat related to the ℓ-class field towers. If $L(K)$ is the ℓ-Hilbert class field and $\tilde{L}(K)$ is the maximal unramified ℓ-extension of K, then $K^{(0)} = K$, $K^{(1)} = L(K)$, and $\tilde{L}(K) = \bigcup_{n=0}^{\infty} K^{(n)}$. By definition,

$\mathrm{Gal}(L(K)/K)$ is the maximal abelian quotient of $\mathrm{Gal}(\tilde{L}(K)/K)$. Observing the same for the n-th layers K_n and passing on to the inverse limit, it can be observed that $X(K_\infty)$ is the maximal abelian quotient of $\mathrm{Gal}(\tilde{L}(K_\infty)/K_\infty) = \varprojlim_n \mathrm{Gal}(\tilde{L}(K_n)/K_n)$. This highlights the connection between Iwasawa modules and class field towers.

There is no known method to decide whether a 2-class field tower of a number field is finite or infinite. But in a special case, Burnside's basis theorem can help in concluding if an ℓ-class field tower terminates. Let G be an ℓ-group for a prime ℓ with commutator subgroup G' and Frattini subgroup $\phi(G)$. From Theorem 1.1.4, any lift of generators of $G/\phi(G)$ will generate G. If G is a pro-ℓ-group such that G/G' is procyclic, then so will $G/\phi(G)$ be. As a consequence of Burnside's basis theorem, this implies that G is procyclic. Applying this result on the ℓ-class field tower of K, we deduce that if $L(K)/K$ is a cyclic extension, then $\tilde{L}(K)/K$ is also cyclic, and hence, an abelian extension. This implies that $\tilde{L}(K) = L(K)$, and the ℓ-class field tower of K terminates at $L(K)$.

2

On the p-rationality of consecutive quadratic fields

2.1 Introduction

Let $p \geq 3$ be a prime number and K be a number field. Let M be the maximal p-ramified pro-p-extension of K with Galois group $\mathrm{Gal}(M/K)$. The field K is said to be p-rational if $\mathrm{Gal}(M/K)$ is a free pro-p-group. The notion of p-rationality was first introduced by Movaheddi (cf. [67]) in connection with the study of non-abelian number fields satisfying Leopoldt's conjecture.

Recently, the study of p-rationality of number fields resurfaced in connection with the work of Greenberg [36] on the construction of Galois extensions of $\mathbb{Q}$ with their Galois group isomorphic to an open subgroup of $GL_n(\mathbb{Z}_p)$. He proved that there exist continuous representations from the absolute Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ of $\mathbb{Q}$ to the general linear group $GL_n(\mathbb{Z}_p)$ for all integers $n \geq 4$, provided there exist p-rational multi-quadratic fields of

arbitrarily large degree. He made a precise conjecture regarding the existence of such fields as follows.

Conjecture 2.1.1. [36, Conjecture 4.8] *Let p be an odd prime number and let $t \geq 1$ be an integer. Then there exists a p-rational number field whose Galois group over $\mathbb{Q}$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^t$.*

Over the past few years, mathematicians have addressed Conjecture 2.1.1 for small values of t. In [6], Barbulescu and Ray proved that the quadratic field $\mathbb{Q}(\sqrt{p^2-1})$ is p-rational for all prime numbers p. In [8], Benmerieme and Movahhedi proved that for all prime $p \geq 5$, the quadratic fields $\mathbb{Q}(\sqrt{p(p+2)})$, $\mathbb{Q}(\sqrt{p(p-2)})$ and the biquadratic field $\mathbb{Q}(\sqrt{p(p+2)}, \sqrt{p(p-2)})$ are all p-rational. They also proved that $\mathbb{Q}(\sqrt{-1}, \sqrt{-3})$ is 3-rational. These results confirm Conjecture 2.1.1 for all odd primes p and for $t = 1$ and 2. Recently, Koperecz [46] addressed the case $t = 3$ and proved that the imaginary triquadratic field $\mathbb{Q}(\sqrt{p(p+2)}, \sqrt{p(p-2)}, \sqrt{-1})$ is p-rational for infinitely many primes p.

We consider the question of p-rationality for certain *consecutive* imaginary as well as real quadratic fields. For any $d \in \mathbb{Z}$, pairs of fields of the form $\mathbb{Q}(\sqrt{d})$, $\mathbb{Q}(\sqrt{d+1})$ are said to be consecutive quadratic fields. Similarly, for any $k \geq 1$, $\mathbb{Q}(\sqrt{d})$, $\mathbb{Q}(\sqrt{d+1}), \ldots, \mathbb{Q}(\sqrt{d+k})$ are said to be $k+1$-consecutive quadratic fields. The motivation for such consideration comes essentially from a recent conjecture of Iizuka [39] and various works centering that. We state Iizuka's conjecture as follows.

Conjecture 2.1.2. [39, Section 3] *Let ℓ be a prime number and let $k \geq 1$ be an integer. Then there exists an infinite family of quadratic fields, real or imaginary, of the form*

$$\mathbb{Q}(\sqrt{d}),\ \mathbb{Q}(\sqrt{d+1}), \ldots, \mathbb{Q}(\sqrt{d+k})$$

with $d \in \mathbb{Z}$ such that the class numbers of all of them are divisible by ℓ.

Iizuka [39] himself settled the conjecture for imaginary quadratic fields for $\ell = 3$ and $k = 1$. Recently, Conjecture 2.1.2 has been settled for $k = 1$ and for all primes ℓ in [48]. In the light of Conjecture 2.1.1 and Conjecture 2.1.2, we ask the following question.

Question 2.1.3. *For any given integer $k \geq 2$, do there exist infinitely many primes p for which there are k consecutive real or imaginary p-rational quadratic fields?*

We affirmatively answer Question 2.1.3 for imaginary quadratic fields by proving the following theorem.

Theorem 2.1.4. *For any integer $k \geq 1$, there exist infinitely many primes p such that the imaginary quadratic fields*

$$\mathbb{Q}(\sqrt{-(p-1)}), \ldots, \mathbb{Q}(\sqrt{-(p-k)})$$

are simultaneously p-rational. Also, there exist infinitely many primes p such that

$$\mathbb{Q}(\sqrt{-p(p-1)}), \ldots, \mathbb{Q}(\sqrt{-p(p-k)})$$

are all p-rational.

To address Question 2.1.3 for real quadratic fields, we prove the following theorem.

Theorem 2.1.5. *For sufficiently large primes p, the real quadratic field $\mathbb{Q}(\sqrt{p^2+1})$ is p-rational whenever p^2+1 is square-free. The same holds true for the real quadratic fields $\mathbb{Q}(\sqrt{p^2-2})$, $\mathbb{Q}(\sqrt{p^2+2})$, and $\mathbb{Q}(\sqrt{p^2+4})$ whenever the respective fundamental discriminants are square-free.*

Corollary 2.1.6. *There exist infinitely many prime numbers p such that all four real quadratic fields of Theorem 2.1.5 are simultaneously p-rational.*

Remark 2.1.7. *In [6], Barbulescu and Ray proved the p-rationality of $\mathbb{Q}(\sqrt{p^2-1})$ for all primes p. This, together with Theorem 2.1.5 and Corollary 2.1.6, provides us with pairs of real quadratic fields of the form $(\mathbb{Q}(\sqrt{p^2-2}), \mathbb{Q}(\sqrt{p^2-1}))$ and $(\mathbb{Q}(\sqrt{p^2+1}), \mathbb{Q}(\sqrt{p^2+2}))$ that are p-rational for infinitely many primes p. This affirmatively answers Question 2.1.3 for for $k=2$ and for real quadratic fields.*

2.2 Criteria for p-rationality

We begin with the following proposition due to Greenberg [36] to check for the p-rationality of abelian number fields.

Proposition 2.2.1. [36, Proposition 3.6] *Let p be a prime number and let K be an abelian*

number field such that the degree $[K : \mathbb{Q}]$ *is indivisible by* p*. Then* K *is* p*-rational if and only if every field* L *with* $\mathbb{Q} \subseteq L \subseteq K$ *and* $L/\mathbb{Q}$ *cyclic is* p*-rational.*

To deal with the p-rationality of quadratic fields, we recall the following criteria due to Greenberg [36].

Proposition 2.2.2. [36, Proposition 4.1] *Let* K *be a quadratic field and let* $p \geq 5$ *be a prime number.*

1. *If* K *is real, then it is* p*-rational if and only if* p *does not divide the class number* h_K *of* K *and the fundamental unit of* K *is not a* p^{th}*-power in the completion* $K_{\mathfrak{p}}$ *for some prime* $\mathfrak{p}$ *of* K *lying above* p*.*

2. *If* K *is imaginary, then* K *is* p*-rational if and only if the Hilbert* p*-class field of* K *is contained in the anti-cyclotomic* $\mathbb{Z}_p$*-extension of* K*. In particular,* K *is* p*-rational if* p *does not divide* h_K*.*

2.3 Consecutive imaginary quadratic p-rational fields

In view of Proposition 2.2.2, to prove Theorem 2.1.4, it is sufficient to prove that the class numbers of all the fields of Theorem 2.1.4 are indivisible by p. We accomplish this by using Louboutin's bound [56] for class numbers of imaginary quadratic fields for the aforementioned fields and showing that all of their discriminants have large square factors, which is essentially a modification of the arguments used in [46]. We state a proposition from [1] which will be used to produce infinitely many primes p with $p-1, \ldots, p-k$ simultaneously having large square factors.

Proposition 2.3.1. [1, Proposition 1] *Let* $m \geq 2$ *be an integer. Then there exists a polynomial* $f(X) = \prod_{i=1}^{m}(a_iX + b_i) \in \mathbb{Z}[X]$ *such that* $\gcd(b_i, b_j) = 1 = \gcd(a_ik + b_i, a_jk + b_j)$ *for all* $k \in \mathbb{Z}$ *and for all* $i, j \in \{1, \ldots, m\}$ *with* $i \neq j$*.*

Now, we prove the following proposition which plays a crucial role in the proof of Theorem 2.1.4. This is a generalization of Proposition 4 of [46].

Proposition 2.3.2. *For a given real number* $A > 0$ *and any given finitely many non-zero integers* $r_1, \ldots, r_s$*, there exist infinitely many prime numbers* p *such that* $p - r_i$ *has a square factor larger than* $(\log p)^A$ *for each* $i \in \{1, \ldots, s\}$*.*

Proof. Let $r = \prod_{i=1}^{s} r_i$ and let $\mathcal{P}$ be the set of all prime numbers dividing r. For an arbitrary but fixed positive integer m, by Proposition 2.3.1, there exist polynomials $f_i(X) = (a_iX + b_i) \in \mathbb{Z}[X]$ for each $i \in \{1, \ldots, m\}$ such that $\gcd(b_i, b_j) = 1$ and $\gcd(a_ik + b_i, a_jk + b_j) = 1$ for all $k \in \mathbb{Z}$ and $i \neq j$. Let $g_i(X) := f_i(rX) = a_irX + b_i$. Then for any $k \in \mathbb{Z}$, we have

$$\gcd(g_i(k), g_j(k)) = \gcd(f_i(rk), f_j(rk)) = 1 \text{ whenever } i \neq j.$$

Now, we notice that for any integer k, the fact $\gcd(g_i(k), r) = 1$ is equivalent to $\gcd(b_i, r) = 1$. We call $g_i(X)$ *admissible* if $\gcd(b_i, r) = 1$. Since $\gcd(b_i, b_j) = 1$ for $i \neq j$, we conclude that each $p \in \mathcal{P}$ divides b_i for at most one i. Consequently, there can be at most $\#\mathcal{P}$ many i for which $g_i(X)$ fails to be admissible. Since m is arbitrary, we can discard all the $g_i(X)$ that fail to be admissible and therefore the collection of the remaining $g_i(X)$ is admissible. In other words, we can find arbitrarily many finite number of linear polynomials $a_iX + b_i \in \mathbb{Z}[X]$ such that $\gcd(a_ik + b_i, a_jk + b_j) = 1$ for $i \neq j$ and $\gcd(a_ik + b_i, r) = 1$ for all $k \in \mathbb{Z}$.

Now, for an integer $v \geq 2$ and a sufficiently large X, we can choose integers $m_1, \ldots, m_s$ such that $\frac{1}{v}(\log X)^A \leq m_i \leq (\log X)^A$, $\gcd(m_i, r) = 1$ for all $i \in \{1, \ldots, s\}$, and for all $i \neq j$, $\gcd(m_i, m_j) = 1$. Now, by Chinese remainder theorem, the system of congruences

$$\begin{aligned} x &\equiv r_1 \pmod{m_1^2} \\ &\vdots \\ x &\equiv r_s \pmod{m_s^2} \end{aligned} \tag{2.1}$$

has a unique solution $\ell \pmod{D}$, where $D = \prod_{i=1}^{s} m_i^2 \leq (\log X)^c$.

Now, we proceed as in [46]. For large positive real number X and positive integers D and ℓ with $\gcd(D, \ell) = 1$, let $\pi(X, D, \ell) := \{p \in \mathbb{N} : p \geq 2 \text{ is prime and } p \equiv \ell \pmod{D}\}$. Then for a fixed real number $c > 0$, the estimate

$$\pi(X, D, \ell) = \frac{1}{\phi(D)} \int_2^X \frac{dt}{\log t} + O(Xe^{-c_1\sqrt{\log X}})$$

holds uniformly for all integers D and ℓ and $1 \leq D \leq (\log X)^c$ [19, Lemma 2.9].

Let $A > 0$ and let $c = 2sA + 1$. From the inequality $\pi(X, D, \ell) - \pi(\frac{X}{v}, D, \ell) > 0$ for an arbitrary but fixed integer $v \geq 2$, we conclude that there exist a prime $p \equiv \ell \pmod{D}$ with $\frac{X}{v} < p < X$ for sufficiently large X.

Now, we choose X suitably large enough so that there exists a prime number $p \in (\frac{X}{v}, X)$ and $p \equiv \ell \pmod{D}$. Then $p \equiv r_i \pmod{m_i^2}$ for all $i \in \{1, \ldots, s\}$. This completes the proof of the proposition. □

One way to prove that the class number h_K of the imaginary quadratic field K is indivisible by a prime p is to show that $h_K < p$. This motivates us to look for suitable upper bounds for the class numbers of imaginary quadratic fields and the following proposition of Louboutin [55] serves the desired purpose.

Proposition 2.3.3. [55, Proposition 2] *For an imaginary quadratic field K with discriminant d_K and class number h_K, we have*

$$h_K \leq \frac{\omega_K \cdot \sqrt{|d_K|}}{4\pi} \left(\log |d_K| + \frac{3}{2} \right),$$

where ω_K stands for the number of roots of unity in K.

2.3.1 Proof of Theorem 2.1.4

Proof. By Proposition 2.3.2, there exist infinitely many primes p such that $p - j$ has a divisor ℓ^2 such that $\ell > (\log p)^2$ for each $j \in \{1, \ldots, k\}$. Let $K_j := \mathbb{Q}(\sqrt{-(p-j)})$. Then the discriminant d_{K_j} of K_j satisfies the inequality

$$|d_{K_j}| \leq 4 \times \text{square-free part of } (p-j) \leq \frac{4(p-j)}{(\log p)^4}.$$

Therefore, by using Proposition 2.3.3, we obtain

$$h_{K_j} \leq \frac{\omega_{K_j}}{4\pi} \sqrt{\frac{4(p-j)}{(\log p)^4}} \left(\log \left(\frac{4(p-j)}{(\log p)^4} \right) + \frac{3}{2} \right). \tag{2.2}$$

Since $\omega_{K_j} = 2, 4$ or 6, we conclude from (2.2) that $h_{K_j} \ll \frac{\sqrt{p}}{\log p} \ll p$. Consequently, $h_{K_j} < p$ for sufficiently large primes p and therefore, p does not divide h_{K_j}. By Proposition 2.2.2, we conclude that each K_j is p-rational.

Similarly, we let $F_j := \mathbb{Q}(\sqrt{-p(p-j)})$. Then the discriminant d_{F_j} of F_j satisfies the inequality

$$|d_{F_j}| \leq 4 \times \text{square-free part of } p(p-j) \leq \frac{4p(p-j)}{(\log p)^4}.$$

Therefore, by using Proposition 2.3.3, we obtain

$$h_{F_j} \leq \frac{\omega_{F_j}}{4\pi}\sqrt{\frac{4p(p-j)}{(\log p)^4}}\left(\log\left(\frac{4p(p-j)}{(\log p)^4}\right)+\frac{3}{2}\right) \ll \frac{\sqrt{p(p-j)}}{\log p} \ll p. \tag{2.3}$$

Hence p does not divide h_{F_j} and thus by Proposition 2.2.2, we conclude that F_j is p-rational. This completes the proof of Theorem 2.1.4. □

2.4 Consecutive real quadratic p-rational fields

In view of Proposition 2.2.2, to establish the p-rationality of a real quadartic field K, it is required to prove that the fundamental unit is not a p^{th}-power in the completion $K_{\mathfrak{p}}$ for some prime $\mathfrak{p}$ of K lying above p. For that, let us recall the following proposition from [75].

Proposition 2.4.1. [75, Page 219, Proposition 9] *Let K be a complete field under a discrete valuation v and* $\text{char}(K) = 0$. *Assume that the residue field $\mathfrak{K}$ has* $\text{char}(\mathfrak{K}) = p \neq 0$. *Let $e = v(p)$ be the absolute ramification index of K. For an integer $m \geq 1$, let $U^{(m)} := \{x \in K : v(x-1) \geq m\}$. Then for $m > \frac{e}{p-1}$, the map $x \mapsto x^p$ is an isomorphism of $U^{(m)}$ onto $U^{(m+e)}$.*

2.4.1 Proof of Theorem 2.1.5

Proof. We give a complete proof for the field $K = \mathbb{Q}(\sqrt{p^2+1})$, assuming that p^2+1 is square-free. The proofs for other three fields follow similar line of argument.

We first prove that the fundamental unit ε is not a p^{th}-power in $K_{\mathfrak{p}}$. Since p is odd, $p^2+1 \equiv 2 \pmod 4$. Also, since p^2+1 is assumed to be square-free, we have $d_K = 4(p^2+1)$. Now, the continued fraction expansion of $\sqrt{p^2+1}$ is $[p, \overline{2p}]$ and hence the fundamental unit of K is $p+\sqrt{p^2+1}$.

Let $K_{\mathfrak{p}}$ be the completion of K with respect to a prime $\mathfrak{p} \subseteq \mathcal{O}_K$ lying above p. For

an integer $m \geq 1$, let $U_{\mathfrak{p}}^{(m)} = \{x \in K_{\mathfrak{p}} : x \equiv 1 \pmod{\mathfrak{p}^m \mathcal{O}_{K_{\mathfrak{p}}}}\}$. From the equation $\varepsilon^2 = 1 + 2p^2 + 2p\sqrt{p^2+1}$, we obtain that $\varepsilon^2 \in U_{\mathfrak{p}}^{(1)} \setminus U_{\mathfrak{p}}^{(2)}$. Since p is totally split in K, by using Proposition 2.4.1, we conclude that the map $x \mapsto x^p$ is an isomorphism from $U_{\mathfrak{p}}^{(1)}$ onto $U_{\mathfrak{p}}^{(2)}$. Now, if $\varepsilon^2 = \alpha^p$ for some $\alpha \in K_{\mathfrak{p}}$, then using $\varepsilon^2 \in U_{\mathfrak{p}}^{(1)}$ and $N(\mathfrak{p}) = p$, we get $1 \equiv \alpha^p \equiv \alpha \pmod{\mathfrak{p}\mathcal{O}_{K_{\mathfrak{p}}}}$. That is, $\alpha \in U_{\mathfrak{p}}^{(1)}$. Consequently, using the isomorphism $U_{\mathfrak{p}}^{(1)} \simeq U_{\mathfrak{p}}^{(2)}$, we see that $\varepsilon^2 = \alpha^p \in U_{\mathfrak{p}}^{(2)}$, which is a contradiction. Hence ε is not a p^{th}-power in $K_{\mathfrak{p}}$.

Next, we prove that the class number h_K is not divisible by p, for sufficiently large primes p. From Dirichlet's class number formula (Equation 1.10), we have $h_K = \dfrac{L(1,\chi_K)\sqrt{d_K}}{2R_K}$, where $R_K := \log(\varepsilon)$ is the regulator of K. Since 2 is ramified in K, it further leads to the following inequality [55, Corollary 2]

$$L(1,\chi_K) \leq \frac{\log d_K + \kappa_2}{4},$$

where $\kappa_2 := 2 + \gamma - \log(\pi) \sim 1.432\ldots$, and γ is the Euler's constant. Using $R_K = \log(p + \sqrt{p^2+1})$, we get the following inequality

$$\begin{aligned}
h_K &< \frac{(\log d_K + 2)}{4} \times \frac{\sqrt{d_K}}{2R_K} \\
&= \frac{\log(4(p^2+1)) + 2}{4} \times \frac{\sqrt{4(p^2+1)}}{2\log(p+\sqrt{p^2+1})} \\
&= \frac{\log(4(p^2+1)) + 2}{2} \times \frac{\sqrt{p^2+1}}{\log((p+\sqrt{p^2+1})^2)} \\
&= \frac{(\log(4(p^2+1)) + 2)\sqrt{p^2+1}}{2\log(p^2+p^2+1+2p\sqrt{p^2+1})} \\
&= \left(\frac{\log(4(p^2+1))}{2\log(2p^2+1+2p\sqrt{p^2+1})} + \frac{1}{\log(2p^2+1+2p\sqrt{p^2+1})}\right)\sqrt{p^2+1}.
\end{aligned}$$

Since $\sqrt{p^2+1} > p$, we obtain

$$\begin{aligned}
2\log(2p^2+1+2p\sqrt{p^2+1}) &> 2\log(2p^2+1+2p^2) \\
&= 2\log(4p^2+1) = \log((4p^2+1)^2) \\
&= \log(16p^4+8p^2+1).
\end{aligned}$$

Therefore, $h_K < \left(\dfrac{\log(4(p^2+1))}{\log(16p^4+8p^2+1)} + \dfrac{1}{\log(2p^2+1+2p\sqrt{p^2+1})} \right) \sqrt{p^2+1}$.
For sufficiently large p, the quantity inside the bracket becomes smaller than 1 and consequently, $h_K < p$, implying that p does not divide h_K for sufficiently large primes p. Therefore, $K = \mathbb{Q}(\sqrt{p^2+1})$ is p-rational whenever p^2+1 is square-free. Since by Proposition 2.4, there exist infinitely many primes p for which p^2+1 is square-free, we obtain the p-rationality for infinitely many such fields. The proofs for the other three families of quadratic fields follow similar lines of arguments. □

2.5 Square-free values of integral polynomials

The next proposition is due to Heath-Brown [37] and is about the square-free values of an integral polynomial at prime arguments. This plays an important role in the proof of Corollary 2.1.6 because it requires us to consider the simultaneous square-free values of certain quadratic polynomials. We recall it as follows.

Proposition 2.5.1. [37, Theorem 1.2] *Let $f(X) = X^d + c \in \mathbb{Z}[X]$ be irreducible and let $k \geq \frac{5d+3}{9}$ be an integer. Suppose that for every prime number p, there exists an integer n_p with $\gcd(p, n_p) = 1$ and $f(n_p) \not\equiv 0 \pmod{p^k}$. For a positive real number X, let $N'_{f,k}(X) := \{p \text{ prime } : p \leq X \text{ and } f(p) \text{ is } k\text{-free}\}$. Then for any fixed $A > 0$, the estimate*

$$N'_{f,k}(X) = \prod_p \left(1 - \frac{\rho'_f(p^k)}{\phi(p^k)}\right) \pi(X) + O_A\left(\frac{X}{(\log X)^A}\right) \tag{2.4}$$

holds and the implied constant depends on A. Here $\pi(X)$ stands for the number of primes up to X and $\rho'_f(d) := \#\{n \pmod d : \gcd(n,d) = 1 \text{ and } f(n) \equiv 0 \pmod d\}$.

Remark 2.5.2. *In Proposition 2.5.1, we immediately see that the hypotheses are satisfied for the particular choice $d = k = 2$ and $c = -2, 1, 2$ and 4. In that case, f is a quadratic polynomial and hence $\rho'_f(p^2) = 0$ or 2, depending on the appropriate congruence class of p modulo 8. In other words, $\rho'_f(p^2)$ is an absolute constant and $\phi(p^2) = p^2 - p$ is of the order of p^2 for large enough p. Thus the Euler product in (2.4) converges to a non-zero constant and hence the square-free values of the respective quadratic polynomials indeed have positive relative density in the set of prime numbers.*

Proof of Corollary 2.1.6

Proof. In the light of Theorem 2.1.5, it suffices to prove that there exist infinitely many prime numbers p, with positive lower relative density, such that all the integers p^2-2, p^2+1, p^2+2 and p^2+4 are simultaneously square-free. Let

$$A_1 := \{p \text{ prime } : p^2+1 \text{ is square-free }\},$$

$$A_2 := \{p \text{ prime } : p^2-2 \text{ is square-free }\},$$

$$A_3 := \{p \text{ prime } : p^2+2 \text{ is square-free }\},$$

$$A_4 := \{p \text{ prime } : p^2+4 \text{ is square-free }\}.$$

For a positive real number X, let $A_i(X) := \{p \in A_i : p \leq X\}$, for each $i = 1, 2, 3$ and 4. We prove that the set $\bigcap_{i=1}^{4} A_i$ has a positive lower relative density.

For each $i \in \{1,2,3,4\}$, let $\delta(A_i)$ denote the relative density of A_i in the set of all prime numbers. That is, $\delta(A_i) := \lim_{X\to\infty} \frac{\#A_i(X)}{\pi(X)}$. Then by Proposition 2.5.1, we conclude that $\delta(A_i)$ exists for each i. Now, for A_1, by Proposition 2.5.1, we have

$$\delta(A_1) = \prod_{p\equiv 1 \pmod 4} \left(1 - \frac{2}{p(p-1)}\right) > \prod_{k=1}^{\infty} \left(1 - \frac{2}{4k(4k+1)}\right) \geq 0.834.$$

Similarly, we obtain $\delta(A_2) \geq 0.931$, $\delta(A_3) \geq 0.920$ and $\delta(A_4) \geq 0.834$. Now, we obtain

$$\liminf_{X\to\infty} \frac{\#(A_1(X)\cap A_2(X))}{\pi(X)} \geq$$
$$\liminf_{X\to\infty} \frac{\#A_1(X)}{\pi(X)} + \liminf_{X\to\infty} \frac{\#A_2(X)}{\pi(X)} - \limsup_{X\to\infty} \frac{\#(A_1(X)\cup A_2(X))}{\pi(X)} \geq 0.834+0.931-1 = 0.765.$$

Similarly, proceeding as above, we obtain $\liminf_{X\to\infty} \frac{\#((A_1(X)\cap A_2(X))\cap A_3(X))}{\pi(X)} \geq 0.685$.

Finally, using the above estimate, we obtain $\liminf_{X\to\infty} \frac{\#\left(\bigcap_{i=1}^{4} A_i(X)\right)}{\pi(X)} \geq 0.519$. This completes the proof of the corollary. □

2.6 Biquadratic and triquadratic p-rational fields

For prime numbers $p > 3$ and positive integers α such that $\gcd(\alpha, p) = 1$, the totally real biquadratic field $K_\alpha := \mathbb{Q}(\sqrt{\alpha p(\alpha p + 2)}, \sqrt{\alpha p(\alpha p - 2)})$ has been mentioned towards the end of [8]. It has been explicitly written (at page number 15 of [8]) that "... *the fundamental unit of each subfield of K_α is not locally a p^{th} power at the p-adic places. So K_α is p-rational as soon as p does not divide h_{K_α}. Though there exist α such that $p \mid h_{K_\alpha}$ (for instance with $p = 5$ and $\alpha = 17$), it would be interesting to find an infinite family of integers α for which p does not divide h_{K_α}.*"

Here, we make an attempt to address a slight variant of this problem by using Proposition 2.3.2. Let $\alpha \geq 1$ be an integer. We notice that the quadratic subfields of K_α are precisely $K_1 := \mathbb{Q}(\sqrt{\alpha p(\alpha p + 2)})$, $K_2 := \mathbb{Q}(\sqrt{\alpha p(\alpha p - 2)})$ and $K_3 := \mathbb{Q}(\sqrt{(\alpha p - 2)(\alpha p + 2)})$. Then as in the system of congruences in (2.1), we may consider

$$\begin{cases} x \equiv 2\alpha^{-1} \pmod{m^2} \\ x \equiv -2\alpha^{-1} \pmod{n^2} \end{cases} \tag{2.5}$$

where m and n are integers suitably chosen in certain range of $\log X$ such that $\gcd(m, n) = \gcd(m, \alpha) = \gcd(n, \alpha) = 1$. This choice is possible because of Proposition 2.3.2. Dirichlet's theorem for primes in arithmetic progressions asserts that there exist infinitely many prime numbers p satisfying the system of congruence (2.5). In other words, there exist infinitely many prime numbers p such that both $\alpha p - 2$ and $\alpha p + 2$ have square divisors $> (\log p)^A$ for arbitrary but fixed constant $A > 0$.

Hence for those choices of prime numbers p, using Le's bound for class numbers of real quadratic fields (cf. [52, Theorem (a)]), we have

$$h_{K_1} \leq \frac{1}{2}\sqrt{d_{K_1}} \leq \frac{1}{2}\sqrt{\frac{\alpha p(\alpha p + 2)}{(\log p)^4}} \ll p.$$

Consequently, for sufficiently large such prime numbers p, we conclude that p does not divide h_{K_1}. Similarly, for h_{K_2} and h_{K_3}, we arrive at the same conclusion. Thus we have proved the following proposition.

Proposition 2.6.1. *For a given integer $\alpha \geq 1$, there exist infinitely many prime numbers p such that the bi-quadratic field K_α is p-rational.*

Moreover, by the concluding remarks in [46], we obtain the following corollary.

Corollary 2.6.2. *For a given integer $\alpha \geq 1$, there exist infinitely many prime numbers p such that the tri-quadratic field $K_\alpha(\sqrt{-1})$ is p-rational.*

By Proposition 4.4 of [8], we know that the bi-quadratic field $\mathbb{Q}(\sqrt{p(p+2)}, \sqrt{p(p-2)})$ is p-rational for all primes p. From this, another interesting thing to observe is the following proposition, which is in a similar spirit as that of Koperecz in [46].

Proposition 2.6.3. *Let $\alpha \geq 1$ be an integer. Then there exist infinitely many primes p such that the tri-quadratic field $F_\alpha := \mathbb{Q}(\sqrt{p(p+2)}, \sqrt{p(p-2)}, \sqrt{-\alpha})$ is p-rational.*

Proof. In view of Proposition 2.2.1, it suffices to establish the p-rationality of the quadratic subfields of F_α. Since the p-rationality is known for $\mathbb{Q}(\sqrt{p(p+2)}, \sqrt{p(p-2)})$ for all primes $p \geq 5$, we only need to check for the p-rationality of the imaginary quadratic fields $\mathbb{Q}(\sqrt{-\alpha})$, $\mathbb{Q}(\sqrt{-p\alpha(p+2)})$, $\mathbb{Q}(\sqrt{-p\alpha(p-2)})$ and $\mathbb{Q}(\sqrt{-\alpha(p-2)(p+2)})$. By Proposition 2.3.2, there exist infinitely many primes p such that $p-2$ and $p+2$ simultaneously have large square divisors. Therefore, proceeding as in the proof of Theorem 2.1.4, we obtain that p does not divide the respective class numbers for sufficiently large primes p. Since α is a fixed integer, we can choose $p > h_{\mathbb{Q}(\sqrt{-\alpha})}$ and hence $h_{\mathbb{Q}(\sqrt{-\alpha})}$ is indivisible by p. Thus all the quadratic subfields of F_α are p-rational. Consequently, F_α is p-rational. This completes the proof of the proposition. □

We furnish some values of the class numbers of the imaginary and real quadratic fields considered in Theorem 2.1.4 and Theorem 2.1.5 for certain values of the prime p. In the following tables, we use the notation $h(d)$ to denote the class number of $\mathbb{Q}(\sqrt{d})$. The computations of the class numbers have been carried out using MAGMA.

Table 2.1: Simultaneous p-rationality of $\mathbb{Q}(\sqrt{-(p-1)}), \ldots, \mathbb{Q}(\sqrt{-(p-5)})$.

p	$h(-(p-1))$	$h(-(p-2))$	$h(-(p-3))$	$h(-(p-4))$	$h(-(p-5))$
23	2	4	2	1	1
29	1	1	6	1	2
31	4	6	1	1	6
37	1	2	4	4	1
41	2	4	6	2	1
43	4	8	2	4	6
47	4	2	1	1	4
53	2	2	1	1	1
59	2	4	4	4	2
61	2	3	2	4	4

Table 2.2: Simultaneous p-rationality of $\mathbb{Q}(\sqrt{-p(p-1)}), \ldots, \mathbb{Q}(\sqrt{-p(p-5)})$.

p	$h(-p(p-1))$	$h(-p(p-2))$	$h(-p(p-3))$	$h(-p(p-4))$	$h(-p(p-5))$
7	4	2	1	4	4
13	4	10	4	2	6
17	4	12	8	16	2
29	4	6	20	6	12
31	24	14	8	4	28
37	2	36	12	32	10
53	40	28	6	6	10
59	52	16	12	48	16
71	56	16	18	52	56
79	40	24	24	12	76

3

Structure of 2-class groups in the $\mathbb{Z}_2$-extensions of certain real quadratic fields

3.1 Introduction

Let ℓ be a prime number and F be a number field with $\mathbb{Z}_\ell$-extension F_∞/F. The ℓ-rank $\text{rank}_\ell \mathcal{C}l_F$ of $\mathcal{C}l_F$ sheds light on the structures of the class groups and their growths in the infinite tower. For a quadratic extension of number fields K/F, with the class number h_F of F being odd, Gras [27] found the 2-rank of $\mathcal{C}l_K$ in certain cases by employing the Genus formulae. In [9], Bosma and Stevenhagen derived an algorithm to calculate the 2-class groups $A(K)$ (when $\ell = 2$), using quadratic forms. In the cases of quadratic and multi-quadratic fields, the fundamental units have been extensively employed to retrieve information about the order and rank of 2-class groups. We refer to [4], [5], [3], [11], [20], [31], [66], [64] and the references listed therein for more information about the same.

In this, and all the subsequent chapters, we use $A(F)$ to denote the 2-class group of

F. Using Fukuda's result together with genus theory, Mizusawa [57, Theorem 1] identified a class of real quadratic fields K with $A(K) \cong A(K_1) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, where K_1 is the first layer in the $\mathbb{Z}_2$-extension of K. Motivated by Mizusawa's work, we ask the following question.

Question 3.1.1. *Classify all the real quadratic fields $K = \mathbb{Q}(\sqrt{d})$ such that $A(K) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ and $\mathrm{rank}_2(A(K_1)) = 2$. In particular, characterize all the square-free integers $d > 0$ such that $A(K_1) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ and $\mathrm{rank}_2 A(K_n) = 2$ for all $n \geq 0$.*

In this chapter, we try to answer Question 3.1.1 by studying $K = \mathbb{Q}(\sqrt{d})$ and $K' = \mathbb{Q}(\sqrt{2d})$, where $d \geq 0$ is odd, square-free and has four distinct prime factors. We derive certain congruence conditions as well as Legendre symbol conditions on the prime factors of d, that provide us with an answer to Question 3.1.1. More precisely, we prove the following theorems.

Theorem 3.1.2. *Let $d \geq 1$ be a square-free integer, $K = \mathbb{Q}(\sqrt{d})$, $K' = \mathbb{Q}(\sqrt{2d})$ and $K_1 = \mathbb{Q}(\sqrt{2}, \sqrt{d})$. Assume that the places above $2\mathcal{O}_K$ are ramified in K_1. Then $\mathrm{rank}_2 A(K) = \mathrm{rank}_2 A(K_1) = 2$ and $\mathrm{rank}_2 A(K') = 3$ if and only if d is one of the following types.*

1. *$d = p_1p_2p_3$, where p_1, p_2 and p_3 are distinct primes with $p_1 \equiv 1$ or $5 \pmod 8$ and $p_2 \equiv p_3 \equiv 5 \pmod 8$.*
2. *$d = p_1p_2q_1q_2$, where p_1, p_2, q_1 and q_2 are distinct primes with $p_1 \equiv p_2 \equiv 5 \pmod 8$, $q_1 \equiv$ either 3 or $7 \pmod 8$ and $q_2 \equiv 3 \pmod 8$.*
3. *$d = q_1q_2q_3q_4$, where q_1, q_2, q_3 and q_4 are distinct primes with $q_1 \equiv 3$ or $7 \pmod 8$ and $q_2 \equiv q_3 \equiv q_4 \equiv 3 \pmod 8$.*

We note that for fields in Theorem 3.1.2, the ranks of the 2-class groups of the consecutive layers in the cyclotomic $\mathbb{Z}_2$-extension of K become equal. As a result, using Theorem 1.8.5, we derive the following corollary.

Corollary 3.1.3. *Let K be a real quadratic field as mentioned in Theorem 3.1.2. Then $\mathrm{rank}_2 A(K_n) = 2$ for all integers $n \geq 0$ and $\mathrm{rank}_2 A(K') = 3$.*

Our next two theorems deal with those real quadratic fields whose discriminants consist of at least one prime divisor that is congruent to 7 modulo 8. We state the theorems as follows.

Theorem 3.1.4. *Let $K = \mathbb{Q}(\sqrt{d})$ be a real quadratic field with $d = p_1p_2q_1q_2$, where p_1, p_2, q_1 and q_2 are distinct primes, $p_1 \equiv p_2 \equiv 5 \pmod 8, q_1 \equiv 7 \pmod 8, q_2 \equiv 3 \pmod 8$. Let $K' = \mathbb{Q}(\sqrt{2d})$ and $K_1 = \mathbb{Q}(\sqrt{2}, \sqrt{d})$. Then $A(K) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, $A(K') \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ and $A(K_1) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ if and only if one of the following choices of Legendre symbols holds.*

1. $\left(\frac{p_1}{p_2}\right) = -1, \left(\frac{p_1}{q_1}\right) = -1, \left(\frac{p_1}{q_2}\right) = 1, \left(\frac{q_1q_2}{p_2}\right) = 1,$
2. $\left(\frac{p_1}{p_2}\right) = -1, \left(\frac{q_1q_2}{p_1}\right) = 1, \left(\frac{p_2}{q_1}\right) = -1, \left(\frac{p_2}{q_2}\right) = 1,$
3. $\left(\frac{p_1}{p_2}\right) = 1, \left(\frac{p_1p_2}{q_1}\right) = -1, \left(\frac{p_1p_2}{q_2}\right) = -1, \left(\frac{p_1}{q_1}\right) = \left(\frac{p_2}{q_2}\right).$

Theorem 3.1.5. *Let $K = \mathbb{Q}(\sqrt{d})$ be a real quadratic number field with $d = q_1q_2q_3q_4$, where q_1, q_2, q_3 and q_4 are distinct primes with $q_1 \equiv 7 \pmod 8$, $q_2 \equiv q_3 \equiv q_4 \equiv 3 \pmod 8$. Let $K' = \mathbb{Q}(\sqrt{2d})$ and $K_1 = \mathbb{Q}(\sqrt{2}, \sqrt{d})$. Then $A(K) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, $A(K') \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ and $A(K_1) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ if one of the following choices of Legendre symbols holds:*

1. $\left(\frac{q_1}{q_3}\right) = \left(\frac{q_2}{q_3}\right) = \left(\frac{q_4}{q_2}\right) = \left(\frac{q_4}{q_1}\right) = 1, \left(\frac{q_4}{q_3}\right) = -1,$
2. $\left(\frac{q_1}{q_3}\right) = \left(\frac{q_2}{q_3}\right) = \left(\frac{q_4}{q_2}\right) = \left(\frac{q_4}{q_1}\right) = -1, \left(\frac{q_4}{q_3}\right) = 1,$
3. $\left(\frac{q_1q_2}{q_3}\right) = -1, \left(\frac{q_1q_2}{q_4}\right) = -1, \left(\frac{q_2}{q_3}\right) = \left(\frac{q_1}{q_4}\right) = \left(\frac{q_3}{q_4}\right),$
4. $\left(\frac{q_1q_2}{q_3}\right) = 1, \left(\frac{q_1q_2}{q_4}\right) = -1, \left(\frac{q_2}{q_3}\right) = \left(\frac{q_2}{q_4}\right), \left(\frac{q_1}{q_2}\right) = \left(\frac{q_4}{q_3}\right),$
5. $\left(\frac{q_1q_2}{q_3}\right) = -1, \left(\frac{q_1q_2}{q_4}\right) = 1, \left(\frac{q_2}{q_3}\right) = \left(\frac{q_1}{q_4}\right), \left(\frac{q_1}{q_2}\right) = \left(\frac{q_3}{q_4}\right),$
6. $\left(\frac{q_1}{q_3}\right) = \left(\frac{q_2}{q_3}\right) = 1, \left(\frac{q_1}{q_4}\right) = 1, \left(\frac{q_2}{q_4}\right) = -1, \left(\frac{q_1}{q_2}\right) = -1,$
7. $\left(\frac{q_1}{q_3}\right) = \left(\frac{q_2}{q_3}\right) = -1, \left(\frac{q_1}{q_4}\right) = -1, \left(\frac{q_2}{q_4}\right) = 1, \left(\frac{q_1}{q_2}\right) = 1, \left(\frac{q_3}{q_4}\right) = 1,$
8. $\left(\frac{q_1}{q_3}\right) = 1, \left(\frac{q_2}{q_3}\right) = -1, \left(\frac{q_1}{q_4}\right) = 1, \left(\frac{q_2}{q_4}\right) = 1, \left(\frac{q_1}{q_2}\right) = -1,$
9. $\left(\frac{q_1}{q_3}\right) = -1, \left(\frac{q_2}{q_3}\right) = 1, \left(\frac{q_1}{q_4}\right) = -1, \left(\frac{q_2}{q_4}\right) = -1, \left(\frac{q_1}{q_2}\right) = 1, \left(\frac{q_3}{q_4}\right) = -1.$

Remark 3.1.6. *The arguments used in the proofs of Theorem 3.1.4 and Theorem 3.1.5 are mostly similar. Hence, we furnish the proof only for Theorem 3.1.4.*

3.2 Ramified primes and the 2-rank

Remark 3.2.1. *Let $K = \mathbb{Q}(\sqrt{d})$ be a real quadratic field and assume that* rank $A(K) = 2$. *Since $A(\mathbb{Q})$ is trivial, the lifting map $j : A(\mathbb{Q}) \to A(K)$ is trivial. By Proposition 1.7.6, we obtain $\#A(K)^G = 2^2 = 4$ and by Equation (1.4) of Theorem 1.4.3, we have*

$$\#A(K)^G = \frac{\#A(\mathbb{Q}) \cdot 2^{t-1}}{\left[E(\mathbb{Q}) : E(\mathbb{Q}) \cap N_{K/\mathbb{Q}}(K^\times)\right]}. \tag{3.1}$$

Since $E(\mathbb{Q}) = \{-1, 1\}$, the denominator in (3.1) is either 1 or 2. As a result, we have $4 = \frac{2^{t-1}}{n}$ where $n = 1$ or 2. Therefore, $t = 3$ or 4.

We now prove a result that provides the norm of the fundamental unit of $\mathbb{Q}(\sqrt{d})$ where $d \geq 0$ is of a certain type.

Proposition 3.2.2. *Let $F = \mathbb{Q}(\sqrt{d})$ be a real quadratic field such that d is divisible by a prime factor congruent to* 3 (mod 4). *Then, $N_{F/\mathbb{Q}}(\varepsilon) = 1$, where ε is the fundamental unit of F.*

Proof. Let $r \equiv 3 \pmod 4$ be a prime divisor of d. Let $\varepsilon = \frac{a + b\sqrt{d}}{2}$ be the fundamental unit of F, where a and b are rational integers of same parity. On the contrary, if $N_{F/\mathbb{Q}}(\varepsilon) = -1$, then reading the equation $N_{F/\mathbb{Q}}(\varepsilon) = \frac{a^2 - db^2}{4} = -1$ modulo r, we obtain $a^2 \equiv -4 \pmod r$. This implies that -1 is a quadratic residue modulo r, which is impossible since $r \equiv 3 \pmod 4$. Therefore, $N_{F/\mathbb{Q}}(\varepsilon) = 1$. □

Once the 2-rank is known, knowing the 4-rank would take us closer to understanding the structure of the 2-class group.

Definition 3.2.3. *The 4-rank of a finite abelian group G is the 2-rank of the quotient group $2G/4G$.*

Clearly, an abelian 2-group G is 2-elementary if and only if $\#(2G/4G) = 1$, i.e., its 4-rank is equal to 0. For any number field F, the 2-class group $A(F)$ can be viewed as a quotient group of the narrow 2-class group $A^+(F)$. A theorem of Rédei and Reichardt (cf. [73], [58, Theorem 2.4]) connects the 4-rank of $A^+(F)$ to the number of ways of expressing D_F as the product of two factors satisfying certain criteria. Let $S_1(F)$ and $S_2(F)$ be the

sets of tuples (D_1, D_2) defined as follows:

$$\begin{aligned}
S_1(F) &:= \{(D_1, D_2) : |D_1| < |D_2|,\ D_F = D_1 D_2,\ D_i \equiv 0 \text{ or } 1 \pmod 4\},\\
T_1(F) &:= \{(D_1, D_2) \in S_1(F) : \chi_{D_1}(p) = 1 \text{ for all primes } p \text{ dividing } D_2\},\\
T_2(F) &:= \{(D_1, D_2) \in S_1(F) : \chi_{D_2}(p) = 1 \text{ for all prime } p \text{ dividing } D_1\},\\
S_2(F) &:= \{(1, D_F)\} \cup (T_1(F) \cap T_2(F)),
\end{aligned}$$

where $\chi_{D_i}(p) = \left(\frac{D_i}{p}\right)$ is the Kronecker symbol, for $i = 1$ and 2. We now state the result by Rédei and Reichardt.

Theorem 3.2.4. ([73], [58, Theorem 2.4]) *With the quantities defined above, we have*

$$\#S_1(F) = \#\left(A^+(F)/2A^+(F)\right) \quad \text{and} \quad \#S_2(F) = \#\left(2A^+(F)/4A^+(F)\right).$$

Remark 3.2.5. *We observe from Theorem 3.2.4 that $A^+(F)$ is 2-elementary if and only if $\#S_2(F) = 1$. Also in that case, we have $\#S_1(F) = \#A^+(F)$.*

Since $A(F)$ is a quotient of $A^+(F)$, if $A^+(F)$ is a 2-elementary group, then so is $A(F)$. The next proposition provides a sufficient condition for the converse to hold.

Proposition 3.2.6. *Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field, where that $d \geq 1$ is a square-free integer having a prime divisor which is congruent to 3 (mod 4). If $A(K)$ is 2-elementary, then so is $A^+(K)$.*

Proof. Assume that d is odd with the prime factorization $d = p_1 \cdots p_m \cdot q_1 \cdots q_n$, where $p_i \equiv 1 \pmod 4$ and $q_j \equiv 3 \pmod 4$. We first furnish the proof assuming that n is even. We observe that $-q_n = \dfrac{d}{\prod_{i=1}^{m} p_i \prod_{j=1}^{n-1}(-q_j)}$. From Theorem 1.3.3, we have

$$K_G^+ = \mathbb{Q}(\sqrt{d}, \sqrt{p_1}, \ldots, \sqrt{p_m}, \sqrt{-q_1}, \ldots, \sqrt{-q_{n-1}})$$

and

$$K_G = K_G^+ \cap \mathbb{R} = \mathbb{Q}(\sqrt{d}, \sqrt{p_1}, \ldots, \sqrt{p_m}, \sqrt{q_1 q_2}, \ldots, \sqrt{q_1 q_{n-1}}).$$

Consequently, $[K_G : K] = 2^{m+n-2}$ and $[K_G^+ : K_G] = 2$. Due to Theorem 1.3.4 $\mathrm{Gal}(K_G/\mathbb{Q})$ is 2-elementary and by Remark 1.3.6, $\mathrm{rank}_2 A(K) = \mathrm{rank}_2 \mathrm{Gal}(K_G/K) = m+n-2$. According

to our hypothesis, $A(K)$ is 2-elementary and therefore, $A(K) \cong \bigoplus_{m+n-2} \mathbb{Z}/2\mathbb{Z}$. Hence, $[L(K) : K] = 2^{m+n-2} = [K_G : K]$, where $L(K)$ is the 2-Hilbert class field of K. Thus, $L(K) = K_G$.

Since $d \geq 1$ is square-free, our assumption and Proposition 3.2.2 yield $N_{K/\mathbb{Q}}(\varepsilon) = 1$. By Theorem 1.3.1, we have $\#Cl_K^+ = 2 \times \#Cl_K$ and thus, $\#A^+(K) = 2 \times \#A(K) = 2^{m+n-1} = [L^+(K) : K]$. This indicates that $L^+(K)$ (which is contained in the narrow Hilbert class field of K) whose Galois group over K corresponds to $A^+(K)$, and K_G^+ have the same degree over K. Once again, we obtain $L^+(K) = K_G^+$. Since $\mathrm{Gal}(K_G^+/K)$ is 2-elementary, therefore $A^+(K) = \mathrm{Gal}(L^+(K)/K)$ must be 2-elementary.

The proof becomes simpler when n is odd as it does not require expressing q_n in terms of d and other prime factors of d, and only the definition of genus (narrow genus) field is sufficient. A similar line of argument also holds when 2 divides d. □

Azizi and Mouhib [4], and subsequently Mizusawa [58] established a criterion for the 2-rank of the ideal class group of totally real biquadratic fields of the type $\mathbb{Q}(\sqrt{2}, \sqrt{d})$. This enables us to calculate the 2-rank of $A(K_1)$.

Theorem 3.2.7. ([4], [58, Theorem 2.7]) *Let $K = \mathbb{Q}(\sqrt{d})$ be a real quadratic field where $d \geq 1$ is an odd square-free integer. Let t_1 be the number of places of $\mathbb{Q}(\sqrt{2})$ ramified in $K_1 = \mathbb{Q}(\sqrt{2}, \sqrt{d})$, and let r_1 be the 2-rank of $A(K_1)$. Then the following hold.*

1. *If d has a prime factor congruent to $3 \pmod 4$, then either $r_1 = t_1 - 2$ or $r_1 = t_1 - 3$. In particular, $r_1 = t_1 - 2$ holds if and only if d has no prime factor which is congruent to $7 \pmod 8$.*

2. *If d has no prime factor congruent to $3 \pmod 4$, then either $r_1 = t_1 - 1$ or $r_1 = t_1 - 2$. In particular, $r_1 = t_1 - 1$ holds if and only if d has no prime factor p such that $p \equiv 1 \pmod 8$ and $2^{\frac{p-1}{4}} \not\equiv (-1)^{\frac{p-1}{8}} \pmod p$.*

We now prove a result that asserts the existence of infinitely many rational primes in prescribed arithmetic progressions satisfying any given set of conditions on the Legendre symbols. This will be quite useful to us in subsequent chapters as it ensures the existence of infinitely many number fields of certain kinds.

Proposition 3.2.8. *Let $t \geq 1$ be an integer. Assume that for each $i \in \{1, \ldots, t\}$, we are given integers $a_i \in \{1, 3, 5, 7\}$, and for each $1 \leq j < k \leq t$, the integers $\varepsilon_{kj} \in \{\pm 1\}$ are specified. Then there exist infinitely many t-tuples $\{p_1, \ldots, p_t\}$ of prime numbers such that $p_i \equiv a_i \pmod 8$ and the Legendre symbol $\left(\frac{p_k}{p_j}\right)$ equals ε_{kj}.*

Proof. We prove this by induction on t. For $t = 2$, we assume that $p_1 \equiv a_1 \pmod 8$ is given. We wish to find $p_2 \equiv a_2 \pmod 8$ such that $\left(\frac{p_2}{p_1}\right) = \varepsilon_{21}$. Let $1 \leq v \leq p_1 - 1$ be an integer such that $\left(\frac{v}{p_1}\right) = \varepsilon_{21}$. Consider the system of congruences

$$\begin{aligned} X &\equiv a_2 \pmod 8 \\ X &\equiv v \pmod{p_1}. \end{aligned}$$

Then by the Chinese Remainder Theorem (Theorem 1.1.5), there exists a unique solution $x_0 \pmod{8p_1}$ to this system. Therefore, $\gcd(x_0, 8p_1) = 1$ and consequently, by Dirichlet's theorem for primes in an arithmetic progression (Theorem 1.1.8), there exist infinitely many primes $\ell \equiv x_0 \pmod{8p_1}$. Then $\ell \equiv x_0 \equiv a_2 \pmod 8$ and $\left(\frac{\ell}{p_1}\right) = \left(\frac{x_0}{p_1}\right) = \left(\frac{v}{p_1}\right) = \varepsilon_{21}$. Thus the statement holds true for $t = 2$.

Now, we assume that the proposition holds true for $t - 1$. That is, for given integers $a_i \in \{1, 3, 5, 7\}$, $1 \leq i \leq t - 1$ and given integers $\varepsilon_{kj} \in \{\pm 1\}$ with $j < k$, there exist infinitely many $(t-1)$-tuples $\{p_1 \ldots p_{t-1}\}$ of rational primes satisfying the hypotheses of the proposition. Now, for a given integer $a_t \in \{1, 3, 5, 7\}$ and given integers $\varepsilon_{tk} \in \{\pm 1\}$ for $k \in \{1, \ldots, t-1\}$, let us consider the following system of congruences:

$$\begin{aligned} X &\equiv a_t \pmod 8 \\ X &\equiv v_1 \pmod{p_1} \\ &\vdots \\ X &\equiv v_{t-1} \pmod{p_{t-1}}, \end{aligned}$$

where $p_1, \ldots, p_{t-1}$ is a $(t-1)$-tuple of prime numbers satisfying the induction hypothesis and $1 \leq v_j \leq p_j - 1$ are such that $\left(\frac{v_j}{p_j}\right) = \varepsilon_{tj}$. Again by the Chinese Remainder Theorem, this system has a unique solution $y_0 \pmod{8p_1 \cdots p_{t-1}}$. Since $\gcd(y_0, 8p_1 \cdots p_{t-1}) = 1$, by Dirichlet's theorem for primes in an arithmetic progression, we have infinitely many primes

$\ell \equiv y_0 \pmod{8p_1 \cdots p_{t-1}}$. Then $\ell \equiv y_0 \equiv a_t \pmod 8$ and $\left(\frac{\ell}{p_j}\right) = \left(\frac{y_0}{p_j}\right) = \left(\frac{v_j}{p_j}\right) = \varepsilon_{tj}$. This completes the proof of the proposition. □

Remark 3.2.9. *In view of Proposition 3.2.8, we see that there are infinitely many tuples of prime numbers satisfying the required Legendre symbol conditions of Theorem 3.1.2, Theorem 3.1.4 and Theorem 3.1.5.*

3.2.1 Proof of Theorem 3.1.2

Proof. Let $K = \mathbb{Q}(\sqrt{d})$ be a real quadratic field. First, we assume that $\text{rank}_2 A(K) = \text{rank}_2 A(K_1) = 2$ and $\text{rank}_2 A(K') = 3$. By Remark 3.2.1, the discriminant D_K can have either 3 or 4 prime factors. Among the odd prime divisors of D_K, let p_i denote those rational primes that are congruent to 1 (mod 4) and let q_j denote the ones that are congruent to 3 (mod 4). We now enlist the suitable choices of d in Table 3.1 and Table 3.2.

Table 3.1: Possibilities of K when $t = 3$

Ramified primes	$K = \mathbb{Q}(\sqrt{d})$	$d \pmod 4$	$D(K)$
$2, p_1, p_2$	$\mathbb{Q}(\sqrt{2p_1p_2})$	2	$8p_1p_2$
$2, p_1, q_1$	$\mathbb{Q}(\sqrt{p_1q_1})$	3	$4p_1q_1$
$2, p_1, q_1$	$\mathbb{Q}(\sqrt{2p_1q_1})$	2	$8p_1q_1$
$2, q_1, q_2$	$\mathbb{Q}(\sqrt{2q_1q_2})$	2	$8q_1q_2$
p_1, p_2, p_3	$\mathbb{Q}(\sqrt{p_1p_2p_3})$	1	$p_1p_2p_3$
p_1, q_1, q_2	$\mathbb{Q}(\sqrt{p_1q_1q_2})$	1	$p_1q_1q_2$

Table 3.2: Possibilities of K when $t = 4$

Ramified primes	$K = \mathbb{Q}(\sqrt{d})$	$d \pmod 4$	$D(K)$
$2, p_1, p_2, p_3$	$\mathbb{Q}(\sqrt{2p_1p_2p_3})$	2	$8p_1p_2p_3$
$2, p_1, p_2, q_1$	$\mathbb{Q}(\sqrt{p_1p_2q_1})$	3	$4p_1p_2q_1$
$2, p_1, p_2, q_1$	$\mathbb{Q}(\sqrt{2p_1p_2q_1})$	2	$8p_1p_2q_1$
$2, p_1, q_1, q_2$	$\mathbb{Q}(\sqrt{2p_1q_1q_2})$	2	$8p_1q_1q_2$
$2, q_1, q_2, q_3$	$\mathbb{Q}(\sqrt{q_1q_2q_3})$	3	$4q_1q_2q_3$
$2, q_1, q_2, q_3$	$\mathbb{Q}(\sqrt{2q_1q_2q_3})$	2	$8q_1q_2q_3$
p_1, p_2, p_3, p_4	$\mathbb{Q}(\sqrt{p_1p_2p_3p_4})$	1	$p_1p_2p_3p_4$
p_1, p_2, q_1, q_2	$\mathbb{Q}(\sqrt{p_1p_2q_1q_2})$	1	$p_1p_2q_1q_2$
q_1, q_2, q_3, q_4	$\mathbb{Q}(\sqrt{q_1q_2q_3q_4})$	1	$q_1q_2q_3q_4$

We observe that the genus field K_G for $K = \mathbb{Q}(\sqrt{2p_1q_1})$ is $\mathbb{Q}(\sqrt{2p_1q_1}, \sqrt{p_1})$. Therefore, $\text{Gal}(K_G/K) \cong \mathbb{Z}/2\mathbb{Z}$. Thus, $\text{rank}_2 A(K) = 1$, which is not of our interest. The

same happens with $\mathbb{Q}(\sqrt{p_1q_1})$ and $\mathbb{Q}(\sqrt{p_1q_1q_2})$ as well. Similarly, the genus field of $K = \mathbb{Q}(\sqrt{p_1p_2p_3p_4})$ is $\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3}, \sqrt{p_4})$ and $\text{rank}_2A(K) = 3$. We restrict ourselves to only those K where the prime above 2 gets ramified in K_1/K. Thus we discard the fields $K = \mathbb{Q}(\sqrt{2p_1p_2}), \mathbb{Q}(\sqrt{2q_1q_2}), \mathbb{Q}(\sqrt{2p_1p_2p_3})$, and $\mathbb{Q}(\sqrt{2p_1q_1q_2})$. In [58] and [57], Mizusawa has covered the fields $\mathbb{Q}(\sqrt{q_1q_2q_3}), \mathbb{Q}(\sqrt{2q_1q_2q_3}), \mathbb{Q}(\sqrt{p_1p_2q_1})$, and $\mathbb{Q}(\sqrt{2p_1p_2q_1})$. Therefore, we are left only with the fields $\mathbb{Q}(\sqrt{p_1p_2q_1q_2})$, $\mathbb{Q}(\sqrt{q_1q_2q_3q_4})$ and $\mathbb{Q}(\sqrt{p_1p_2p_3})$. Now, we assume that $\text{rank}_2A(K_1) = 2$ to find more information about the primes p_i's and q_j's.

Let $K = \mathbb{Q}(\sqrt{p_1p_2q_1q_2})$. Since $d \equiv 1 \pmod 4$, the place above 2 is unramified in K but it is ramified in $\mathbb{Q}(\sqrt{2})$. Since ramification index is multiplicative in a tower of number fields, we conclude that the place above the rational prime 2 in $\mathbb{Q}(\sqrt{2})$ must be unramified in K_1. We now appeal to the Case 1 of Theorem 3.2.7, and taking $r_1 = \text{rank}_2A(K_1) = 2$, we consider the following cases.

Case 1. $r_1 = t_1 - 2$. In this case, d must not have a prime factor congruent to 7 (mod 8). This gives us that $q_1 \equiv q_2 \equiv 3 \pmod 8$. Also, $t_1 = 4$ implies that exactly 4 places of $\mathbb{Q}(\sqrt{2})$ must be ramified in K_1. Since $q_1 \equiv q_2 \equiv 3 \pmod 8$, the primes above q_1 and q_2 must be inert in $\mathbb{Q}(\sqrt{2})$. Thus, there is exactly one prime in $\mathbb{Q}(\sqrt{2})$ lying above q_j $(j = 1, 2)$ which must be ramified in K_1. Now if for some i, $p_i \equiv 1 \pmod 8$, then p_i be must totally split in $\mathbb{Q}(\sqrt{2})$. This contributes two places above p_i, making the total number of places in $\mathbb{Q}(\sqrt{2})$ ramified in K_1 at least 5, which is not possible. Hence $p_1 \equiv p_2 \equiv 5 \pmod 8$. Combining all these, we get $p_1 \equiv p_2 \equiv 5 \pmod 8$, $q_1 \equiv q_2 \equiv 3 \pmod 8$.

Case 2. $r_1 = t_1 - 3$. In this case, $t_1 = 5$ and hence, at least one of the q_j's must be congruent to 7 (mod 8). If $q_j \equiv 7 \pmod 8$, then it must be totally split in $\mathbb{Q}(\sqrt{2})$, creating two places above q_j. Each p_i contributes at least one place above itself that is ramified in K_1. Since the total number of ramified primes is exactly five, we conclude that $p_1 \equiv p_2 \equiv 5 \pmod 8, q_1 \equiv 7 \pmod 8, q_2 \equiv 3 \pmod 8$.

On the similar lines, we find that for $K = \mathbb{Q}(\sqrt{q_1q_2q_3q_4})$, $\text{rank}_2A(K) = 2$, $\text{rank}_2A(K') = 3$ and for $\text{rank}_2A(K_1) = 2$ to hold, we need to have either $q_1 \equiv q_2 \equiv q_3 \equiv q_4 \equiv 3 \pmod 8$ or $q_1 \equiv 7 \pmod 8$, $q_2 \equiv q_3 \equiv q_4 \equiv 3 \pmod 8$.

For the field $K = \mathbb{Q}(\sqrt{p_1p_2p_3})$, we follow a similar line of argument to obtain $p_1 \equiv p_2 \equiv p_3 \equiv 5 \pmod 8$ or $p_1 \equiv 1 \pmod 8$, $p_2 \equiv p_3 \equiv 5 \pmod 8$.

We prove the converse part only for $p_i \equiv 5 \pmod 8$ and $q_j \equiv 3 \pmod 8$ as the remaining cases follow similarly. In this case, we observe that the narrow genus field is given by

$$K_G^+ = \mathbb{Q}(\sqrt{p_1p_2q_1q_2}, \sqrt{p_1}, \sqrt{p_2}, \sqrt{-q_1}, \sqrt{-q_2}) = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{-q_1}, \sqrt{-q_2}).$$

Hence we obtain the genus field $K_G = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{q_1q_2})$, $\mathrm{Gal}(K_G/K) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, and $\mathrm{rank}_2 A(K) = 2$. Likewise, we find that for the field K', its genus field K'_G is given by $\mathbb{Q}(\sqrt{2}, \sqrt{p_1}, \sqrt{p_2}, \sqrt{q_1q_2})$ and $\mathrm{rank}_2 A(K') = 3$. Again, by using Theorem 3.2.7, we conclude that $\mathrm{rank}_2 A(K_1) = 2$. This completes the proof of Theorem 3.1.2. □

Proof of Corollary 3.1.3

Proof. For each of the fields mentioned in Theorem 3.1.2, the prime above the rational prime 2 is unramified in K. Hence, the prime above $2\mathcal{O}_K$ is ramified in the extension K_1/K. Since $[K_1 : K] = 2$, the prime above $2\mathcal{O}_K$ is totally ramified. Let $K_n = K\mathbb{Q}_n$ be the n^{th} layer in the cyclotomic $\mathbb{Z}_2$-extension of K. In the tower $\mathbb{Q}_0 = \mathbb{Q} \subset \mathbb{Q}_1 \subset \cdots \subset \mathbb{Q}_n \subset K_n$, we see that the prime above 2 is ramified with ramification degree 2 in each extension $\mathbb{Q}_i/\mathbb{Q}_{i-1}$ for $i = 1, \ldots, n$ and it is unramified in $K_n/\mathbb{Q}_n$. This proves that 2 is totally ramified in the extension K_n/K for any $n \in \mathbb{N}$. Since 2 is the only prime that is ramified in the $\mathbb{Z}_2$-extension K_∞/K and it is totally ramified in each extension K_n/K, it is totally ramified in K_∞/K.

Using Theorem 3.1.2 and Theorem 1.8.5, we conclude that $\mathrm{rank}_2 A(K) = \mathrm{rank}_2 A(K_1) = 2$ entails $\mathrm{rank}_2(A_n) = 2$ for all $n \geq 0$. This completes the proof of the corollary. □

3.2.2 Proof of Theorem 3.1.4

Proof. Let us consider $K = \mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{p_1p_2q_1q_2})$ with $p_1 \equiv p_2 \equiv 5 \pmod 8$, $q_1 \equiv 7 \pmod 8$ and $q_2 \equiv 3 \pmod 8$. Since d has prime factors that are congruent to 3 (mod 4), using Proposition 3.2.6, $A(K)$ is 2-elementary if and only if $A^+(K)$ is 2-elementary. Also, we have

$$S_1(K) = \{(1, p_1p_2q_1q_2), (p_1, p_2q_1q_2), (p_2, p_1q_1q_2), (-q_1, -p_1p_2q_2), (-q_2, -p_1p_2q_1), (p_1p_2, q_1q_2),$$
$$(-p_1q_1, -p_2q_2), (-p_2q_1, -p_1q_2)\}.$$

We note that the order of the appearance of the terms in any of the above pairs can be rearranged depending on which one is bigger in terms of the absolute value. We consider the following table (cf. Table 3.3) where we list all possible Kronecker symbols corresponding to each pair in order to appeal to Theorem 3.2.4.

Table 3.3: Kronecker symbols corresponding to each element in $S_1(K)$

Sr. No.	Tuple	Kronecker Symbols
1	$(p_1, p_2q_1q_2)$	$\left(\frac{p_1}{p_2}\right), \left(\frac{p_1}{q_1}\right), \left(\frac{p_1}{q_2}\right), \left(\frac{p_2q_1q_2}{p_1}\right)$
2	$(p_2, p_1q_1q_2)$	$\left(\frac{p_2}{p_1}\right), \left(\frac{p_2}{q_1}\right), \left(\frac{p_2}{q_2}\right), \left(\frac{p_1q_1q_2}{p_2}\right)$
3	$(-q_1, -p_1p_2q_2)$	$\left(\frac{-q_1}{p_1}\right), \left(\frac{-q_1}{p_2}\right), \left(\frac{-q_1}{q_2}\right), \left(\frac{-p_1p_2q_2}{q_1}\right)$
4	$(-q_2, -p_1p_2q_1)$	$\left(\frac{-q_2}{p_1}\right), \left(\frac{-q_2}{p_2}\right), \left(\frac{-q_2}{q_1}\right), \left(\frac{-p_1p_2q_1}{p_2}\right)$
5	(p_1p_2, q_1q_2)	$\left(\frac{p_1p_2}{q_1}\right), \left(\frac{p_1p_2}{q_2}\right), \left(\frac{q_1q_2}{p_1}\right), \left(\frac{q_1q_2}{p_2}\right)$
6	$(-p_1q_1, -p_2q_2)$	$\left(\frac{-p_1q_1}{p_2}\right), \left(\frac{-p_1q_1}{q_2}\right), \left(\frac{-p_2q_2}{p_1}\right), \left(\frac{-p_2q_2}{q_1}\right)$
7	$(-p_1q_2, -p_2q_1)$	$\left(\frac{-p_1q_2}{p_2}\right), \left(\frac{-p_1q_2}{q_1}\right), \left(\frac{-p_2q_1}{p_1}\right), \left(\frac{-p_2q_1}{q_2}\right)$

For $\#S_2(K)$ to be equal to 1, we require at least one entry in each row of Table 3 to be equal to -1. By considering the combinations of the Legendre symbols $\left(\frac{p_i}{q_j}\right)$, we find that any of the following conditions are necessary and sufficient for $\#S_2(K) = 1$ to hold.

1. $\left(\frac{p_1}{p_2}\right) = -1$ and $\left(\frac{q_1q_2}{p_1}\right) = -1$,
2. $\left(\frac{p_1}{p_2}\right) = -1$, $\left(\frac{q_1q_2}{p_1}\right) = 1$ and $\left(\frac{q_1q_2}{p_2}\right) = -1$,
3. $\left(\frac{p_1}{p_2}\right) = 1$, $\left(\frac{q_1q_2}{p_1}\right) = -1$ and $\left(\frac{q_1q_2}{p_2}\right) = -1$.

Therefore, when any one of the above Legendre symbol conditions occurs, we have $\#S_2(K) = 1$ and consequently, $A^+(K)$ is 2-elementary. This implies that $\#S_1(K) = \#A^+(K) = 8$ and $A(K) \cong \mathbb{Z}/2Z \oplus \mathbb{Z}/2\mathbb{Z}$. But we simultaneously require $A(K') \cong \mathbb{Z}/2Z \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. As $D_{K'} = 8p_1p_2q_1q_2$, we see that $\#S_1(K') = 16$. Out of the Legendre symbols obtained above, we see that $\#S_2(K') = 1$ if and only if one of the following holds.

1. $\left(\frac{p_1}{p_2}\right) = -1$, $\left(\frac{p_1}{q_1}\right) = -1$, $\left(\frac{p_1}{q_2}\right) = 1$, $\left(\frac{q_1q_2}{p_2}\right) = 1$,

2. $\left(\frac{p_1}{p_2}\right) = -1, \left(\frac{q_1q_2}{p_1}\right) = 1, \left(\frac{p_2}{q_1}\right) = -1, \left(\frac{p_2}{q_2}\right) = 1,$
3. $\left(\frac{p_1}{p_2}\right) = 1, \left(\frac{p_1p_2}{q_1}\right) = -1, \left(\frac{p_1p_2}{q_2}\right) = -1, \left(\frac{p_1}{q_1}\right) = \left(\frac{p_2}{q_2}\right).$

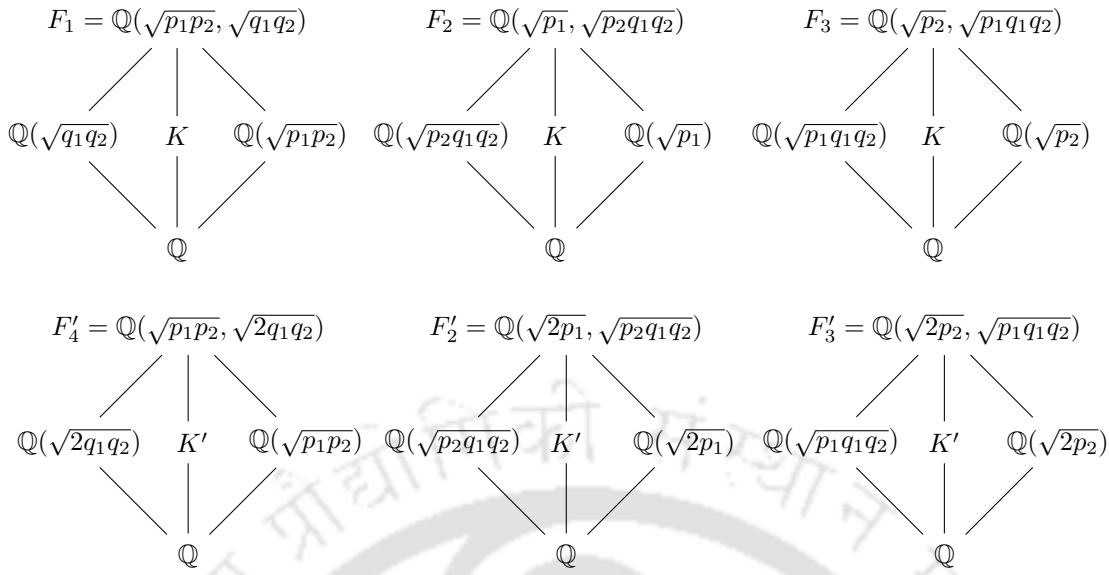
We prove the theorem only for the first set of Legendre symbol conditions because all other cases follow a similar line of argument. We first find the decomposition fields for places in K lying above the rational primes $2, p_1, p_2, q_1$ and q_2 with respect to the extension $L(K)/K$. We try to find the decomposition field of each prime by incorporating Proposition 1.2.10. For that, we first look at the biquadratic extensions F_i of $\mathbb{Q}$ such that $\mathbb{Q} \subseteq K \subseteq F_i \subseteq L(K)$. Since $L(K) = K_G = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{q_1q_2})$, we find that

$$F_1 := \mathbb{Q}(\sqrt{p_1p_2}, \sqrt{q_1q_2}), F_2 := \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2q_1q_2}), \text{ and } F_3 := \mathbb{Q}(\sqrt{p_2}, \sqrt{p_1q_1q_2}).$$

Similarly for $K' = \mathbb{Q}(\sqrt{2p_1p_2q_1q_2})$, $L(K') = \mathbb{Q}(\sqrt{2p_1p_2q_1q_2}, \sqrt{p_1}, \sqrt{p_2}, \sqrt{q_1q_2})$, and the biquadratic subfields satisfying $\mathbb{Q} \subseteq K' \subseteq F_i' \subseteq L(K')$ are

$$F_1' := \mathbb{Q}(\sqrt{2}, \sqrt{p_1p_2q_1q_2}), F_2' := \mathbb{Q}(\sqrt{2p_1}, \sqrt{p_2q_1q_2}), F_3' := \mathbb{Q}(\sqrt{2p_2}, \sqrt{p_1q_1q_2}),$$
$$F_4' := \mathbb{Q}(\sqrt{2q_1q_2}, \sqrt{p_1p_2}), F_5' := \mathbb{Q}(\sqrt{2p_1p_2}, \sqrt{q_1q_2}), F_6' := \mathbb{Q}(\sqrt{p_1}, \sqrt{2p_2q_1q_2}), \text{ and}$$
$$F_7' := \mathbb{Q}(\sqrt{p_2}, \sqrt{2p_1q_1q_2}).$$

Since $p_1p_2q_1q_2 \equiv 5 \pmod 8$, the rational prime 2 must be inert in K, and hence, $2\mathcal{O}_K = \mathfrak{l}$ is a prime ideal in $\mathcal{O}_K$. Also, by congruence modulo 8 conditions on the primes, we find that the prime above 2 splits in $\mathbb{Q}(\sqrt{p_1p_2})/\mathbb{Q}$. Thus, $\mathfrak{l}$ must be totally decomposed in F_1/K. Likewise, $\mathfrak{l}$ must be totally decomposed in F_2 and F_3. Hence the decomposition field of $\mathfrak{l}$ in $L(K)/K$ is the compositum $F_1F_2F_3$, which is $L(K)$ itself. For the field K', the rational prime 2 is ramified and we have $2\mathcal{O}_{K'} = \mathfrak{l}'^2$ where $\mathfrak{l}'$ is a prime ideal in $\mathcal{O}_{K'}$. Again from the congruence conditions, we find that $\mathfrak{l}'$ is totally decomposed only in the fields F_2', F_3' and F_4'. Hence their compositum $F_2'F_3'F_4'$ must be the decomposition field of $\mathfrak{l}'$ in $L(K')/K'$.



Since $\left(\frac{q_1q_2}{p_2}\right) = 1$, we have either $\left(\frac{p_2}{q_1}\right) = \left(\frac{p_2}{q_2}\right) = 1$ or $\left(\frac{p_2}{q_1}\right) = \left(\frac{p_2}{q_2}\right) = -1$. Let $p_i\mathcal{O}_K = \mathfrak{p}_i^2$ for $i = 1, 2$ and $q_j\mathcal{O}_K = \mathfrak{q}_j^2$ for $j = 1, 2$. Applying the Legendre symbol conditions and the fact that ramification index and residue degree are multiplicative, we conclude that when $\left(\frac{p_2}{q_1}\right) = \left(\frac{p_2}{q_2}\right) = 1$, the decomposition field of $\mathfrak{q}_2$ is same as that of $\mathfrak{l}$, which equals $L(K)$. Hence, the corresponding decomposition groups must be equal (in fact it would be the trivial group as the primes are totally decomposed in $L(K)$). Therefore, the respective Artin symbols of $\mathfrak{q}_2$ and $\mathfrak{l}$ must be equal. That is, $\left(\frac{L(K)/K}{\mathfrak{q}_2}\right) = \left(\frac{L(K)/K}{\mathfrak{l}}\right)$.

Hence, $[\mathfrak{l}] = [\mathfrak{q}_2]$ and $\langle\alpha\rangle\mathfrak{q}_2 = \mathfrak{l} = 2\mathcal{O}_K$ for some $\alpha \in K^\times$. Squaring both sides, we obtain $\langle\alpha^2\rangle q_2\mathcal{O}_K = 4\mathcal{O}_K$ which implies $4 = \varepsilon^n\alpha^2q_2$ for some $n \in \mathbb{Z}$, where ε is the fundamental unit of K. If n is even, then $2 = \varepsilon^{\frac{n}{2}}\alpha\sqrt{q_2}$ leads to $\sqrt{q_2} \in K$. That way, $\mathbb{Q}(\sqrt{q_2}) = \mathbb{Q}(\sqrt{p_1p_2q_1q_2})$, which is a contradiction. Therefore, n must be odd. In that case, $2 = \sqrt{\varepsilon}\beta\sqrt{q_2}$, where $\beta = \varepsilon^{\frac{n-1}{2}}\alpha$. Now, if $\sqrt{\varepsilon} \in K_1$, then $K_1 = K_1(\sqrt{\varepsilon}) = K_1(\sqrt{q_2})$, which is again not possible as $K_1 \neq K_1(\sqrt{q_2})$. Therefore, $\sqrt{\varepsilon} \notin K_1$ and $K_1(\sqrt{\varepsilon}) = K_1(\sqrt{q_2})$.

If we have $\left(\frac{p_2}{q_1}\right) = \left(\frac{p_2}{q_2}\right) = -1$, then the decomposition field of $\mathfrak{q}_1$ is same as that of $\mathfrak{p}_2$. Correspondingly, we obtain $\langle{\alpha_1}^2\rangle p_2\mathcal{O}_K = q_1\mathcal{O}_K$ which further implies $p_2 = \varepsilon^n{\alpha_1}^2q_1$ for some $n \in \mathbb{Z}$ and $\alpha_1 \in K^\times$. If n is even, then $\sqrt{p_2} = \varepsilon^{\frac{n}{2}}\alpha_1\sqrt{q_1}$, and thus $K(\sqrt{p_2}) = K(\sqrt{q_1})$, which is not possible. Therefore, n must be odd. In that case, $\sqrt{p_2} = \sqrt{\varepsilon}\beta_1\sqrt{q_1}$ where $\beta_1 \in K^\times$. If $\sqrt{\varepsilon} \in K_1$, then we obtain that $K_1(\sqrt{p_2}) = K_1(\sqrt{q_1})$ which is not true. Therefore, $\sqrt{\varepsilon} \notin K_1$ and also, $K_1(\sqrt{\varepsilon}) = K_1\left(\sqrt{\frac{p_2}{q_1}}\right) = K_1(\sqrt{p_1q_2})$.

For the field K', let $p_i\mathcal{O}_{K'} = \mathfrak{p}'_i{}^2$ for $i = 1, 2$ and $q_j\mathcal{O}_{K'} = \mathfrak{q}'_j{}^2$ for $j = 1, 2$. Irrespective of whether $\left(\frac{p_2}{q_1}\right) = \left(\frac{p_2}{q_2}\right) = \pm 1$, the decomposition field of $\mathfrak{p}'_1$ and $\mathfrak{l}'$ are equal, arguing as before. Proceeding as above, we find that $\varepsilon' \notin K_1$ and $K_1(\sqrt{\varepsilon'}) = K_1(\sqrt{p_1})$. Also, we note that $K_1(\sqrt{\varepsilon}) \neq K_1(\sqrt{\varepsilon'})$. If $\sqrt{\varepsilon\varepsilon'} \in K_1$, then $\sqrt{\varepsilon\varepsilon'} \in K_1 \subseteq K_1(\sqrt{\varepsilon})$. This implies $\sqrt{\varepsilon'} \in K_1(\sqrt{\varepsilon})$ and consequently, we have $K_1(\sqrt{\varepsilon'}) \subseteq K_1(\sqrt{\varepsilon})$. Similarly, if we consider the containment $\sqrt{\varepsilon\varepsilon'} \in K_1 \subseteq K_1(\sqrt{\varepsilon'})$, then $\sqrt{\varepsilon'} \in K_1(\sqrt{\varepsilon'})$ implies $K_1(\sqrt{\varepsilon}) = K_1(\sqrt{\varepsilon'})$, which is a contradiction.

Therefore, we conclude that $\sqrt{\varepsilon}, \sqrt{\varepsilon'}, \sqrt{\varepsilon\varepsilon'} \notin K_1$, which means that any system of fundamental units of K_1 does not contain the square-roots of the fundamental units of K or K', nor does it contain the product of their square roots. We note that the subfields of K_1 are K, K' and $\mathbb{Q}(\sqrt{2})$. The fundamental unit of $\mathbb{Q}(\sqrt{2})$ is $1 + \sqrt{2}$, and it has norm $N_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(1 + \sqrt{2}) = -1$. From Theorem 1.7.8, we deduce that a system of fundamental units of K_1 must be $\{\varepsilon, \varepsilon', 1 + \sqrt{2}\}$. Hence, the Hasse unit index $Q(K_1) = 1$. As the class number of $\mathbb{Q}(\sqrt{2})$ equals 1, we have $\#A(\mathbb{Q}(\sqrt{2})) = 1$, and by Theorem 1.7.8, we obtain

$$\#A(K_1) = \frac{1}{4} \cdot Q(K_1) \cdot \#A(K) \cdot \#A(K') \cdot \#A(\mathbb{Q}(\sqrt{2})) = \frac{1}{4} \cdot 1 \cdot 4 \cdot 8 \cdot 1 = 8.$$

Since rank $A(K_1) = 2$, and $\#A(K_1) = 8$, we have $A(K_1) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. This completes the proof of case 1 of Theorem 3.1.4. □

4

Stability of 2-class groups in the $\mathbb{Z}_2$-extension of certain real quadratic fields

4.1 Introduction

While classifying real quadratic fields with cyclic Iwasawa module, Mouhib and Movahhedi [66] obtained the family given by $K = \mathbb{Q}(\sqrt{\ell_1\ell_2\ell_3})$, where ℓ_1, ℓ_2 and ℓ_3 are distinct primes satisfying $\ell_1 \equiv 5 \pmod 8$, $\ell_2 \equiv 3 \pmod 8$, and $\ell_3 \equiv 3 \pmod 4$. They proved that the Iwasawa module $X(K_\infty)$ corresponding to the $\mathbb{Z}_2$-extension of K is a (finite or infinite) cyclic group (cf. Theorem 3.8, part (iv), [66]). Further, they proved that if $\ell_3 \equiv 7 \pmod 8$, the corresponding λ-invariant is equal to 0 (cf. Theorem 4.4, [66]), and thus, $X(K_\infty)$ is not only cyclic but finite as well in this case. Driven by their results, we focus on the finer structure of $X(K_\infty)$ for the aforementioned fields. In particular, we show that $X(K_\infty)$ is finite and cyclic of order 2 when the primes satisfy certain Legendre symbol conditions. We also verify Greenberg's conjecture on vanishing of λ-invariant for some additional cases. In

this chapter, the number fields K that we revolve around are of the following kind:

$$K = \mathbb{Q}(\sqrt{p_1q_1q_2}),\ p_1 \equiv 5 \pmod 8,\ q_1 \equiv 3 \pmod 8,\ q_2 \equiv 3 \pmod 8, \tag{4.1}$$

$$K = \mathbb{Q}(\sqrt{p_1q_1q_2}),\ p_1 \equiv 5 \pmod 8,\ q_1 \equiv 7 \pmod 8,\ q_2 \equiv 3 \pmod 8, \tag{4.2}$$

where p_1, q_1 and q_2 denote three distinct primes. We prove the following results:

Theorem 4.1.1. *Let $K = \mathbb{Q}(\sqrt{p_1q_1q_2})$ be a real quadratic number field such that $p_1 \equiv 5 \pmod 8$, $q_1, q_2 \equiv 3 \pmod 8$. Then, $\#A(K_1) = \#A(K_0)$ if $\left(\frac{q_1q_2}{p_1}\right) = -1$.*

Corollary 4.1.2. *Let $K = \mathbb{Q}(\sqrt{p_1q_1q_2})$ and $F = \mathbb{Q}(\sqrt{2p_1q_1q_2})$ be real quadratic number fields such that $p_1 \equiv 5 \pmod 8$, $q_1, q_2 \equiv 3 \pmod 8$, and $\left(\frac{q_1q_2}{p_1}\right) = -1$. Then, $A(K_n) \cong \mathbb{Z}/2\mathbb{Z}$ for all $n \geq 0$, and the Iwasawa module $X(K_\infty)$ corresponding to the $\mathbb{Z}_2$-extension of K is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. In particular, the λ-invariant for the $\mathbb{Z}_2$-extension of K as well as F is equal to 0.*

We note that while cyclicity of $X(K_\infty)$ under the assumptions of Corollary 4.1.2 was shown in [66], our result proves that $X(K_\infty)$ is in fact a finite group of order 2, resulting in vanishing of the λ-invariant.

Theorem 4.1.3. *Let $K = \mathbb{Q}(\sqrt{p_1q_1q_2})$ be a real quadratic number field such that $p_1 \equiv 5 \pmod 8$, $q_1, q_2 \equiv 3 \pmod 8$, $\left(\frac{q_1}{p_1}\right) = 1$, and $\left(\frac{q_2}{p_1}\right) = 1$. Then, the ideal $\mathfrak{p}_1$ in K lying above p_1 is principal if and only if $\#A(K_1) \neq \#A(K_0)$.*

Corollary 4.1.4. *Let $K = \mathbb{Q}(\sqrt{p_1q_1q_2})$ be a real quadratic number field such that $p_1 \equiv 5 \pmod 8$, $q_1, q_2 \equiv 3 \pmod 8$, $\left(\frac{q_1}{p_1}\right) = 1$, and $\left(\frac{q_2}{p_1}\right) = 1$. If the ideal $\mathfrak{p}_1$ is non-principal, then the Iwasawa module $X(K_\infty)$ corresponding to K is isomorphic to $\mathbb{Z}/2^m\mathbb{Z}$ for some $m \geq 2$. Consequently, the Iwasawa λ-invariant for such fields is equal to 0 if there are no integers a and b such that $a^2 - b^2p_1q_1q_2 = 4p_1$. Under these circumstances, the Iwasawa module corresponding to $F = \mathbb{Q}(\sqrt{2p_1q_1q_2})$ has the same structure, with $\lambda = 0$.*

Theorem 4.1.5. *Let $K = \mathbb{Q}(\sqrt{p_1q_1q_2})$ be a real quadratic number field such that $p_1 \equiv 5 \pmod 8$, $q_1 \equiv 7 \pmod 8$, $q_2 \equiv 3 \pmod 8$, and $\left(\frac{q_1}{p_1}\right) = -1$. Then, $A(K_n) \cong \mathbb{Z}/2\mathbb{Z}$ for all $n \geq 1$, and the Iwasawa module $X(K_\infty)$ corresponding to the $\mathbb{Z}_2$-extension of K is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.*

It also follows from Theorem 4.1.5 that the λ-invariant associated with the $\mathbb{Z}_2$-extension of K as well as $F = \mathbb{Q}(\sqrt{2p_1q_1q_2})$ vanishes, as proven earlier in [66].

Remark 4.1.6. *The existence of infinitely many real quadratic fields of the form (4.1) and (4.2) follows easily from Dirichlet's theorem on primes in arithmetic progression using the Chinese remainder theorem. In particular, Proposition 3.2.8 ensures the validity of Greenberg's conjecture for infinitely many real quadratic fields arising out of Corollary 4.1.2 and Corollary 4.1.4.*

4.2 The 2-class group of $\mathbb{Q}(\sqrt{p_1q_1q_2})$ and $\mathbb{Q}(\sqrt{2p_1q_1q_2})$

The class number of $\mathbb{Q}$ is equal to 1, and its 2-class group is trivial. For a quadratic extension $K = \mathbb{Q}(\sqrt{d})$, Proposition 1.7.6 implies that

$$2^{\,\mathrm{rank}_2 A(K)} = \frac{2^{t-1}}{\left[E(\mathbb{Q}) : E(\mathbb{Q}) \cap N_{K/\mathbb{Q}}(K^\times)\right]},$$

where t is the number of rational primes ramified in $K/\mathbb{Q}$. The group $A(K)$ is cyclic if and only if its 2-rank is equal to 1. Since $E(\mathbb{Q}) = \{-1, 1\}$, the index in the denominator of the formula is either 1 or 2. In such a situation, we have $2^{t-1} = 2$ or 4 and $t = 2$ or 3. Here, we emphasise that our cases of interest require $t = 3$.

Remark 4.2.1. *From [66, Theorem 3.8, part iv], we infer that $A(K_n)$ is cyclic for all $n \geq 0$, where K satisfies condition (4.1) or (4.2).*

We now prove a lemma concerning the order of $A(K)$ for $K = \mathbb{Q}(\sqrt{p_1q_2q_2})$, where the primes p_1, q_1 and q_3 satisfy $p_1 \equiv 1 \pmod 4$ and $q_1,\ q_2 \equiv 3 \pmod 4$.

Lemma 4.2.2. *Let $K = \mathbb{Q}(\sqrt{p_1q_1q_2})$ such that $p_1 \equiv 1 \pmod 4$ and $q_1,\ q_2 \equiv 3 \pmod 4$. Then, $\#A(K) = 2$ if and only if $-1 \in \left\{\left(\frac{q_1}{p_1}\right), \left(\frac{q_2}{p_1}\right)\right\}$.*

Proof. Consider the field $K = \mathbb{Q}(\sqrt{p_1q_1q_2})$. From the congruence modulo 4 conditions on the prime factors of the discriminant of K, the narrow genus field K_G^+ of K turns out to be $\mathbb{Q}(\sqrt{p_1q_1q_2}, \sqrt{p_1}, \sqrt{-q_1}, \sqrt{-q_2})$. As K is real, the genus field K_G of K is equal to $\mathbb{Q}(\sqrt{p_1q_1q_2}, \sqrt{p_1}, \sqrt{q_1q_2}) = Q(\sqrt{p_1q_1q_2}, \sqrt{p_1})$.

We first prove the forward part of the result, assuming that $\left(\frac{q_1}{p_1}\right) = -1$. A similar proof holds true if the other Legendre symbol is (or both the symbols are) equal to -1. Since $\left(\frac{q_1}{p_1}\right) = -1$, q_1 is inert in the extension $\mathbb{Q}(\sqrt{p_1})/\mathbb{Q}$. It follows that the prime $\mathfrak{q}_1$ in K which lies above q_1 is inert in K_G/K. Thus, $\mathfrak{q}_1$ is not totally split in $L(K)/K$, where $L(K)$ is the 2-Hilbert class field of K. By class field theory, $\mathfrak{q}_1$ is a non-principal ideal in K. Thus, $[\mathfrak{q}_1]$ must be of order 2 as $\mathfrak{q}$ lies above a ramified prime. Let $\mathcal{A} : A(K) \to \mathrm{Gal}(K_G/K)$ be the Artin map. Since $\mathfrak{q}_1$ does not split in K_G, by Remark 1.2.8, the Artin symbol $\left(\frac{K_G/K}{\mathfrak{q}_1}\right)$ must be non-trivial. Therefore, $[\mathfrak{q}_1]$ does not belong to $Ker(\mathcal{A})$. Let G be the group $\mathrm{Gal}(K/\mathbb{Q})$. Then, Theorem 1.3.4 implies that $Ker(\mathcal{A}) = A(K)^2$, and by Proposition 1.4.2, $A(K)^G = \{id, [\mathfrak{q}_1]\} = A(K)[2]$, where $[\mathfrak{q}_1] \notin A(K)^2$. Thus, $A(K) = A(K)^2 \cup [\mathfrak{q}_1]A(K)^2 = \{id, [\mathfrak{q}_1]\}A(K)^2$. Hence, by Nakayama's lemma 1.8.4, $A(K) = \{id, [\mathfrak{q}_1]\}$, which is of order 2.

Conversely, suppose $\#A(K) = 2$, but $\left(\frac{q_1}{p_1}\right) = 1$ and $\left(\frac{q_2}{p_1}\right) = 1$. From the order of $A(K)$, we gather that $L(K) = K(G) = \mathbb{Q}(\sqrt{p_1q_1q_2}, \sqrt{p_1})$. If both the Legendre symbols are equal to 1, then the primes $\mathfrak{p}_1, \mathfrak{q}_1$ and $\mathfrak{q}_2$ which lie above p_1, q_1 and q_2 respectively in K must be totally split in the extension $K_G/K = L(K)/K$. Thus, all three prime ideals must be principal in K, and hence, $[\mathfrak{p}_1] = [\mathfrak{q}_1] = [\mathfrak{q}_2]$ in $A(K)$. Therefore, there exists $\alpha \in K^\times$ such that $\mathfrak{q}_1 = \langle\alpha\rangle\mathfrak{q}_2$. Squaring both sides and using the fact that the generators of a principal ideal differ by a factor of a unit, we obtain that $q_1 = \alpha^2 q_2 \varepsilon^n$, where ε is the fundamental unit of K and $n \in \mathbb{Z}$. If n is even, then this implies that $\sqrt{\frac{q_1}{q_2}} \in K$, which is a contradiction. Therefore, n must be odd. In that case, $K(\sqrt{\varepsilon}) = K(\sqrt{\frac{q_1}{q_2}}) = K(\sqrt{p_1})$. Since $[\mathfrak{p}_1] = [\mathfrak{q}_1]$, following the same argument, we get $K(\sqrt{\varepsilon}) = K(\sqrt{\frac{q_1}{p_1}}) = K(\sqrt{q_2}) \neq K(\sqrt{p_1})$. That way, we again arrive at a contradiction. Hence, at least one of $\left(\frac{q_1}{p_1}\right)$ and $\left(\frac{q_2}{p_1}\right)$ must be -1. □

For a real quadratic field $K = \mathbb{Q}(\sqrt{p_1q_1q_2})$ where the three prime factors satisfy conditions (4.1) or (4.2) of Section 1, we use F to denote the field $\mathbb{Q}(\sqrt{2p_1q_1q_2})$. The orders of $A(K_0)$ and $A(F)$ can help in estimating the order of $A(K_1)$, as we shall see more generally in Lemma 4.3.1. In this section, we examine the structure of $A(F)$. The discriminant D_F of F is equal to $8p_1q_1q_2$, and has two prime factors that are congruent to 3 modulo 4. Thus, the genus field F_G of F is equal to $\mathbb{Q}(\sqrt{2}, \sqrt{p_1}, \sqrt{q_1q_2})$. We note that $\mathrm{Gal}(F_G/F)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Hence, the 2-rank of $A(F)$ is equal to 2. In order to compute the order of $A(F)$ under certain Legendre symbol criteria on the prime factors, we recall

the result by Réidei and Reichardt (cf. [73]).

Lemma 4.2.3. *Let $F = \mathbb{Q}(\sqrt{2p_1q_1q_2})$ with $p_1 \equiv 5 \pmod 8$, $q_1 \equiv 3 \pmod 8$, and $q_2 \equiv 3 \pmod 8$. Then the 2-class group $A(F)$ is of the form $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ if and only if one of the following conditions hold:*

1. $\left(\frac{q_1q_2}{p_1}\right) = -1$.
2. $\left(\frac{q_1}{p_1}\right) = 1$ *and* $\left(\frac{q_2}{p_1}\right) = 1$.

Proof. By Proposition 3.2.6, it suffices to prove the equivalence for $A^+(F)$ in place of $A(F)$. For $A^+(F)$, we employ Theorem 3.2.4. The discriminant of F is equal to $8p_1q_2q_2$, which can be expressed in the following ways as D_1D_2, where $D_i \equiv 0, 1 \pmod 4$ and $|D_1| < |D_2|$.

$$(1, 8p_1q_1q_2),\ (8, p_1q_1q_2),\ (p_1, 8q_1q_2),\ (-q_1, -8p_1q_2),$$
$$(-q_2, -8p_1q_1),\ (8p_1, q_1q_2),\ (-8q_1, -p_1q_2),\ (-8q_2, -p_1q_1).$$

These tuples account for the elements of the set $S_1(F)$. We now enlist the Kronecker symbols corresponding to each tuple in $S_1(F)$ other than $(1, 8p_1q_1q_2)$ in Table 4.1 to see which of these belong to the set $S_2(F)$.

Table 4.1: Kronecker symbols corresponding to each element in $S_1(F)$

Sr. No.	Tuple	Kronecker Symbols
1	$(8, p_1q_1q_2)$	$\left(\frac{2}{p_1}\right), \left(\frac{2}{q_1}\right), \left(\frac{2}{q_2}\right), \left(\frac{p_1q_1q_2}{2}\right)$
2	$(p_1, 8q_1q_2)$	$\left(\frac{p_1}{2}\right), \left(\frac{p_1}{q_1}\right), \left(\frac{p_1}{q_2}\right), \left(\frac{2q_1q_2}{p_1}\right)$
3	$(-q_1, -8p_1q_2)$	$\left(\frac{-q_1}{2}\right), \left(\frac{-q_1}{p_1}\right), \left(\frac{-q_1}{q_2}\right), \left(\frac{-2p_1q_2}{q_1}\right)$
4	$(-q_2, -8p_1q_1)$	$\left(\frac{-q_2}{2}\right), \left(\frac{-q_2}{p_1}\right), \left(\frac{-q_2}{q_1}\right), \left(\frac{-2p_1q_1}{q_2}\right)$
5	$(8p_1, q_1q_2)$	$\left(\frac{2p_1}{q_1}\right), \left(\frac{2p_1}{q_2}\right), \left(\frac{q_1q_2}{2}\right), \left(\frac{q_1q_2}{p_1}\right)$
6	$(-8q_1, -p_1q_2)$	$\left(\frac{-2q_1}{p_1}\right), \left(\frac{-2q_1}{q_2}\right), \left(\frac{-p_1q_2}{2}\right), \left(\frac{-p_1q_2}{q_1}\right)$
7	$(-8q_2, -p_1q_1)$	$\left(\frac{-2q_2}{p_1}\right), \left(\frac{-2q_2}{q_1}\right), \left(\frac{-p_1q_1}{2}\right), \left(\frac{-p_1q_1}{q_2}\right)$

In each case of the aforementioned criteria on Legendre symbols, we notice that there is at

least one symbol that has value -1 in each row of Table 4.1. This implies that in each of the cases, order of $S_2(F)$ is equal to 1. This means that $A^+(F)$, and hence $A(F)$, are both 2-elementary. As $\text{rank}_2 A(F) = 2$, it indeed must be isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

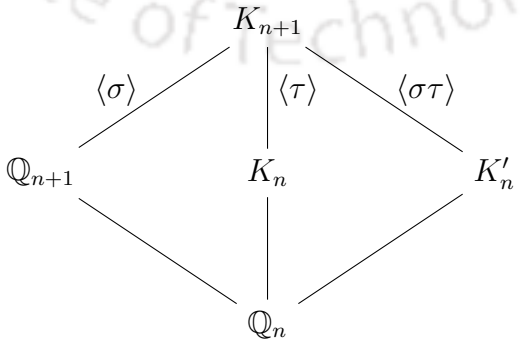
Conversely, assuming $A(F)$ is 2-elementary, by Proposition 3.2.6, $A^+(F)$ must be 2-elementary. In that case, at least one entry from each row in Table 4.1 should be equal to -1. By supposing that at least one entry is -1, we exactly obtain the options mentioned in this lemma. □

Following the same approach, we obtain the next result (irrespective of any Legendre symbol restrictions).

Lemma 4.2.4. *Let* $F = \mathbb{Q}(\sqrt{2p_1q_1q_2})$ *with* $p_1 \equiv 5 \pmod 8$, $q_1 \equiv 7 \pmod 8$, *and* $q_2 \equiv 3 \pmod 8$. *Then the 2-class group* $A(F)$ *is isomorphic to* $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

4.3 2-class groups of the sub-extensions of K_∞/K

While inspecting the field $F = \mathbb{Q}(\sqrt{pq})$, where $p \equiv 3 \pmod 8$ and $q \equiv 9 \pmod{16}$ with some additional conditions, Kumakawa in [50, Lemma 2.1] derived an upper bound on the order of $A(F_{n+1})$ for all $n \geq 0$ in terms of the orders of 2-class groups of subfields of F_{n+1}. More precisely, the subfields involved were F_n and F_n', where F_n' denotes the subfield of F_{n+1} containing $\mathbb{Q}_n$, different from F_n and $\mathbb{Q}_{n+1}$. For example, if $F = \mathbb{Q}(\sqrt{d})$, then $F_0' = \mathbb{Q}(\sqrt{2d})$, $F_1' = \mathbb{Q}\left(\sqrt{(2+\sqrt{2})d}\right)$, and so on. In the spirit of Kumakawa's work, we extract a tighter upper bound for the fields $K = \mathbb{Q}(\sqrt{d})$ where $d \equiv 1 \pmod 4$.



Lemma 4.3.1. *Let* $K = \mathbb{Q}(\sqrt{d})$ *with* $d \equiv 1 \pmod 4$ *and* $n \geq 0$. *Suppose* τ *is the generator of* $\text{Gal}(K_{n+1}/K_n)$ and σ is the generator of $\text{Gal}(K_{n+1}/\mathbb{Q}_{n+1})$. Then $\#A(K_{n+1}) \leq$

$\#A(K_{n+1})^{\tau+1} \cdot \#A(K'_n)/2$. In particular, $\#A(K_{n+1}) \leq \#A(K_n) \cdot \#A(K'_n)/2$.

Proof. Since $K_{n+1}/\mathbb{Q}_n$ is a bi-quadratic extension, $\mathrm{Gal}(K_{n+1}/K'_n) = \langle \sigma\tau \rangle$. We consider the following subgroups of $A(K_{n+1})$:

- $A(K_{n+1})^{\sigma\tau-1} := \{[\mathfrak{a}]^{\sigma\tau} \cdot [\mathfrak{a}]^{-1} : [\mathfrak{a}] \in A(K_{n+1})\}$ and
- $A(K_{n+1})^{\tau+1} := \{[\mathfrak{a}]^{\tau} \cdot [\mathfrak{a}] : [\mathfrak{a}] \in A(K_{n+1})\}$.

As $h(\mathbb{Q}_{n+1})$ is odd (cf. Theorem 10.4 of [80]), the lifting map from $A(\mathbb{Q}_{n+1})$ to $A(K_{n+1})$ is trivial. Hence, from Equation 1.7, we deduce that σ acts as -1 on $A(K_{n+1})$. This implies that $A(K_{n+1})^{\sigma\tau-1} = A(K_{n+1})^{\tau+1}$. We now consider the following exact sequence:

$$1 \longrightarrow A(K_{n+1})^{\langle \sigma\tau \rangle} \longrightarrow A(K_{n+1}) \longrightarrow A(K_{n+1})^{\sigma\tau-1} \longrightarrow 1.$$

Thus, we obtain,

$$\#A(K_{n+1}) = \#A(K_{n+1})^{\langle \sigma\tau \rangle} \cdot \#A(K_{n+1})^{\sigma\tau-1} = \#A(K_{n+1})^{\langle \sigma\tau \rangle} \cdot \#A(K_{n+1})^{\tau+1}.$$

Now, applying the genus formula for the quadratic extension K_{n+1}/K'_n, we have

$$\#A(K_{n+1})^{\mathrm{Gal}(K_{n+1}/K'_n)} = \#A(K_{n+1})^{\langle \sigma\tau \rangle} = \frac{\#A(K'_n) \cdot 2^{t-1}}{[E(K'_n) : E(K'_n) \cap N_{K_{n+1}/K'_n}(K_{n+1}^{\times})]},$$

where t is the number of primes of K'_n ramified in K_{n+1}. As $d \equiv 1 \pmod 4$, the extension K_{n+1}/K'_n is unramified. Hence, $t = 0$, $\#A(K_{n+1})^{\langle \sigma\tau \rangle} \leq \#A(K'_n)/2$, and $\#A(K_{n+1}) \leq \#A(K_{n+1})^{\tau+1} \cdot \#A(K'_n)/2$. This produces the first inequality of the lemma.

The prime(s) above 2 in K_n is(are) ramified in K_{n+1} as $d \equiv 1 \pmod 4$ for all $n \geq 0$. Thus, the norm map of ideal classes N_{K_{n+1}/K_n} is surjective. Therefore, from Equation (1.7), we obtain $A(K_{n+1})^{1+\tau} = j \circ N_{K_{n+1}/K_n}(A(K_{n+1})) = j(A(K_n))$. Since $\#j(A(K_n)) \leq \#A(K_n)$, we conclude that $\#A(K_{n+1})^{1+\tau} \leq \#A(K_n)$. This yields the second inequality, $\#A(K_{n+1}) \leq \#A(K_n) \cdot \#A(K'_n)/2$. □

For the fields $K = \mathbb{Q}(\sqrt{d})$ that satisfy Condition (4.1) or (4.2), $d \equiv 1 \pmod 4$. Hence, Lemma 4.3.1 is applicable for such fields.

4.4 The case of (5,3,3)

4.4.1 Proof of Theorem 4.1.1

Proof. Suppose the primes p_1, q_1 and q_2 are congruent to 5, 3 and 3 modulo 8 respectively, along with $\left(\frac{q_1q_2}{p_1}\right) = -1$. We have $K_1 = \mathbb{Q}(\sqrt{2}, \sqrt{p_1q_1q_2})$, and from Remark 4.2.1, $A(K_1)$ is cyclic. By Lemma 4.3.1, $\#A(K_1) \leq \#A(K_0) \cdot \#A(F)/2$, where $F = K_0' = \mathbb{Q}(\sqrt{2p_1q_1q_2})$. Combining Lemma 4.2.2 and Lemma 4.2.3, we conclude that $A(K_1)$ is a cyclic group of order 2 or 4. Further, we note from Lemma 4.3.1 that the order of $A(K_1)$ also depends on $A(K_1)^{\tau+1}$, where $\mathrm{Gal}(K_1/K) = \langle\tau\rangle$. Since $A(K_1)^{\tau+1} \subseteq A(K_1)^{\langle\tau\rangle}$, we have $\#A(K_1)^{\tau+1} \leq \#A(K_1)^{\langle\tau\rangle}$. By the genus formula, $\#A(K_1)^{\langle\tau\rangle} \leq \#A(K_0) \cdot 2^{t-1}$, where t is the number of places of K ramified in K_1. From the congruence modulo 8 conditions, $D_K \equiv 5 \pmod 8$, where D_K is the discriminant of K. Consequently, the rational prime 2 is inert in $K/\mathbb{Q}$, and only one place of K gets ramified in K_1. Therefore, $t = 1$ and $\#A(K_1)^{\tau+1} \leq \#A(K_1)^{\langle\tau\rangle} \leq 2$.

If $\#A(K_1)^{\langle\tau\rangle} = 1$, then $\#A(K_1) \leq 1 \cdot 4/2 = 2$ by Lemma 4.3.1. With the 2-rank of $A(K_1)$ being 1, order of $A(K_1)$ must be 2. Hence, $\#A(K_1) = \#A(K_0) = 2$.

Now we suppose that $\#A(K_1)^{\langle\tau\rangle} = 2$. We claim that $A(K_1)$ cannot have order 4. Suppose on the contrary, $A(K_1) = \langle[\mathfrak{a}]\rangle$ such that $[\mathfrak{a}]$ has order 4. In that case, $A(K_1)^{\langle\tau\rangle} = \{id, [\mathfrak{a}]^2\}$. Since $A(K_1)$ is a $\mathrm{Gal}(K_1/K)$-module, $[\mathfrak{a}]^\tau$ is equal to one of $[\mathfrak{a}]$ and $[\mathfrak{a}]^{-1}$. If $[\mathfrak{a}]^\tau = [\mathfrak{a}]$, then $\#A(K_1)^{\langle\tau\rangle} = 4$, which is not true. Therefore, $[\mathfrak{a}]^\tau = [\mathfrak{a}]^{-1}$, and consequently, $A(K_1)^{\tau+1} = \{id\}$. We have $\#A(K_1) \leq \#A(K_1)^{\tau+1} \cdot \#A(F)/2$ by Lemma 4.3.1. It follows that $\#A(K_1) \leq 1 \cdot 4/2 = 2$, which contradicts our assumption. Therefore, $\#A(K_1) = \#A(K_0) = 2$. □

Proof of Corollary 4.1.2

Proof. Since the discriminant D_K is congruent to 5 modulo 8, the prime 2 is inert in $K/\mathbb{Q}$. Moreover, 2 is ramified in $\mathbb{Q}_1/\mathbb{Q}$. Thus, the prime above 2 is totally ramified in K_1/K. The same argument holds for any extension K_n/K for all $n \geq 1$. Applying Theorem 4.1.1 and Theorem 1.8.5 together, $\#A(K_n) = \#A(K_0) = 2$ for all $n \geq 0$. Thus, $A(K_n)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ for all $n \geq 0$, and the Iwasawa module $X(K_\infty)$ corresponding to the $\mathbb{Z}_2$-extension

of K is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. It follows that the Iwasawa invariant λ vanishes.

When we look at the $\mathbb{Z}_2$-extension of F, we recognize that the fields at layers $n \geq 1$ are the same as the ones in the $\mathbb{Z}_2$-extension of K. As the order of the class group at each layer is 2, the Iwasawa module associated with F is also isomorphic to $\mathbb{Z}/2\mathbb{Z}$ and the corresponding λ-invariant vanishes. □

4.4.2 Proof of Theorem 4.1.3

Proof. Let $\mathfrak{p}_1$, $\mathfrak{q}_1$ and $\mathfrak{q}_2$ be the prime ideals above the rational primes p_1, q_1 and q_2 respectively in $K/\mathbb{Q}$, and $\mathfrak{p}_1'$, $\mathfrak{q}_1'$ and $\mathfrak{q}_2'$ be the corresponding ideals in $F/\mathbb{Q}$. We employ Kuroda-Kubota's class number formula to get the desired result. In order to appeal to the formula, we need to evaluate the Hasse unit index $Q(K_1)$ which involves the fundamental units of K, F, and $\mathbb{Q}_1$ along with their square-roots. Let ε_1, ε_2 and ε_3 be the fundamental units of K, F, and $\mathbb{Q}_1$ respectively. Due to Proposition 3.2.2, $N_{K/\mathbb{Q}}(\varepsilon_1) = 1$, and likewise, $N_{F/\mathbb{Q}}(\varepsilon_2) = 1$. The fundamental unit $\varepsilon_3 = 1+\sqrt{2}$ has norm -1 over $\mathbb{Q}$. From all these norm values, we conclude from Theorem 1.7.8 that the fundamental system of units of K_1 must be one of $\{\varepsilon_1, \varepsilon_2, \varepsilon_3\}, \{\sqrt{\varepsilon_1}, \varepsilon_2, \varepsilon_3\}, \{\sqrt{\varepsilon_1}, \sqrt{\varepsilon_2}, \varepsilon_3\}$, and $\{\sqrt{\varepsilon_1\varepsilon_2}, \varepsilon_2, \varepsilon_3\}$. We now eliminate certain possibilities. For convenience, we provide our argument in two parts.

Part 1. We follow the technique discussed in the proof of Theorem 3.1.4. Let us suppose that $\left(\frac{q_1}{p_1}\right) = 1$, and $\left(\frac{q_2}{p_1}\right) = 1$. Since $A(F)$ is 2-elementary (from Lemma 4.2.3), its 2-Hilbert class field $L(F)$ and its genus field F_G must be the same, which is the field $\mathbb{Q}(\sqrt{2}, \sqrt{p_1}, \sqrt{q_1q_2})$. The field F_G has three subfields that are bi-quadratic over $\mathbb{Q}$ which contain F. These are, $L_1(= K_1) := \mathbb{Q}(\sqrt{2}, \sqrt{p_1q_1q_2}), L_2 := \mathbb{Q}(\sqrt{p_1}, \sqrt{2q_1q_2})$, and $L_3 := \mathbb{Q}(\sqrt{2p_1}, \sqrt{q_1q_2})$. Let ℓ' be the prime above 2 in F. Then from the congruence modulo 8 and Legendre symbol criteria, we observe that the prime $\mathfrak{p}_1'$ and ℓ' split completely only in the extension L_3/F. Thus, the primes $\mathfrak{p}_1'$ and ℓ' have the same decomposition field L_3 in the extension $L(F)/F$, and the primes $\mathfrak{q}_1'$ and $\mathfrak{q}_2'$ have the decomposition field L_2 in $L(F)/F$. Since $L(F)/L_3$ is a quadratic extension, by Artin map, $\left(\frac{L(F)/F}{\mathfrak{p}_1'}\right) = \left(\frac{L(F)/F}{\ell'}\right)$. Thus, the ideals $\mathfrak{p}_i'$ and ℓ' differ by a principal fractional ideal, say $\langle\beta\rangle$, where $\beta \in F^\times$. Therefore, $\mathfrak{p}_1' = \langle\beta\rangle\ell'$, which upon squaring implies $\langle p_1\rangle = \langle 2\beta^2\rangle$. Hence, there exists $n \in \mathbb{Z}$ such that $p_1 = 2\beta^2\varepsilon_2^n$. If n is even, then $\sqrt{p_1} \in K_1$, which is not possible. Therefore, n must be odd. This produces the equality $\sqrt{\varepsilon_2} = \beta_1\sqrt{p_1/2}$, where $\beta_1^{-1} = \beta\varepsilon_2^{\frac{n-1}{2}} \in F$. Now, if $\sqrt{\varepsilon_2} \in K_1$,

then again, $\sqrt{p_1} \in K_1$, which is a contradiction. Hence, $\sqrt{\varepsilon_2} \notin K_1$. Also, we stress that $K_1(\sqrt{\varepsilon_2}) = K_1(\sqrt{p_1})$.

Now we proceed to prove that $\sqrt{\varepsilon_1}$ and $\sqrt{\varepsilon_1\varepsilon_2}$ do not belong to K_1 if the ideal $\mathfrak{p}_1$ is not principal in K, and only $\sqrt{\varepsilon_1\varepsilon_2}$ belongs to K_1 if $\mathfrak{p}_1$ is principal in K.

Part 2. Since $\left(\frac{q_1}{p_1}\right) = 1$ and $\left(\frac{q_2}{p_1}\right) = 1$, $\#A(K_0) \geq 4$ by Lemma 4.2.2. As each of the primes p_1, q_1 and q_2 are ramified in the extension $K/\mathbb{Q}$, the order of the ideal classes $[\mathfrak{p}_1], [\mathfrak{q}_1]$ and $[\mathfrak{q}_2]$ must be at the most 2. Given that $A(K_0)$ is cyclic, it has exactly one element of order 2. Thus, at least two ideal classes out of $[\mathfrak{p}_1], [\mathfrak{q}_1]$ and $[\mathfrak{q}_2]$ must be equal. We achieve our goal of proving that square-roots of certain fundamental units are not present in K_1 by making the following claims:

Claim 1: If $\mathfrak{p}_1$ is principal, then $\#A(K_1) = 2 \cdot \#A(K_0)$.
If $\mathfrak{p}_1$ is principal, then it must be equivalent to the ideal $\langle 2 \rangle$ in K. Therefore, there exists $\alpha \in K^\times$ such that $\mathfrak{p}_1 = \langle 2\alpha \rangle$. As argued in Part 1, there exists $\alpha_1 \in K^\times$ such that $\sqrt{p_1} = 2\alpha_1\sqrt{\varepsilon_1}$. This again implies that $\sqrt{\varepsilon_1} \notin K_1$, and $K_1(\sqrt{\varepsilon_1}) = K_1(\sqrt{p_1}) = K_1(\sqrt{\varepsilon_2})$. It follows that $\sqrt{\varepsilon_1\varepsilon_2} \in K_1$ as it is fixed under the action of the Galois group of $K_1(\sqrt{\varepsilon_1})/K_1$ $(= K_1(\sqrt{\varepsilon_2})/K_1)$. Hence, from Part 1, the system of fundamental units of K_1 is $\{\sqrt{\varepsilon_1\varepsilon_2}, \varepsilon_2, \varepsilon_3\}$. Thus, $Q(K_1) = 2$, and by Theorem 1.7.8, $\#A(K_1) = \frac{1}{4}\#A(K_0) \cdot \#A(F) \cdot \#A(\mathbb{Q}(\sqrt{2})) \cdot Q(K_1) = 2 \cdot \#A(K_0)$.

From Lemma 4.3.1 and Lemma 4.2.3, it is evident that $\#A(K_1) \neq 2 \cdot \#A(K_0)$ is equivalent to $\#A(K_1) = \#A(K_0)$. Thus, we register here that $\#A(K_1) = \#A(K_0)$ implies $\mathfrak{p}_1$ is not principal in K.

Claim 2: The ideals $\mathfrak{q}_1$ and $\mathfrak{q}_2$ cannot be simultaneously principal.
Suppose on the contrary, both the ideals are principal. Then each of the ideals must be equivalent to the ideal $\langle 2 \rangle$ in K. Proceeding as Part 1, we obtain $K(\sqrt{\varepsilon_1}) = K(\sqrt{q_1}) = K(\sqrt{q_2})$, which is a contradiction as $K(\sqrt{q_1}) \neq K(\sqrt{q_2})$. Therefore, our claim stands true. In addition, if $[\mathfrak{q}_1] = [\mathfrak{q}_2]$, then both the classes must be of order 2.

Claim 3: The ideal $\mathfrak{p}_1$ is principal if and only if $[\mathfrak{q}_1] = [\mathfrak{q}_2]$ in $\mathcal{C}l(K)$.
Suppose $\mathfrak{p}_1$ is principal. Then from Claim 1, $K_1(\sqrt{\varepsilon_1}) = K_1(\sqrt{p_1})$. If $[\mathfrak{q}_1] \neq [\mathfrak{q}_2]$, then exactly one of $\mathfrak{q}_1$ and $\mathfrak{q}_2$ must be principal. Without loss of generality, suppose $\mathfrak{q}_1$ is principal (similar arguments are applicable for $\mathfrak{q}_2$). Then the ideals $\mathfrak{p}_1$ and $\mathfrak{q}_1$ must be equivalent and must differ by a factor of a principal fractional ideal. This yields that

$K_1(\sqrt{\varepsilon_1}) = K(\sqrt{\frac{p_1}{q_1}}) = K_1(\sqrt{q_2}) \neq K_1(\sqrt{p_1})$. This is a contradiction, and hence both the classes $[\mathfrak{q}_1]$ and $[\mathfrak{q}_2]$ have to be equal (which internally implies that the classes should be of order 2 because of Claim 2).

Conversely, suppose $[\mathfrak{q}_1] = [\mathfrak{q}_2]$, and $\mathfrak{p}_1$ is not principal. Then all the three classes $[\mathfrak{p}_1], [\mathfrak{q}_1]$, and $[\mathfrak{q}_2]$ must be equal with order 2 (from Claim 2). Now following the previous technique, $[\mathfrak{p}_1] = [\mathfrak{q}_1]$ implies that $K_1(\sqrt{\varepsilon_1}) = K_1(\sqrt{q_2})$, and $[\mathfrak{p}_1] = [\mathfrak{q}_2]$ implies $K_1(\sqrt{\varepsilon_1}) = K_1(\sqrt{q_1})$, which cannot occur in unison. Hence there is an inconsistency, which implies our claim.

Claim 4: If $\mathfrak{p}_1$ is not principal, then $\#A(K_1) = \#A(K_0)$.
If $\mathfrak{p}_1$ is not principal, then by Claim 3, $[\mathfrak{q}_1] \neq [\mathfrak{q}_2]$. Thus, exactly one of $\mathfrak{q}_1$ or $\mathfrak{q}_2$ is principal. Without loss of generality, suppose $\mathfrak{q}_1$ is that non-principal ideal. Then, $\mathfrak{p}_1$ and $\mathfrak{q}_1$ must be equivalent and therefore, following the lines of argument in Part 1, $\sqrt{\varepsilon_1} \notin K_1$ and $K_1(\sqrt{\varepsilon_1}) = K_1(\sqrt{\frac{p_1}{q_1}}) = K_1(\sqrt{q_2}) \neq K_1(\sqrt{\varepsilon_2})$. For that reason, both $\sqrt{\varepsilon_1}$ and $\sqrt{\varepsilon_2}$ are not in K_1.

If $\sqrt{\varepsilon_1\varepsilon_2} \in K_1$, then $\sqrt{\varepsilon_1\varepsilon_2} \in K_1(\sqrt{\varepsilon_1})$, and this means that $\sqrt{\varepsilon_2} \in K_1(\sqrt{\varepsilon_1})$. Similarly, $\sqrt{\varepsilon_1} \in K_1(\sqrt{\varepsilon_2})$. This leads to the equality $K_1(\sqrt{\varepsilon_1}) = K_1(\sqrt{\varepsilon_2})$. But this is absurd because $K_1(\sqrt{\varepsilon_1}) = K_1(\sqrt{q_2}) \neq K_1(\sqrt{p_1}) = K_1(\sqrt{\varepsilon_2})$. Therefore, $\sqrt{\varepsilon_1\varepsilon_2} \notin K_1$. The fundamental system of units of K_1 is the set $\{\varepsilon_1, \varepsilon_2, \varepsilon_3\}$, and the Hasse unit index $Q(K_1)$ is equal to 1. From Theorem 1.7.8, $\#A(K_1) = 1/4 \cdot \#A(K_0) \cdot \#A(F) \cdot \#A(\mathbb{Q}(\sqrt{2})) \cdot Q(K_1) = 2 = \#A(K_0)$. Thus, Claim 4 follows.

We have shown that $\mathfrak{p}_1$ is principal implies $\#A(K_1) \neq \#A(K_0)$ (from Part 1 and Claim 1), and $\mathfrak{p}_1$ is not principal implies that $\#A(K_1) = \#A(K_0)$ (from Part 1 and Claim 4). This completes the proof that $\mathfrak{p}_1$ is principal if and only if $\#A(K_1) \neq \#A(K_0)$. □

Proof of Corollary 4.1.4

Proof. If the ideal $\mathfrak{p}_1$ is principal, then there exist integers a and b of same parity such that $N_{K/\mathbb{Q}}(\frac{a+b\sqrt{p_1q_1q_2}}{2}) = p_1$ or $-p_1$, i.e, $a^2 - b^2p_1q_1q_2 = 4p_1$ or $-4p_1$. If the norm is equal to $-p_1$, then taking equation modulo q_1, we obtain $a^2 \equiv -4p_1 \pmod{q_1}$, which indicates that $-p_1$ is a quadratic residue modulo q_1. But this is impossible as $\left(\frac{q_1}{p_1}\right) = \left(\frac{p_1}{q_1}\right) = 1$, and $q_1 \equiv 3 \pmod 8$. As a result, if the prime $\mathfrak{p}_1$ is principal, then there must exist integers a and b of same parity such that $a^2 - b^2p_1q_1q_2 = 4p_1$. If there are no such integers, then $\mathfrak{p}_1$

Table 4.2: Fields $K = \mathbb{Q}(\sqrt{p_1q_1q_2})$ where the prime $\mathfrak{p}_1$ above p_1 is not principal

p_1	q_1	q_2	$\#A(K_0)$	$\#A(K_1)$
5	11	19	4	4
5	11	139	4	4
5	11	179	4	4
5	19	211	4	4
13	43	107	4	4
13	131	107	8	8
13	107	131	4	4
29	59	107	8	8
29	59	67	4	4
29	67	83	4	4

Table 4.3: Fields $K = \mathbb{Q}(\sqrt{p_1q_1q_2})$ where the prime $\mathfrak{p}_1$ above p_1 is principal

p_1	q_1	q_2	$\#A(K_0)$	$\#A(K_1)$
5	11	131	4	8
5	19	59	4	8
5	11	211	4	8
5	19	139	4	8
5	19	179	4	8
13	43	179	8	16
29	59	83	4	8
29	83	107	4	8
29	59	227	4	8
53	11	43	16	32

is not principal.

From the Legendre symbol values and Lemma 4.2.2, the group $A(K_0)$ is cyclic with order at least 4. If $\mathfrak{p}_1$ is not principal in K, then from Theorem 4.1.3, $\#A(K_1) = \#A(K_0)$. From the congruence modulo 8 conditions, the prime above 2 is totally ramified in K_n/K for all $n \geq 1$. Thus, $A(K_n)$ is isomorphic to $\mathbb{Z}/2^m\mathbb{Z}$ for some $m \geq 2$ and for all $n \geq 0$. Hence, we deduce that the Iwasawa module $X(K_\infty)$ is isomorphic to $\mathbb{Z}/2^m\mathbb{Z}$ for some $m \geq 2$, and the Iwasawa invariant λ_2 is equal to 0. The same holds when we study F instead of K. The associated Iwasawa module has the same structure, with vanishing λ-invariant. □

We exhibit Theorem 4.1.3 through some examples in Table 4.2 and Table 4.3. The computations have been carried out through `SageMath`.

4.5 The case of (5,7,3)

4.5.1 Proof of Theorem 4.1.5

Proof. Let $K = \mathbb{Q}(\sqrt{d})$ satisfy Condition (4.2). The proof of Theorem 4.1.5 predominantly follows the approach used in the proof of Theorem 4.1.3. We furnish the proof for the case $\left(\frac{p_1}{q_2}\right) = 1$ as the proof for the other case is similar. When $\left(\frac{q_1q_2}{p_1}\right) = -1$, the prime p_1 is inert in $\mathbb{Q}(\sqrt{q_1q_2})$. Thus, the prime $\mathfrak{p}_1$ above p_1 in K is inert in the extension $K_G = K(\sqrt{p_1})$. Also, $\mathfrak{q}_1$ is inert in K_G/K as $\left(\frac{q_1}{p_1}\right) = -1$. Since $A(K_0)$ is cyclic of order 2, $[\mathfrak{p}_1] = [\mathfrak{q}_1]$. Thus, $\sqrt{p_1} = \sqrt{q_1}\alpha_1\sqrt{\varepsilon_1}$, for some $\alpha_1 \in K^\times$, $\sqrt{\varepsilon_1} \notin K_1$, and $K_1(\sqrt{\varepsilon_1}) = K_1(\sqrt{q_2})$.

We recall the fields L_1, L_2, and L_3 such that $F \subset L_i \subset F_G$ for $i = 1, 2, 3$, defined in Part 1 of the proof of Theorem 4.1.3. The primes $\mathfrak{p}_1'$ and $\mathfrak{q}_2'$ above p_1 and q_2 in F have the same decomposition field L_2. Thus, $[\mathfrak{p}_1] = [\mathfrak{q}_2]$ as their corresponding Artin symbols are equal with respect to the extension $F_G/F = L(F)/F$. Hence, we deduce that $\sqrt{\varepsilon_2} \notin K_1$, and $K_1(\sqrt{\varepsilon_2}) = K_1(\sqrt{q_1})$. As explained in the last part of the proof of Theorem 4.1.3, since $K_1(\sqrt{\varepsilon_1}) \neq K_1(\sqrt{\varepsilon_2})$, $\sqrt{\varepsilon_1\varepsilon_2} \notin K_1$. Again by Theorem 1.7.8, $Q(K_1) = 1$, and $\#A(K_1) = \#A(K_0) = 2$. By Fukuda's result on the stability of order of $A(K_n)$ (Theorem 1.8.5), $\#A(K_n) = 2$ for all $n \geq 0$. Thus, $X(K_\infty)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. The same occurs when we consider the field F instead of K as both these fields have the same $\mathbb{Z}_2$-extension, barring the base fields. Consequently, the Iwasawa module $X(K_\infty)$ corresponding to F is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ and its λ-invariant vanishes. □

When $\left(\frac{q_1}{p_1}\right) = 1$

In this section, we focus on the case $p_1 \equiv 5 \pmod 8$, $q_1 \equiv 7 \pmod 8$, $q_2 \equiv 3 \pmod 8$, and $\left(\frac{q_1}{p_1}\right) = 1$. We find that the prime $\mathfrak{q}_1'$ splits completely in all the fields L_i, $i = 1, 2, 3$. Thus, the ideal $\mathfrak{q}_1'$ is principal in F by class field theory. Accordingly, there exists some $\alpha \in F^\times$ such that $\mathfrak{q}_1' = \langle 2\alpha \rangle$. Again squaring both sides and equating the resultant principal ideals, we obtain $\sqrt{q_1} = 2\alpha_1\sqrt{\varepsilon_2}$ for some $\alpha_1 \in F^\times$. That being so, $\sqrt{\varepsilon_2} \notin K_1$, and $K_1(\sqrt{\varepsilon_2}) = K_1(\sqrt{q_1})$.

Case 1: If $\left(\frac{q_2}{p_1}\right) = -1$, then the ideals $\mathfrak{p}_1$ and $\mathfrak{q}_2$ are non-principal in K, and $A(K_0)$ is cyclic of order 2 by Lemma 4.2.2. Thus, $[\mathfrak{p}_1] = [\mathfrak{q}_2]$, which leads to $\sqrt{\varepsilon_1} \notin K_1$, and

$K_1(\sqrt{\varepsilon_1}) = K_1(\sqrt{q_1}) = K_1(\sqrt{\varepsilon_2})$. Therefore, $\sqrt{\varepsilon_1\varepsilon_2} \in K_1$, and $Q(K_1) = 2$, which brings about the relation $\#A(K_1) = 2 \cdot \#A(K_0)$. Since it has been proven in [66] that the Iwasawa invariant λ_2 of K is equal to 0, $X(K_\infty)$ is finite and cyclic. Additionally, $\#A(K_1) = 2 \cdot \#A(K_0) = 4$ implies that $X(K_\infty)$ is isomorphic to $\mathbb{Z}/2^m\mathbb{Z}$, for some $m \geq 2$.

Case 2: If $\left(\frac{q_2}{p_1}\right) = 1$, then we have two subcases, depending on whether $\mathfrak{q}_1$ is principal or not.

Subcase a: If $\mathfrak{q}_1$ is principal in K, then from the equivalence of the principal ideals $\mathfrak{q}_1$ and $\langle 2\rangle$, we can prove that $\sqrt{\varepsilon_1}$ and $\sqrt{\varepsilon_2}$ do not belong to K_1, $\sqrt{\varepsilon_1\varepsilon_2} \in K_1$, $Q(K_1) = 2$, and $\#A(K_1) = 2 \cdot \#A(K_0)$. From Lemma 4.2.2, $\#A(K_0) \geq 4$, and thus, $\#A(K_1) \geq 8$, and finally, $X(K_\infty)$ is of the form $\mathbb{Z}/2^m\mathbb{Z}$, for some $m \geq 3$.

Subcase b: For the other possibility, as discussed in the proof of Theorem 4.1.3, we make the following claims to prove that $\#A(K_1) = \#A(K_0)$ if and only if $\mathfrak{q}_1$ is not principal in K:

Claim 1. If $\mathfrak{q}_1$ is principal, then $\#A(K_1) = 2 \cdot \#A(K_0)$. Therefore, if $\#A(K_1) = \#A(K_0)$, then $\mathfrak{q}_1$ is not principal in K.

Claim 2. The ideals $\mathfrak{p}_1$ and $\mathfrak{q}_2$ cannot be simultaneously principal in K.

Claim 3. The ideal $\mathfrak{q}_1$ is principal in K if and only if $[\mathfrak{p}_1] = [\mathfrak{q}_2]$ in $\mathcal{C}l(K)$.

Claim 4. If the ideal $\mathfrak{q}_1$ is not principal in K, then $\#A(K_1) = \#A(K_0)$. Thus, $A(K_n)$ is isomorphic to $A(K_0)$ for all $n \geq 1$.

These claims merge to prove that $X(K_\infty)$ is isomorphic to $\mathbb{Z}/2^m\mathbb{Z}$ for some $m \geq 2$ when $\left(\frac{q_1}{p_1}\right) = \left(\frac{q_2}{p_1}\right) = 1$, and the ideal $\mathfrak{q}_1$ is not principal in K. Therefore from both the cases, we observe that when K satisfies Condition (4.2) and $\left(\frac{q_1}{p_1}\right) = 1$, $X(K_\infty)$ is not just finite and cyclic, but also, its order must be greater than or equal to 4.

5

Study of Iwasawa module via a bounded quotient

5.1 Introduction

Let F be a number field, ℓ be a prime number and $X(F_\infty)$ be the Iwasawa module corresponding to a $\mathbb{Z}_\ell$-extension F_∞ of F. Then, Iwasawa's class number formula allows one to investigate $X(F_\infty)$ through the ℓ-class groups $A_\ell(F_n)$, and vice-versa. In this chapter, we study $X(F_\infty)$ with the help of its quotient. Let $D_\ell(F_n)$ be the subgroup of $A_\ell(F_n)$ generated by the ideal classes of prime ideals above ℓ in F_n. In other words, if

$$T_\ell(F_n) := \langle [\mathfrak{p}] \in \mathcal{C}l_{F_n} : \mathfrak{p}|\ell \rangle, \text{ then } D_\ell(F_n) = A_\ell(F_n) \cap T_\ell(F_n).$$

Let $L(F_n)$ be the maximal unramified abelian ℓ-extension of F_n. Then, the quotient group $A_\ell(F_n)/D_\ell(F_n)$, denoted by $A'_\ell(F_n)$ corresponds to the maximal sub-extension $L'(F_n)/F_n$ of $L(F_n)/F_n$, where all the primes above ℓ split completely. For any $m \geq n \geq 0$,

the norm map is well-defined from $D_\ell(F_m)$ to $D_\ell(F_n)$, and hence, from $A'_\ell(F_m)$ to $A'_\ell(F_n)$. Thus $\{D_\ell(F_n) : n \geq 0\}$ and $\{A'_\ell(F_n) : n \geq 0\}$ form inverse systems with respect to norm maps. We denote the corresponding inverse limits by $D(F_\infty)$ and $X'(F_\infty)$. Since $D_\ell(F_n)$ is finite for each n, it satisfies the Mittag-Lefler condition. Therefore by Lemma 1.1.2, we can pass the exact sequence

$$1 \longrightarrow D_\ell(F_n) \longrightarrow A_\ell(F_n) \longrightarrow A'_\ell(F_n) \longrightarrow 1$$

to inverse limits and obtain

$$1 \longrightarrow D(F_\infty) \longrightarrow X(F_\infty) \longrightarrow X'(F_\infty) \longrightarrow 1.$$

In particular, $X'(F_\infty)$ can be viewed as a quotient of $X(F_\infty)$.

Most intermediate results in literature that facilitate the proof of Greenberg's conjecture on Iwasawa invariants require the existence of only one prime factor of ℓ in the base field K. We make a slightly different attempt by focusing on an infinite family of real quadratic fields where $\ell = 2$ splits. Throughout this article, we fix $\ell = 2$, and $K = \mathbb{Q}(\sqrt{pqr})$, where p, q, and r are distinct odd primes satisfying the following conditions:

$$p \equiv 9 \pmod{16},\ q \equiv 3 \pmod{8},\ r \equiv 3 \pmod{8},\ \left(\frac{qr}{p}\right) = -1,\ \left(\frac{2}{p}\right)_4 = -1. \tag{5.1}$$

Here, for $p \equiv 1 \pmod 8$, $\left(\frac{2}{p}\right)_4$ denotes the quartic power residue symbol with respect to p. The symbol is given by $\left(\frac{2}{p}\right)_4 \equiv 2^{\frac{p-1}{4}} \equiv \pm 1 \pmod p$. For $\ell = 2$, we use the notations $A(K_n)$, $D(K_n)$, and $A'(K_n)$. In this chapter, we simultaneously examine both $A(K_n)$ and $A'(K_n)$, and obtain the precise structure of $X(K_\infty)$. We thus prove the following results:

Theorem 5.1.1. *Let $K = \mathbb{Q}(\sqrt{pqr})$ be a number field, where p, q, and r are distinct odd primes satisfying $p \equiv 9 \pmod{16}$, $q \equiv 3 \pmod 8$, $r \equiv 3 \pmod 8$, $\left(\frac{qr}{p}\right) = -1$, $\left(\frac{2}{p}\right)_4 = -1$. Then, the quotient Iwasawa module $X'(K_\infty)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.*

Corollary 5.1.2. *The order of $A(K_n)$ is bounded independent of n as n tends to infinity. Thus, the Iwasawa invariant λ corresponding to the $\mathbb{Z}_2$-extension of K vanishes.*

One may notice that a similar approach is followed in [10] to study the Iwasawa module of certain families of quadratic fields. In contrast to the techniques based on capitulation used there, we solely study $A'(K_0)$ and $A'(K_1)$ by finding some unramified extensions of K_0 and K_1. One of the advantages of our method is that we are also able to compute the 4-rank via elementary group and module theoretic arguments. We conclude by obtaining a bound on the order of $A(K_n)$ in terms of n. We now state our second theorem.

Theorem 5.1.3. *For each n, the group $A(K_n)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^{a_n}\mathbb{Z}$, where $0 \leq a_n \leq n$, and there exists a stage $n_0 \geq 1$ such that $1 \leq a_n = a_{n_0}$ for all $n \geq n_0$. Thus, the 4-rank of $A(K_n)$ is at most 1 for all $n \geq 0$. Moreover, $X(K_\infty)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^{a_{n_0}}\mathbb{Z}$.*

Remark 5.1.4. *Let $F = \mathbb{Q}(\sqrt{2pqr})$, where the primes p, q, and r satisfy Condition (5.1). The $\mathbb{Z}_2$-extension of F is same as that of K, barring the base field. Therefore, the Iwasawa λ-invariant corresponding to $X(F_\infty)$ is also equal to 0, with same the 2-class group as that of K_n at each level $n \geq 1$.*

5.2 Boundedness of $A'_\ell(F_n)$ and $A_\ell(F_n)^{\langle\tau_n\rangle}$

Following similar lines of arguments used by Fukuda while proving Theorem 1.8.5, Mizusawa proved an analogous result for the quotient groups $A'_\ell(F_n)$ in the cyclotomic $\mathbb{Z}_\ell$-extension of a number field F. We state it as follows:

Theorem 5.2.1. [59, Proposition 3] *Let F be a number field, and suppose that the cyclotomic $\mathbb{Z}_\ell$-extension F_∞/F is totally ramified at any prime lying over ℓ. Then, the following hold.*

1. *If $\#A'_\ell(F_1) = \#A'_\ell(F)$, then $\#A'_\ell(F_n) = \#A'_\ell(F)$ for all $n \geq 0$. In particular, $\#A'_\ell(F_n)$ is isomorphic to $\#A'_\ell(F)$ for all $n \geq 0$.*

2. *If $\mathrm{rank}_\ell A'_\ell(F_1) = \mathrm{rank}_\ell A'_\ell(F)$, then $\mathrm{rank}_\ell A'_\ell(F_n) = \mathrm{rank}_\ell A'_\ell(F)$ for all $n \geq 0$.*

For a totally real number field F and any prime ℓ, suppose that the $\mathbb{Z}_\ell$-extension F_∞/F is topologically generated by γ. We recall from Section 1.8 that for each n, γ induces a map on F_n via restriction, which we denote by τ_n. The extension F_n/F is cyclic and its

Galois group is generated by τ_n. Suppose $[\mathfrak{a}]$ denotes the ideal class of an ideal $\mathfrak{a}$ in F_n. Then we consider

$$A_\ell(F_n)^{\langle\tau_n\rangle} = \{[\mathfrak{a}] \in A_\ell(F_n) : [\mathfrak{a}]^{\tau_n} = [\mathfrak{a}]\}.$$

We observe that if we apply genus formula (Theorem 1.4.3, Equation (1.2)) for the cyclic extension F_n/F, then the formula provides the order of $A_\ell(F_n)^{\langle\tau_n\rangle}$. We use this group at a later stage. We now state an important result proved by Greenberg regarding the order of $A_\ell(F_n)^{\langle\tau_n\rangle}$.

Proposition 5.2.2. [35, Proposition 1] *Let F be a totally real number field for which Leopoldt's conjecture holds true. Then, the order of $A_\ell(F_n)^{\langle\tau_n\rangle}$ remains bounded as n tends to infinity.*

As the field K of our consideration given by Condition (5.1) is a real quadratic extension of $\mathbb{Q}$, Leopoldt's conjecture holds true for K, and hence, the requirement in Proposition 5.2.2 is fulfilled by K.

5.3 Extensions of $\mathbb{Q}_1$ based on factors of p in $\mathbb{Q}_1$

As $p \equiv 9 \pmod{16}$, we have the factorization $\langle p\rangle = \mathfrak{p}_1\mathfrak{p}_2$ in $\mathbb{Q}_1$. These prime ideals are principal as $\mathbb{Q}_1$ is a PID. The generators of these ideals can be chosen in such a way that they are totally positive. Let p_1 and p_2 be such elements in $\mathbb{Q}_1$. From [70, page no. 242], we obtain that $p_i \equiv \pm 3, \pm(1+2\sqrt{2}) \pmod{4\sqrt{2}}$, for $i = 1, 2$. As a preparation to determine unramified extensions of K_1, we first refer to some results that are employed frequently to characterize extensions of $\mathbb{Q}_1$ that are ramified only at certain primes (cf. [23], [50], [59], [70]).

Lemma 5.3.1. [59, Lemma 5] *Let $\alpha \in \mathbb{Q}_1$ be a non-square element, coprime to 2. Then, the following hold:*

1. *The ideal $\langle\sqrt{2}\rangle$ is unramified in $\mathbb{Q}_1(\sqrt{\alpha})/\mathbb{Q}_1$ if and only if $\alpha \equiv 1$ or $3+2\sqrt{2} \pmod 4$.*
2. *The ideal $\langle\sqrt{2}\rangle$ splits in $\mathbb{Q}_1(\sqrt{\alpha})/\mathbb{Q}_1$ if and only if $\alpha \equiv 1$ or $3+2\sqrt{2} \pmod{4\sqrt{2}}$.*

Lemma 5.3.2. [70, Lemma 1] *Let $p \equiv 9 \pmod{16}$ be a prime with a factorization $p = p_1p_2$ in $\mathbb{Q}_1$ where p_1 and p_2 are totally positive, prime elements in $\mathbb{Q}_1$. Then, there exists a quadratic extension of $\mathbb{Q}_1$, unramified outside p_i if and only if $\left(\frac{2}{p}\right)_4 \neq 1 \pmod{p}$.*

Based on these two lemmas, we deduce the following:

Proposition 5.3.3. *Let $p \equiv 9 \pmod{16}$ be a prime number with a factorization $p = p_1p_2$ in $\mathbb{Q}_1$ where $p_i, i = 1, 2$ are totally positive, prime elements in $\mathbb{Q}_1$. If $\left(\frac{2}{p}\right)_4 = -1$, then the prime ideal $\langle\sqrt{2}\rangle$ is inert in $\mathbb{Q}_1(\sqrt{p_i})/\mathbb{Q}_1$.*

Proof. We furnish a proof for p_1 as the same holds for p_2. As $\left(\frac{2}{p}\right)_4 = -1$, $\mathbb{Q}_1$ has a quadratic extension unramified outside p_1 (from Lemma 5.3.2). Let that extension be $\mathbb{Q}_1(\sqrt{\alpha})$ for some non-square $\alpha \in \mathbb{Z}[\sqrt{2}]$. As the extension is unramified outside p_1, it has to be a real extension unramified at $\langle\sqrt{2}\rangle$. Also, since the class number of $\mathbb{Q}_1$ is equal to 1, any non-trivial extension of $\mathbb{Q}_1$ has to be ramified at some prime. Putting these together, we obtain that $\mathbb{Q}_1(\sqrt{\alpha}) = \mathbb{Q}_1(\sqrt{p_1})$, along with $p_1 \equiv 1$ or $3 + 2\sqrt{2} \pmod{4}$ (from Lemma 5.3.1, part 1). We already have that $p_1 \equiv \pm 3$ or $\pm(1 + 2\sqrt{2}) \pmod{4\sqrt{2}}$. If $p_1 \equiv 3$ or $(1 + 2\sqrt{2}) \pmod{4\sqrt{2}}$, then $p_1 \equiv 3$ or $(1 + 2\sqrt{2}) \pmod{4}$, which is not possible. Therefore, $p_1 \equiv -3$ or $-(1 + 2\sqrt{2}) \pmod{4\sqrt{2}}$, which is not congruent to any of 1 or $3 + 2\sqrt{2} \pmod{4\sqrt{2}}$. Thus, $\langle\sqrt{2}\rangle$ is inert in the extension $\mathbb{Q}_1(\sqrt{p_1})/\mathbb{Q}_1$. □

5.4 Structure of $A(K_n)$

We consider $K = \mathbb{Q}(\sqrt{pqr})$ such that p, q and r satisfy Condition (5.1). From the congruence conditions on p, q, and r, the discriminant D_K of K is equal to pqr, and the prime above 2 splits in $K_n/\mathbb{Q}_n$ for all $n \geq 0$. As D_K has a prime factor congruent to 3 modulo 8, -1 is not a norm in the extension $K/\mathbb{Q}$ (from Proposition 3.2.2). Since $h(\mathbb{Q}) = 1$, genus formula (Equation (1.4)) for $K/\mathbb{Q}$ implies that $\text{rank}_2 A(K) = 1$. Additionally, the genus field K_G of K is given by $K(\sqrt{p}) = \mathbb{Q}(\sqrt{p}, \sqrt{qr})$. We now recall Lemma 4.2.2 which covers a larger family of fields containing K. That allows us to make the following conclusion:

Remark 5.4.1. *Let $K = \mathbb{Q}(\sqrt{pqr})$ such that K satisfies Condition (5.1). Then, $\#A(K) = 2$.*

The quadratic subfields of a bi-quadratic extension govern the properties of the class group of the bigger field to a large extent. In case of a quadratic field $\mathbb{Q}(\sqrt{d})$, the first layer in its $\mathbb{Z}_2$-extension is $\mathbb{Q}(\sqrt{2},\sqrt{d})$. Thus, before moving to the first layer, it is imperative to inspect $\mathbb{Q}(\sqrt{2d})$. Let $F=\mathbb{Q}(\sqrt{2pqr})$, where the primes p,q, and r satisfy Condition (5.1). We now prove the following lemma which enables us to determine the structure of $A(F)$.

Lemma 5.4.2. *Let $F=\mathbb{Q}(\sqrt{2pqr})$ with $p\equiv 1 \pmod 8$, $q,r\equiv 3 \pmod 8$, and $\left(\frac{qr}{p}\right)=-1$. Then, $A(F)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$.*

Proof. From the genus formula, the 2-rank of $A(F)$ is 2, and its genus field is $F_G=\mathbb{Q}(\sqrt{2},\sqrt{p},\sqrt{qr})$. The three quadratic subfields of F_G containing F are $F(\sqrt{2})$, $F(\sqrt{p})$, and $F(\sqrt{qr})$. Let $\mathfrak{p}',\mathfrak{q}'$ and $\mathfrak{r}'$ be the prime ideals above p,q and r in F. Without loss of generality, suppose $\left(\frac{q}{p}\right)=\left(\frac{p}{q}\right)=-1$. The other case can be dealt with in a similar manner. In this case, $\langle q\rangle$ is inert in $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$, and thus, $\mathfrak{q}'$ is inert in $F(\sqrt{p})/F$. Likewise, $\mathfrak{r}'$ and $\mathfrak{p}'$ are inert in $F(\sqrt{qr})/F$, as $\langle r\rangle$ and $\langle p\rangle$ are inert in $\mathbb{Q}(\sqrt{2p})/\mathbb{Q}$ and $\mathbb{Q}(\sqrt{qr})/\mathbb{Q}$ respectively. As the ideals $\mathfrak{r}'$ and $\mathfrak{p}'$ are not totally split in F_G/F, they cannot split completely in $L(F)/F$, where $L(F)$ is the 2-Hilbert class field of F. Hence, they are not principal by class field theory. Thus, the classes $[\mathfrak{p}'],[\mathfrak{q}']$ and $[\mathfrak{r}']$ are non-trivial, and of order 2 in $A(F)$. The decomposition fields of the primes $\mathfrak{p}',\mathfrak{q}'$ and $\mathfrak{r}'$ in F_G/F are different, so their ideal classes must be mutually distinct. Since $\operatorname{rank}_2 A(F)=2$, $[\mathfrak{p}'],[\mathfrak{q}']$ and $[\mathfrak{r}']$ must be the only ideal classes of order 2. So, we may take $[\mathfrak{p}']\cdot[\mathfrak{q}']=[\mathfrak{r}']$.

Since $\mathfrak{p}',\mathfrak{q}'$ and $\mathfrak{r}'$ do not split in F_G, the image of their ideal classes must be non-trivial in $\mathrm{Gal}(F_G/F)$. This yields that $[\mathfrak{p}'],[\mathfrak{q}']$ and $[\mathfrak{r}']$ do not belong to $A(F)^2$, and $\mathrm{Gal}(F_G/F)\cong A(F)/A(F)^2\cong A(F)[2]=\langle[\mathfrak{p}'],[\mathfrak{q}']\rangle$. As $[\mathfrak{p}'],[\mathfrak{q}']\notin A(F)^2$, $A(F)=\langle[\mathfrak{p}'],[\mathfrak{q}']\rangle\cdot A(F)^2$. By Nakayama's lemma, $A(F)=\langle[\mathfrak{p}'],[\mathfrak{q}']\rangle$, which is isomorphic to $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$. □

We now proceed to study $A(K_1)$ by using the genus formula (Equation (1.4)) for the extension $K_1/\mathbb{Q}_1$. In order to do so, we need to determine the index $[E(\mathbb{Q}_1):E(\mathbb{Q}_1)\cap N_{K_1/\mathbb{Q}_1}K_1^\times]$. The group $E(\mathbb{Q}_1)/(E(\mathbb{Q}_1)\cap N_{K_1/\mathbb{Q}_1}K_1^\times)$ is 2-elementary, as the square of any element of $E(\mathbb{Q}_1)$ is clearly a norm in the extension $K_1/\mathbb{Q}_1$. We note that $E(\mathbb{Q}_1)$ is generated by -1 and $1+\sqrt{2}$, and prove the following results.

Proposition 5.4.3. *Let $K=\mathbb{Q}(\sqrt{d})$ where d has a prime factor congruent to 3 modulo 4. Then, for $K_1=K(\sqrt{2})$, $1+\sqrt{2}$ is not a norm in the extension $K_1/\mathbb{Q}_1$.*

Proof. Suppose there exists an element α in $K_1 = \mathbb{Q}(\sqrt{2}, \sqrt{d})$ such that $N_{K_1/\mathbb{Q}_1}(\alpha) = 1 + \sqrt{2}$. Then we have $N_{\mathbb{Q}_1/\mathbb{Q}}\left(N_{K_1/\mathbb{Q}_1}(\alpha)\right) = -1$. On the other hand, since K_1 is bi-quadratic over $\mathbb{Q}$, $N_{\mathbb{Q}_1/\mathbb{Q}}\left(N_{K_1/\mathbb{Q}_1}(\alpha)\right) = N_{K/\mathbb{Q}}\left(N_{K_1/K}(\alpha)\right)$. This means that there is an element in K, whose norm is equal to -1 over $\mathbb{Q}$. This is a contradiction to Proposition 3.2.2 as d has a prime factor congruent to 3 modulo 4. Thus, the proposition follows. □

Lemma 5.4.4. *In the extension $K_1/\mathbb{Q}_1$, -1 is a norm, and* $\text{rank}_2 A(K_1) = 2$.

Proof. As $K_1 = \mathbb{Q}_1(\sqrt{pqr})$, -1 is a norm in $K_1/\mathbb{Q}_1$ if and only if $\left(\frac{-1, pqr}{\mathfrak{P}}\right) = 1$ for every prime ideal $\mathfrak{P}$ of $\mathbb{Q}_1$. Since -1 is a unit, it is obvious that $\left(\frac{-1, pqr}{\mathfrak{P}}\right) = 1$ for any prime ideal $\mathfrak{P}$ of $\mathbb{Q}_1$ which is unramified in K_1. Therefore, we need to examine the symbol with respect to the prime ideals above p, q, and r in $\mathbb{Q}_1$. As $p \equiv 1 \pmod 8$, p splits completely in $\mathbb{Q}_1$, and $\langle p \rangle = \mathfrak{p}_1\mathfrak{p}_2$, where $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are prime ideals dividing p in $\mathbb{Q}_1$. Owing to the multiplicative property of the Hilbert symbol (Proposition 1.6.1, part 2), for $i = 1, 2$, we have

$$\left(\frac{-1, pqr}{\mathfrak{p}_i}\right) = \left(\frac{-1, p}{\mathfrak{p}_i}\right)\left(\frac{-1, q}{\mathfrak{p}_i}\right)\left(\frac{-1, r}{\mathfrak{p}_i}\right).$$

The primes $\mathfrak{p}_i$ are unramified in the extension $\mathbb{Q}_1(\sqrt{q})/\mathbb{Q}_1$ and $\mathbb{Q}_1(\sqrt{r})/\mathbb{Q}_1$, and -1 is a unit. Therefore, for $i = 1$ and 2,

$$\left(\frac{-1, q}{\mathfrak{p}_i}\right) = \left(\frac{-1, r}{\mathfrak{p}_i}\right) = 1, \text{ and } \left(\frac{-1, pqr}{\mathfrak{p}_i}\right) = \left(\frac{-1, p}{\mathfrak{p}_i}\right).$$

As $\left(\frac{-1, p}{\mathfrak{p}_i}\right) = \left(\frac{p, -1}{\mathfrak{p}_i}\right)^{-1}$ (Proposition 1.6.1, part 3), we consider the extension $\mathbb{Q}_1(\sqrt{-1})/\mathbb{Q}_1$. Since $p \equiv 1 \pmod 8$, p splits completely in $\mathbb{Q}_1/\mathbb{Q}$ and $\mathbb{Q}(\sqrt{-2})/\mathbb{Q}$. Thus, the primes $\mathfrak{p}_i$ split completely in $\mathbb{Q}_1(\sqrt{-1})/\mathbb{Q}_1$. By Remark 1.2.8, the corresponding Frobenius elements are equal to the identity map. As a result,

$$\left(\frac{p, -1}{\mathfrak{p}_i}\right)^{-1} = \left(\frac{-1, p}{\mathfrak{p}_i}\right) = \left(\frac{-1, pqr}{\mathfrak{p}_i}\right) = 1.$$

Next, we deal with q. Since $q \equiv 3 \pmod 8$, $\langle q \rangle$ is a prime ideal in $\mathbb{Q}_1$. As before, we have

$$\left(\frac{-1, pqr}{\langle q \rangle}\right) = \left(\frac{-1, p}{\langle q \rangle}\right)\left(\frac{-1, q}{\langle q \rangle}\right)\left(\frac{-1, r}{\langle q \rangle}\right) = \left(\frac{-1, q}{\langle q \rangle}\right) = \left(\frac{q, -1}{\langle q \rangle}\right)^{-1}.$$

Now, $q \equiv 3 \pmod 8$ implies $\left(\frac{-2}{q}\right) = 1$, which further leads to $\langle q \rangle$ being split in $\mathbb{Q}(\sqrt{-2})/\mathbb{Q}$, and hence in $\mathbb{Q}_1(\sqrt{-1})/\mathbb{Q}_1$. Again, the Frobenius element corresponding to $\langle q \rangle$ in $\mathbb{Q}_1(\sqrt{-1})/\mathbb{Q}_1$ is the identity map. It follows immediately that $\left(\frac{-1, pqr}{\langle q \rangle}\right) = 1$. The same argument holds for $\langle r \rangle$. Consequently, we have $\left(\frac{-1, pqr}{\langle r \rangle}\right) = 1$. Therefore, the Hilbert symbol $\left(\frac{-1, pqr}{\mathfrak{P}}\right)$ has value 1 for all the prime ideals $\mathfrak{P}$ of $\mathbb{Q}_1$, and hence, -1 is a norm in $K_1/\mathbb{Q}_1$. Given that -1 is a norm and $1+\sqrt{2}$ is not a norm (from Proposition 5.4.3) in $K_1/\mathbb{Q}_1$, we conclude that $-(1+\sqrt{2})$ is also not a norm in $K_1/\mathbb{Q}_1$. The number of primes ramified in $K_1/\mathbb{Q}_1$ is equal to 4. Employing these facts in the genus formula for $K_1/\mathbb{Q}_1$, we obtain, $2^{\,\mathrm{rank}_2 A(K_1)} = 2^{4-1}/2 = 2^2$. Hence, $\mathrm{rank}_2 A(K_1) = 2$. □

We recall Lemma 4.3.1 from Chapter 4 for our field K. In particular, it gives an upper bound on the order of $A(K_1)$. Along with the previous lemma, we immediately obtain the following corollary.

Corollary 5.4.5. *The group $A(K_1)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.*

Proof. It is clear that K_0' is a sub-class of fields F mentioned in Lemma 5.4.2. The group $A(K_1)$ has rank 2 from Lemma 5.4.4. From Lemma 4.3.1, we have $\#A(K_1) \leq \#A(K_0) \cdot \#A(K_0')/2$. The order of each of these groups can be found in Remark 5.4.1 and Lemma 5.4.2. Therefore, $\#A(K_1) \leq 2 \cdot 4/2 = 4$. Hence, its order must be exactly equal to 4, and the group must be isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. □

As the next step, we prove the following lemma on the rank of the 2-class groups of the subsequent fields K_n in the $\mathbb{Z}_2$-extension of K for $n \geq 2$.

Lemma 5.4.6. *The 2-rank of $A(K_2)$ is equal to 2. Further, $\mathrm{rank}_2 A(K_n) = 2$ for all $n \geq 1$.*

Proof. As the class numbers of $\mathbb{Q}_1$ and $\mathbb{Q}_2$ are odd, it is clear from the genus formula (Equation (1.4)) that the norm map from $\mathbb{Q}_2^\times$ to $E(\mathbb{Q}_1)$ is surjective. Thus, there exists an element α in $\mathbb{Q}_2$, whose norm over $\mathbb{Q}_1$ is equal to $1+\sqrt{2}$. Now suppose (if possible), that there exists a u in $K_2^\times$ such that $N_{k_2/\mathbb{Q}_2}(u) = \alpha$. Then, taking norm over $\mathbb{Q}_1$, we get $N_{\mathbb{Q}_2/\mathbb{Q}_1}(N_{K_2/\mathbb{Q}_2}(u)) = N_{\mathbb{Q}_2/\mathbb{Q}_1}(\alpha) = 1+\sqrt{2}$. But this means that $N_{K_2/\mathbb{Q}_1}(u) = N_{K_1/\mathbb{Q}_1}(N_{K_2/K_1}(u)) = 1+\sqrt{2}$, which shows that K_1 has an element of norm $1+\sqrt{2}$ over $\mathbb{Q}_1$.

This is a contradiction to Proposition 5.4.3, and hence, no such u exists in K_2. Therefore, $E(\mathbb{Q}_2) \neq E(\mathbb{Q}_2) \cap N_{K_2/\mathbb{Q}_2}(K_2^\times)$, and $[E(\mathbb{Q}_2) : E(\mathbb{Q}_2) \cap N_{K_2/\mathbb{Q}_2}(K_2^\times)] \geq 2$.

Since $p \equiv 9 \pmod{16}$, the primes $\mathfrak{p}_1$ and $\mathfrak{p}_2$ of $\mathbb{Q}_1$ lying above $\langle p \rangle$ remain inert in $\mathbb{Q}_2/\mathbb{Q}_1$. Therefore, only four primes of $\mathbb{Q}_2$ are ramified in $K_2/\mathbb{Q}_2$. Incorporating this with the aforementioned conclusion in the genus formula for $K_2/\mathbb{Q}_2$, we obtain $\text{rank}_2 A(K_2) \leq 2$. The primes above 2 are totally ramified in K_2/K_1 and hence, the norm map from $A(K_2)$ to $A(K_1)$ is surjective. Consequently, $\text{rank}_2 A(K_2) \geq \text{rank}_2 A(K_1) = 2$, and thus, $\text{rank}_2 A(K_2) = 2 = \text{rank}_2 A(K_1)$. The primes above 2 are totally ramified in K_∞/K, and hence in K_∞/K_1. Therefore, from part (2) of Theorem 1.8.5, $\text{rank}_2 A(K_n) = 2$ for all $n \geq 1$. □

5.5 Structure of $A'(K_n)$

In this section, we primarily focus on the groups $A'(K_0)$ and $A'(K_1)$, with the objective of gathering information on their orders.

Proposition 5.5.1. *Suppose $K = \mathbb{Q}(\sqrt{pqr})$ with $p \equiv 1 \pmod 8$, $q, r \equiv 3 \pmod 4$ such that $qr \equiv 1 \pmod 8$, and $-1 \in \left\{ \left(\frac{q}{p}\right), \left(\frac{r}{p}\right) \right\}$. Then, $\#A'(K) = 2$.*

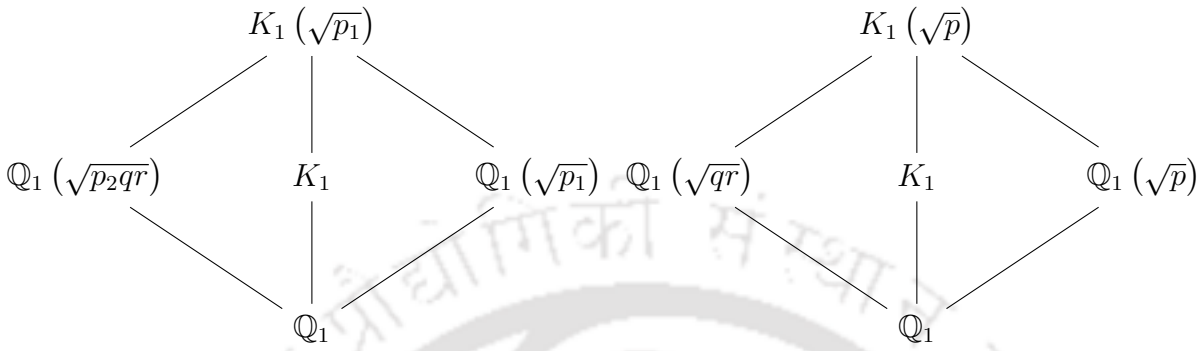
Proof. From Lemma 4.2.2, $\#A(K) = 2$ and the 2-Hilbert class field of K is same as its genus field $K_G = Q(\sqrt{p}, \sqrt{qr})$. Since $p \equiv 1 \pmod 8$ and $qr \equiv 1 \pmod 8$, the prime 2 splits completely in the field extensions $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$ and $\mathbb{Q}(\sqrt{qr})/\mathbb{Q}$. Thus, the primes above 2 in K split completely in K_G by Proposition 1.2.10. Therefore by definition, $A'(K)$ is isomorphic to $\text{Gal}(K_G/K)$, which is of order 2. □

Remark 5.5.2. *The family of fields K adhering to Condition (5.1) forms a sub-class of fields mentioned in the proposition above. Hence, for such K, $\#A'(K) = \#A'(K_0) = 2$.*

5.5.1 Proof of Theorem 5.1.1

Proof. Let K be a real quadratic field satisfying Condition 5.1. Let $p = p_1 p_2$ be a factorization of p in $\mathbb{Q}_1$ as given in Proposition 5.3.3. Then from its proof, $p_2 \equiv -3$ or $-(1 + 2\sqrt{2}) \pmod{4\sqrt{2}}$. Since $qr \equiv 1 \pmod 8$ implies $qr \equiv 1 \pmod{4\sqrt{2}}$, we obtain the following congruences: $p_2 qr \equiv -3$ or $-(1+2\sqrt{2}) \pmod{4\sqrt{2}}$, $p_2 qr \equiv 1$ or $3+2\sqrt{2} \pmod 4$,

and $p_2qr \not\equiv 1$ or $3+2\sqrt{2} \pmod{4\sqrt{2}}$. Therefore, $\langle\sqrt{2}\rangle$ is inert in $\mathbb{Q}_1(\sqrt{p_2qr})/\mathbb{Q}_1$ from Lemma 5.3.1, part (2). Consider the fields $K_1(\sqrt{p_1})$ and $K_1(\sqrt{p})$. We now claim that these are unramified over K_1.



Let $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{q}$ and $\mathfrak{r}$ be the prime ideals above p, q and r in $\mathbb{Q}_1$. Suppose ℓ_{11} and ℓ_{12} denote the primes above $\langle\sqrt{2}\rangle$ in K_1. The primes $\mathfrak{p}_2, \mathfrak{q}$ and $\mathfrak{r}$ are unramified in $\mathbb{Q}_1(\sqrt{p_1})/\mathbb{Q}_1$, but ramified in $K_1/\mathbb{Q}_1$ and $\mathbb{Q}_1(\sqrt{p_2qr})/\mathbb{Q}_1$. Thus, the primes above p_2, q, and r in K_1 must be unramified in $K_1(\sqrt{p_1})$. The ideal $\mathfrak{p}_1$ is ramified in $\mathbb{Q}_1(\sqrt{p_1})/\mathbb{Q}_1$ and $K_1/\mathbb{Q}_1$, but unramified in $\mathbb{Q}_1(\sqrt{p_2qr})/\mathbb{Q}_1$. Therefore, the prime above $\mathfrak{p}_1$ in K_1 is unramified in $K_1(\sqrt{p_1})$. The ideal $\langle\sqrt{2}\rangle$ splits in $K_1/\mathbb{Q}_1$, and remains inert in $\mathbb{Q}_1(\sqrt{p_1})$ and $\mathbb{Q}_1(\sqrt{p_2qr})$. Therefore, the primes ℓ_{11} and ℓ_{12} are inert in $K_1(\sqrt{p_1})/K_1$. Similarly, $K_1(\sqrt{p})/K_1$ is an unramified extension. But, $p, qr \equiv 1 \pmod 8$ imply that ℓ_{11} and ℓ_{12} split completely in $K_1(\sqrt{p})/K_1$. Thus, our claim stands true.

Moreover, $K_1(\sqrt{p_1}, \sqrt{p})/K_1$ is an unramified extension with Galois group isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. From Corollary 5.4.5, it is clear that $K_1(\sqrt{p_1}, \sqrt{p})$ must be the 2-Hilbert class field of K_1. In this extension, the primes ℓ_{11} and ℓ_{12} do not split completely, and the largest subfield where they are split is $K_1(\sqrt{p})$. Hence, $A'(K_1)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. From Remark 5.5.2, $\#A'(K_0) = \#A'(K_1) = 2$. The extension K_n/K is totally ramified at all primes above 2 for each $n \geq 1$. Invoking part (1) of Theorem 5.2.1, $\#A'(K_n) = 2$ for all $n \geq 0$. Therefore, $X'(K_\infty)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. □

Proof of Corollary 5.1.2

Proof. From Theorem 5.1.1, we note that for each $n \geq 0$, $A(K_n)/D(K_n) \cong \mathbb{Z}/2\mathbb{Z}$. It is evident that the order of $A(K_n)$ is bounded independent of n if the order of $D(K_n)$ is bounded as n tends to infinity. For each n, K_n/K is a cyclic extension of degree 2^n. Let τ_n be the generator of the Galois group of K_n/K induced by the topological generator γ of k_∞/k. As the prime above 2 splits in $K_n/\mathbb{Q}_n$ for all n, there exist prime ideals ℓ_{n1} and ℓ_{n2} in K_n lying above 2, and above the ideals ℓ_{01} and ℓ_{02} of K in particular. As K_n/K is totally ramified at ℓ_{01} and ℓ_{02}, $\ell_{n1}^{\tau_n} = \ell_{n1}$ and $\ell_{n2}^{\tau_n} = \ell_{n2}$. Thus, in case of the corresponding ideal classes, we have $[\ell_{n1}]^{\tau_n} = [\ell_{n1}]$ and $[\ell_{n2}]^{\tau_n} = [\ell_{n2}]$. Therefore, $D(K_n)$ must be contained in $A(K_n)^{\langle\tau_n\rangle}$ (as defined before Proposition 5.2.2). From Proposition 5.2.2, the order of $A(K_n)^{\langle\tau_n\rangle}$ is bounded, and hence the order of $D(K_n)$ must be bounded as n tends to infinity. Consequently, the order of $A(K_n)$ must stabilise for sufficiently large n and the Iwasawa invariant λ associated with the $\mathbb{Z}_2$-extension of K must be equal to 0. □

5.5.2 Proof of Theorem 5.1.3

Proof. For each n, $A(K_n), D(K_n)$ and $A'(K_n)$ are modules over $\mathbb{Z}_2[\Gamma_n]$, and we have the exact sequence

$$1 \longrightarrow D(K_n) \longrightarrow A(K_n) \longrightarrow A'(K_n) \longrightarrow 1.$$

For $n = 0$, as $A'(K_0) = A(K_0)$, $D(K_0)$ is the trivial group. As $\mathbb{Z}_2[\Gamma_n]$ is an integral domain, $\text{rank}_2 A(K_n) = \text{rank}_2 D(K_n) + \text{rank}_2 A'(K_n)$. Since $X'(K_\infty) \cong \mathbb{Z}/2\mathbb{Z}$, $A'(K_n)$ has rank 1 for all $n \geq 0$. For all $n \geq 1$, $\text{rank}_2 A(K_n) = 2$ by Lemma 5.4.6. Combining these yields $\text{rank}_2 D(K_n) = 1$ for all $n \geq 1$. For $n = 1$ in particular, we have already shown that $A(K_1)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ and $A'(k_1)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. Hence, $D(K_1)$ is cyclic, and of order 2.

For each $n \geq 1$, there exist integers a_n, b_n and c_n, all at least equal to 1 such that $A(K_n)$ and $D(K_n)$ are isomorphic to $\mathbb{Z}/2^{a_n}\mathbb{Z} \oplus \mathbb{Z}/2^{b_n}\mathbb{Z}$ and $\mathbb{Z}/2^{c_n}\mathbb{Z}$ respectively. Without loss of generality, suppose $c_n \leq a_n$. Then, by Theorem 5.1.1,

$$\mathbb{Z}/2\mathbb{Z} \cong A'(K_n) = A(K_n)/D(K_n) \cong \mathbb{Z}/2^{a_n - c_n}\mathbb{Z} \oplus \mathbb{Z}/2^{b_n}\mathbb{Z}.$$

As there is a drop in rank of the quotient by 1, $a_n = c_n$, and $b_n = 1$ for all $n \geq 1$. It is thus implied that $A(K_n) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^{a_n}\mathbb{Z}$ for all $n \geq 1$. The subgroup $D(K_n)$ is one of the maximal cyclic subgroups of $A(K_n)$. As the Iwasawa invariant λ is equal to 0, there must exist $n_0 \geq 1$ such that $a_n = a_{n_0}$ for all $n \geq n_0$.

As the prime ideal above 2 in $\mathbb{Q}_n$ is principal, and it splits in K_n, as classes, $[\ell_{n1}]^{-1} = [\ell_{n2}]$. Hence, $T(K_n)$ is cyclic, and is generated by $[\ell_{n1}]$. For $n = 0$, $D(K_0) = A(K_0) \cap T(K_0)$ is trivial. Therefore, $T(K_0)$ is either the trivial group, or, the order of $[\ell_{01}]$ is odd. If T_0 is trivial, then, ℓ_{01} and ℓ_{02} are principal. Because of total ramification in K_n/K, for all $n \geq 1$, order of $[\ell_{n1}]$ is at most 2^n. Thus, $\#D(K_n) \leq 2^n$. Otherwise, if $[\ell_{01}]$ has odd order greater than 1, then for any n, the order of $[\ell_{n1}^{2^n}]$ (which is equal to $[\ell_{01}\mathcal{O}_{K_n}]$) must be odd because of the lifting map $j : \mathcal{C}l_K \to \mathcal{C}l_{K_n}$. In that case, $[\ell_{n1}]^{2^n \cdot (2m+1)}$ must be identity for some $m \geq 0$ (we allow $m = 0$ due to possible capitulation). Thus the order of $[\ell_{n1}]$, which is same as the order of $T(K_n)$, must divide $2^n \cdot (2m + 1)$. Therefore, the even part of $T(K_n)$, which is $D(K_n)$ can have order at most 2^n.

The 4-rank of $A(K_n)$ is equal to the 2-rank of $2A(K_n)/4A(K_n)$. It is apparent from the structure of $A(K_n)$ that its 4-rank is at most equal to 1 for all $n \geq 0$. Summing up, we conclude that $X(K_\infty)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^{a_{n_0}}\mathbb{Z}$. □

6

Stability of 2-class groups in the $\mathbb{Z}_2$-extension of certain real biquadratic fields

6.1 Introduction

Though Greenberg's conjecture is not completely settled for real quadratic fields, lately even multiquadratic number fields with discriminants having a small number of prime factors are being investigated. In this chapter, we focus on the cyclotomic $\mathbb{Z}_2$-extension of an infinite family of real biquadratic fields given by $K = \mathbb{Q}(\sqrt{p}, \sqrt{r})$ where the constituent primes satisfy Condition 1, namely

$$p \equiv 9 \pmod{16},\ r \equiv 3 \pmod{4},\ \left(\frac{p}{r}\right) = -1,\ \left(\frac{2}{p}\right)_4 = -1. \tag{6.1}$$

Our aim is to validate Greenberg's conjecture for this family of fields by looking into rank and order stability. It is already known that the Iwasawa invariants μ and λ are equal to 0

for the $\mathbb{Z}_2$-extensions of the subfields $\mathbb{Q}(\sqrt{p})$, $\mathbb{Q}(\sqrt{r})$, and $\mathbb{Q}(\sqrt{pr})$ (cf. [66], [71], [23], [70]). We shall record how the 2-class groups of the subfields $\mathbb{Q}_n(\sqrt{r}), \mathbb{Q}_n(\sqrt{p})$, and $\mathbb{Q}_n(\sqrt{pr})$ of K_n influence the structure of its 2-class groups. To achieve our results, we require genus theory and results on class field towers that terminate. We utilize some theorems on capitulation in ramified and unramified extensions, and we thoroughly study the action of Galois groups of certain extensions on class groups. We also employ the family of fields K under our consideration to know more about the maximal abelian 2-extensions of $\mathbb{Q}_n(\sqrt{r})$ and $\mathbb{Q}_n(\sqrt{p})$ unramified outside $2, p$, and r. We now state our results:

Theorem 6.1.1. *Let $K = \mathbb{Q}(\sqrt{p}, \sqrt{r})$ with $p \equiv 9 \pmod{16}$, $r \equiv 3 \pmod{4}$, $\left(\frac{p}{r}\right) = -1$, and $\left(\frac{2}{p}\right)_4 = -1$. Suppose K_∞ is the $\mathbb{Z}_2$-extension of K with n-th layers K_n. Then, the corresponding Iwasawa module $X(K_\infty) = \varprojlim_n A(K_n)$ is finite and cyclic, with $\#A(\mathbb{Q}_n(\sqrt{p})) \leq \#A(K_n) \leq 2 \cdot \#A(\mathbb{Q}_n(\sqrt{p}))$ for all $n \geq 0$. In particular, the corresponding Iwasawa invariant λ vanishes for K.*

As the Iwasawa invariants μ and λ of $\mathbb{Q}(\sqrt{p})$ corresponding to its $\mathbb{Z}_2$-extension are equal to 0, there exists $n_0 \geq 0$ such that $\#A(\mathbb{Q}_n(\sqrt{p})) = \#A(\mathbb{Q}_{n_0}(\sqrt{p}))$ for all $n \geq n_0$. With this n_0, from Theorem 6.1.1, we conclude:

Corollary 6.1.2. *Let $n_0 \geq 0$ with $\#A(\mathbb{Q}_n(\sqrt{p})) = \#A(\mathbb{Q}_{n_0}(\sqrt{p}))$ for all $n \geq n_0$. Then, $\#X(\mathbb{Q}_\infty(\sqrt{p})) \leq \#X(K_\infty) \leq 2^{n_0+1} \cdot \#X(\mathbb{Q}_\infty(\sqrt{p}))$, where $X(\mathbb{Q}_\infty(\sqrt{p}))$ is the Iwasawa module corresponding to the $\mathbb{Z}_2$-extension of $\mathbb{Q}(\sqrt{p})$.*

Let S be a finite set of prime integers coprime to 2. For any number field $\mathfrak{f}$, suppose $A_S(\mathfrak{f})$ denotes the 2-part of the ray class group of $\mathfrak{f}$ modulo the product of all the prime ideals of $\mathfrak{f}$ that divide p in S. Let $(\mathbb{Q}_\infty)_S$ be the maximal pro-2-extension of $\mathbb{Q}_\infty$ unramified outside S. In other words, $A_S(\mathfrak{f})$ is the Galois group of the maximal abelian 2-extension of $\mathfrak{f}$ unramified outside S. In an attempt to classify the sets S for which $\mathrm{Gal}((\mathbb{Q}_\infty)_S/\mathbb{Q}_\infty)$ is prometacyclic, Mizusawa (cf. [61, Theorem 3.1]) obtained a result that helps us evaluate the 2-rank of $A_S(\mathfrak{f})$ via certain quadratic extensions $F/\mathfrak{f}$. As an outcome of that result and Theorem 6.1.1, we obtain the following corollary.

Corollary 6.1.3. *Suppose $p \equiv 9 \pmod{16}$, $r \equiv 3 \pmod{4}$, $\left(\frac{p}{r}\right) = -1$, and $\left(\frac{2}{p}\right)_4 = -1$. Then we have $\mathrm{rank}_2 A_{\{p\}}(\mathbb{Q}_n(\sqrt{r})) = 2$.*

Although $\#A(K_n) \geq \#A(\mathbb{Q}_n(\sqrt{p}))$ as $K_n/\mathbb{Q}_n(\sqrt{p})$ is a ramified extension, it would be interesting to know when these orders are equal. Our next theorem is aimed in this direction.

Theorem 6.1.4. *Let $K = \mathbb{Q}(\sqrt{p}, \sqrt{r})$ with $p \equiv 9 \pmod{16}$, $r \equiv 3 \pmod{4}$, $\left(\frac{p}{r}\right) = -1$, and $\left(\frac{2}{p}\right)_4 = -1$. For any $n \geq 0$, $L(K_n)$, the 2-Hilbert class field of K_n is always abelian over $\mathbb{Q}_n(\sqrt{p})$. For $n = 0$, $\#A(K_0) = \#A(\mathbb{Q}_0(\sqrt{p})) = 1$. Furthermore, if $n \geq 1$, then $\#A(K_n) = \#A(\mathbb{Q}_n(\sqrt{p}))$ if and only if some non-trivial ideal class of $A(\mathbb{Q}_n(\sqrt{p}))$ capitulates in $A(K_n)$.*

As the field $L(K_n)$ is ramified at primes above 2 and r over $\mathbb{Q}_n(\sqrt{p})$, we obtain the next corollary.

Corollary 6.1.5. *Let $p \equiv 9 \pmod{16}$, $r \equiv 3 \pmod{4}$, $\left(\frac{p}{r}\right) = -1$, and $\left(\frac{2}{p}\right)_4 = -1$. Let $\mathbb{Q}_n(\sqrt{p})$ be the n-th layer in the $\mathbb{Z}_2$-extension of $\mathbb{Q}(\sqrt{p})$. Then, the 2-rank of the maximal abelian extension of $\mathbb{Q}_n(\sqrt{p})$ unramified outside the primes above 2 and r is at least 2.*

Finally, we deal with the case $n = 1$ and provide an alternate condition for the equality $\#A(K_1) = \#A(\mathbb{Q}_1(\sqrt{p}))$.

Theorem 6.1.6. *Let $K = \mathbb{Q}(\sqrt{p}, \sqrt{r})$ with $p \equiv 9 \pmod{16}$, $r \equiv 3 \pmod{4}$, $\left(\frac{p}{r}\right) = -1$, and $\left(\frac{2}{p}\right)_4 = -1$. Suppose a and b are nonzero integers such that $p = a^2 - 2b^2$. If $\left(\frac{a}{p}\right) = -1$, or equivalently, $\left(\frac{b}{p}\right) = 1$, then $\#A(K_1) = \#A(\mathbb{Q}_1(\sqrt{p})) = 2$.*

Remark 6.1.7. *In light of Theorem 6.1.4 and Theorem 6.1.6, if p satisfies the said conditions, then a non-trivial ideal of $A(\mathbb{Q}_1(\sqrt{p}))$ capitulates in $A(K_1)$.*

6.2 Fields with 2-class group $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$

By Theorem 1.3.3, it is trivial that $K = \mathbb{Q}(\sqrt{p}, \sqrt{r})$ is the genus field of $k = \mathbb{Q}(\sqrt{pr})$, where p and r satisfy Condition (6.1). Inductively, we can also show that for any $n \geq 0$, K_n/k_n is an unramified extension, where K_n and k_n are the n-th layers of the $\mathbb{Z}_2$-extension of K and k, respectively. Fukuda and Komatsu (cf. [23]), and then Nishino (cf. [70]) studied the $\mathbb{Z}_2$-extension of $k = \mathbb{Q}(\sqrt{pr})$ with p and r satisfying Condition (6.1) and proved that such fields follow Greenberg's conjecture. They explicitly found the group

structure of $X(k_\infty)$ using methods that involved ray class groups and surjectivity of norm maps under certain conditions. We now merge their results into one and state it as follows.

Theorem 6.2.1. ([23, Theorem 2.2, Proposition 3.4], [70, Theorem 2]) *Let $k = \mathbb{Q}(\sqrt{pr})$, $p \equiv 9 \pmod{16}$, $r \equiv 3 \pmod 4$, $\left(\frac{p}{r}\right) = -1$, and $\left(\frac{2}{p}\right)_4 = -1$. The Iwasawa λ-invariant corresponding to the $\mathbb{Z}_2$-extension of k is equal to 0. For $n \geq 1$, if $A(k_n)$ denotes the 2-class group of k_n, then $A(k_n) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Furthermore, the 2-Hilbert class field of k_n for $n \geq 1$ is given by $L(k_n) = \mathbb{Q}_n(\sqrt{p}, \sqrt{r}, \sqrt{p_1})$, where $p = p_1 p_2$ with $p_i \in \mathbb{Q}_1 = \mathbb{Q}(\sqrt{2})$ and $p_i > 0$.*

Also for $n = 0$, they found the order of $A(k) = A(k_0)$ using splitting of primes and Nakayama's lemma. The technique used is similar to what is followed in Lemma 4.2.2 and Lemma 5.4.2, and can be extended to bigger classes of primes, based on modulo 4 conditions. We state it as follows:

Lemma 6.2.2. *Let $\mathfrak{K} = \mathbb{Q}(\sqrt{pr})$ such that $p \equiv 1 \pmod 4$, $r \equiv 3 \pmod 4$, and $\left(\frac{p}{r}\right) = -1$. Then, $\#A(\mathfrak{K}) = 2$.*

Considering the primes p and r individually, we present the results on the Iwasawa modules of $\mathbb{Q}(\sqrt{r})$ and $\mathbb{Q}(\sqrt{p})$, respectively.

Theorem 6.2.3. [71, Section 2] *For $r \equiv 3 \pmod 4$, the Iwasawa module $X(\mathbb{Q}(\sqrt{r})_\infty)$ corresponding to the $\mathbb{Z}_2$-extension of $\mathbb{Q}(\sqrt{r})$ is trivial.*

Theorem 6.2.4. [66, Theorems 3.8, 4.1] *Let $p \equiv 1 \pmod 8$ and $\left(\frac{2}{p}\right)_4 = -1$. Then, the Iwasawa module $X(\mathbb{Q}(\sqrt{p})_\infty)$ is cyclic with $\lambda = 0$.*

Next, we state the result by Gorenstein (cf. [26, Chapter 5, Theorem 4.5]) which characterizes all the groups G of order 2^m, where $m \geq 3$ and $G/G' \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. This result is essential because it helps us determine the 2-groups associated with 2-class field towers.

Theorem 6.2.5. [45, Theorem 1] *Let G be a finite group of order 2^m with $m \geq 3$. Suppose G' denotes the commutator subgroup of G, and $G/G' \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Then, G is one of D_{2^m} (dihedral group of order 2^m), Q_{2^m} (generalized quaternion group of order 2^m), or S_{2^m} (semi-dihedral group of order $2^m, m > 3$).*

While studying cyclic unramified extensions of number fields of degree ℓ, where ℓ is an odd prime, Taussky (cf. [78]) introduced two conditions in terms of capitulation of ideal classes. These were further utilized by Kisilevsky for $\ell = 2$, and are now widely known as "Taussky conditions". Let F/K be a cyclic unramified extension of a prime degree ℓ, $j : \mathcal{C}l_K \to \mathcal{C}l_F$ be the lifting map and $N_{F/K} : \mathcal{C}l_F \to \mathcal{C}l_K$ be the norm map, respectively. Then, the Taussky conditions are given by:

(A) $\#\left(Ker(j) \cap N_{F/K}(\mathcal{C}l_F)\right) > 1$

(B) $\#\left(Ker(j) \cap N_{F/K}(\mathcal{C}l_F)\right) = 1.$

Kisilevsky studied these conditions in [44] and even found some cohomlogical criteria for which Condition (B) holds. If F is a number field whose 2-class group is isomorphic to $(2, 2)$, then Taussky and Furtwängler (cf. [25], [77]) proved that the 2-class field tower of F terminates at the first level $F^{(1)} = L(F)$ or at the second level $F^{(2)} = L(F^{(1)})$ of the 2-class field tower. If it is the latter case, then there exists an intermediate field $L \subseteq \tilde{L}(F)$ such that L/F is an unramified non-abelian extension of degree 8. Using Taussky conditions along with certain cohomological and group theoretic arguments, Kisilevsky proved a remarkable result which helps us identify $\mathrm{Gal}(L/F)$ and $\mathrm{Gal}(F^{(2)}/F)$.

Theorem 6.2.6. [45, Theorem 2] *Let $\mathfrak{K}$ be a number field with $A(\mathfrak{K}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Suppose $\mathfrak{K}^{(1)} = L(\mathfrak{K})$, $\mathfrak{K}^{(2)} = L(\mathfrak{K}^{(1)})$, and $\mathfrak{K}_i$ and L be fields satisfying:*

$$\mathfrak{K} \subset \mathfrak{K}_1,\ \mathfrak{K}_2,\ \mathfrak{K}_3 \subset \mathfrak{K}^{(1)} \subset L \subseteq \mathfrak{K}^{(2)}.$$

Let $j_i : \mathcal{C}l(\mathfrak{K}) \to \mathcal{C}l(\mathfrak{K}_i)$ be the lifting map for $i = 1, 2, 3$. Then,

1. *If $\mathfrak{K}^{(2)} = \mathfrak{K}^{(1)}$, then for each $i \in \{1, 2, 3\}$, $\#Ker(j_i) = 4$ and each field $\mathfrak{K}_i$ satisfies Condition (A).*

2. *If $\mathrm{Gal}(L/\mathfrak{K}) \cong Q_8$, where Q_8 is the quaternion group of order 8, then for each i, $\mathfrak{K}_i$ satisfies Condition (A) with $\#Ker(j_i) = 2$. Also, $L = \mathfrak{K}^{(2)}$.*

3. *If $\mathrm{Gal}(L/\mathfrak{K}) \cong D_8$, where D_8 is the dihedral group of order 8, then $\mathfrak{K}_1, \mathfrak{K}_2$ satisfy Condition (B) and $\#Ker(j_1) = \#Ker(j_2) = 2$. In addition, the following hold:*

   (a) If $\mathfrak{K}_3$ satisfies Condition (B), then $\#Ker(j_3) = 2$, and $\mathrm{Gal}(\mathfrak{K}^{(2)}/\mathfrak{K}) \cong S_{2^m}$.

(b) If $\mathfrak{K}_3$ satisfies Condition (A) and $\#Ker(j_3) = 2$, then $\mathrm{Gal}(\mathfrak{K}^{(2)}/\mathfrak{K}) \cong Q_{2^m}$.

(c) If $\mathfrak{K}_3$ satisfies Condition (A) and $\#Ker(j_3) = 4$, then $\mathrm{Gal}(\mathfrak{K}^{(2)}/\mathfrak{K}) \cong D_{2^m}$.

It is to be noted from the proof of this theorem that all these cases are mutually exclusive and exhaustive. Hence, these are the only possible combinations of Taussky conditions and order of kernels.

Mouhib and Movahhedi proved a result on real number fields whose maximal unramified 2-extension is either the quaternion group or the semidihedral group of order $2^m, m \geq 3$. We now state it as follows.

Theorem 6.2.7. [65, Theorem 3.1] *Let F be a number field with $X(F_\infty) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Let n_0 be the smallest integer such that F_∞/F_{n_0} is totally ramified at the prime(s) above 2, and $A(F_{n_0}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. If* $\mathrm{Gal}(\tilde{L}(F_{n_0})/F_{n_0})$ *is either the quaternion group or the semidihedral group, then* $\mathrm{Gal}(\tilde{L}(F_\infty)/F_\infty) \cong \mathrm{Gal}(\tilde{L}(F_{n_0})/F_{n_0})$.

Later, Mizusawa particularly studied the possibility of $\mathrm{Gal}(\tilde{L}(F_\infty)/F_\infty)$ being isomorphic to the semidihedral group and proved the following result:

Theorem 6.2.8. [60, Theorem 1] *Let F be a real quadratic field. Then, the Galois group of the maximal unramified pro-2-extension of F_∞ which is* $\mathrm{Gal}(\tilde{L}(F_\infty)/F_\infty)$ *is not the semidihedral group.*

6.2.1 Groups of order 16

In addition to the groups mentioned in Theorem 6.2.6, we also require some properties of groups of order 16. It is known that there are 14 distinct groups of order 16 up to isomorphism (cf. [15], [16]). Of these, the abelian groups are of the form $\mathbb{Z}/16\mathbb{Z}, \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, and $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Using generators, relations, and the order of the group elements, we draw some conclusions on some of the nonabelian groups of order 16 which will be essential at a later stage.

Remark 6.2.9.

1. *The groups D_{16}, Q_{16}, and S_{16} do not have a subgroup of type $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.*

2. *The group $\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ (the semidirect product of $\mathbb{Z}/4\mathbb{Z}$ with itself) has only one subgroup of type $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.*

3. *The group M_{16} (modular group of order 16) has only 3 subgroups of order 8. These are $\mathbb{Z}/8\mathbb{Z}$ (occurring twice) and $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Hence, this group can have only 3 quotients of type $\mathbb{Z}/2\mathbb{Z}$.*

4. *The group $(\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}) \rtimes \mathbb{Z}/4\mathbb{Z}$ has no normal cyclic subgroup of order 4.*

6.3 Capitulation and norm maps in cyclic extensions

We recall the definition of capitulation of an ideal class from Section 1.5. In general, obtaining the ideal classes that capitulate in an extension is challenging. In case of cyclic unramified extensions, even though Hilbert's Theorem 94 (cf. Theorem 1.5.3) asserts capitulation of a nontrivial ideal class, it does not provide the exact number of classes that capitulate. One of the reasons for this difficulty is the presence of the units in the ring of integers, and it is best illustrated for cyclic unramified extensions by Equation (1.6).

Let K/F be a Galois extension of number fields. If ν is the algebraic norm of an ideal class, then from Equation (1.7), we have $(j \circ N_{K/F}) = \nu$, and it is clear that $Ker(N_{K/F}) \subset Ker(\nu)$. Thus, the question arises on whether the reverse containment holds or not. From Kisilevsky's work, it turns out that this need not be true for cyclic unramified extensions. We consider the following exact sequence from [44, Theorem 1]:

$$1 \longrightarrow \kappa_{K/F} \cap N_{K/F}(\mathcal{C}l_K) \xrightarrow{i} N_{K/F}(\mathcal{C}l_K) \xrightarrow{j} \nu(\mathcal{C}l_K) \longrightarrow 1.$$

Here, i and j denote the inclusion and the lifting maps, respectively. Due to the exactness and the first isomorphism theorem of groups, it is immediate that $[Ker(\nu) : Ker(N_{K/F})] = \#(\kappa_{K/F} \cap N_{K/F}(\mathcal{C}l_K))$. We also note the natural occurrence of the intersection considered by Taussky in this setup. For a cyclic unramified extension K/F with Galois group generated by σ, we use the notation ${}_\nu\mathcal{C}l_K$ for $Ker(\nu)$. From Theorem 1.5.5, $Ker(N_{K/F}) = \mathcal{C}l_K^{1-\sigma}$, and thus from [44, Theorem 1], we obtain,

$$[{}_\nu\mathcal{C}l_K : \mathcal{C}l_K^{1-\sigma}] = \#(\kappa_{K/F} \cap N_{K/F}(\mathcal{C}l_K)). \tag{6.2}$$

This relation provides us with a way of identifying which Taussky condition holds in an unramified cyclic extension. This will be quite useful to us at a later stage.

The next result by Gras is vital for understanding capitulation in ramified extensions.

Theorem 6.3.1. [33, Theorem 1.1, part 2] *Let K/F be a cyclic, totally ramified ℓ-extension of degree ℓ^N, $N \geq 1$. Let $G = \mathrm{Gal}(K/F) = \langle \psi \rangle$, $\ell^{(e(K))}$ be the exponent of $A(K)$, and let $m(K)$ be the minimal integer such that $(\psi - 1)^{m(K)}$ annihilates $A(K)$. Let $[y] \in A(K)$ be of order ℓ^e, annihilated by $(\psi - 1)^m$, where, for $s \in [0, N-1]$, if $m \in [\ell^s, \ell^{s+1} - 1]$, then $e \in [1, N-s]$. In that case, $[x] = N_{K/F}([y]) \in A(F)$ capitulates in $A(K)$.*

6.4 The rank of $A(K_n)$

This section onwards, we fix $K = \mathbb{Q}(\sqrt{p}, \sqrt{r})$ and $k = \mathbb{Q}(\sqrt{pr})$ where p and r follow Condition (6.1). For $p \equiv 1 \pmod 4$, the genus field of $\mathbb{Q}(\sqrt{p})$ is itself. Since $\mathrm{rank}_2 A(\mathbb{Q}(\sqrt{p})) = \mathrm{rank}_2 \mathrm{Gal}(\mathbb{Q}(\sqrt{p})_G / \mathbb{Q}(\sqrt{p})) = 0$, $\mathbb{Q}(\sqrt{p})$ does not have a nontrivial unramified 2-extension, and $\#A(\mathbb{Q}_0(\sqrt{p})) = \#A(\mathbb{Q}(\sqrt{p})) = 1$. When $p \equiv 1 \pmod 8$ with $\left(\frac{2}{p}\right)_4 = -1$, then it has been shown in [66, Theorem 4.1] that $\#A(\mathbb{Q}_1(\sqrt{p})) = 2$. We now delve into $A\left(\mathbb{Q}_2(\sqrt{p})\right)$ with some more conditions on p.

Proposition 6.4.1. *Let $p \equiv 9 \pmod{16}$ with $\left(\frac{2}{p}\right)_4 = -1$. Then, there exists $p_1 \in \mathbb{Q}_1 = \mathbb{Q}(\sqrt{2})$ such that $L(\mathbb{Q}_1(\sqrt{p})) = \mathbb{Q}_1(\sqrt{p}, \sqrt{p_1})$, and $\#A\left(\mathbb{Q}_2(\sqrt{p})\right) \leq 4$.*

Proof. If $p \equiv 9 \pmod{16}$, then, as mentioned in Section 5.3, there exist totally positive prime elements p_1, p_2 in $\mathbb{Q}_1$ such that $p = p_1 p_2$. Furthermore, if $\left(\frac{2}{p}\right)_4 = -1$, then from Proposition 5.3.3, the prime above 2 is unramified in $\mathbb{Q}_1(\sqrt{p_i})/\mathbb{Q}_1$. Thus, $\mathbb{Q}_1(\sqrt{p}, \sqrt{p_1})/\mathbb{Q}_1(\sqrt{p})$ is an unramified abelian extension of degree 2, and $L(\mathbb{Q}_1(\sqrt{p})) = \mathbb{Q}_1(\sqrt{p}, \sqrt{p_1})$.

From [66, Proposition 3.6], we note that when $p \equiv 9 \pmod{16}$ and $\left(\frac{2}{p}\right)_4 = -1$, the Iwasawa module corresponding to $\mathbb{Q}(\sqrt{p})$ is cyclic if and only if we have $A(M) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, where $M = \mathbb{Q}\left(\sqrt{p(2+\sqrt{2})}\right)$. Since the cyclicity of the module is already established, due to the conditions taken on p, we obtain $A(M) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Employing Lemma 4.3.1 for the field $\mathbb{Q}(\sqrt{p})$ and using $A(M) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, we derive that for $n = 2$, $\#A(\mathbb{Q}_2(\sqrt{p})) \leq 1/2 \cdot \#A(\mathbb{Q}_1(\sqrt{p})) \cdot \#A(M) = 1/2 \cdot 2 \cdot 4 = 4$. □

Hereafter, for $p \equiv 9 \pmod{16}$ and $\left(\frac{2}{p}\right)_4 = -1$, p_1 and p_2 will always denote the factors of p in $\mathbb{Q}_1$ as mentioned in the proof of Proposition 6.4.1. As the first step towards understanding K_n, we study $A(K)$ and the rank of $A(K_1)$, where $K_1 = K(\sqrt{2})$.

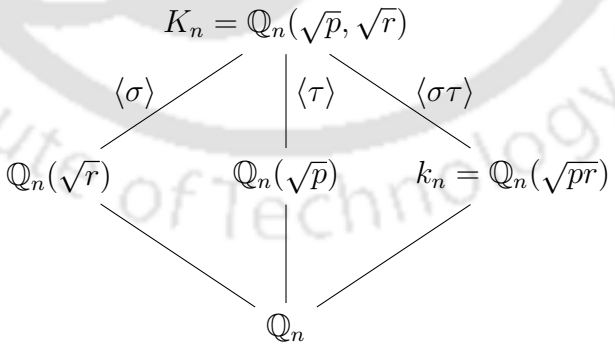
Lemma 6.4.2. *Let $K = \mathbb{Q}(\sqrt{p}, \sqrt{r})$ where p and r satisfy Condition 1. Then $A(K)$ is the trivial group, and $\text{rank}_2 A(K_1) = 1$, where $K_1 = K(\sqrt{2})$.*

Proof. From Lemma 6.2.2, since $A(k) \cong \mathbb{Z}/2\mathbb{Z}$, $k_G = K$ must be the 2-Hilbert class field of k. As K/k is a cyclic extension, according to Burnside's basis theorem, $\tilde{L}(k) = K = \tilde{L}(K)$, and $A(K) = \{id\}$.

Viewing K as a biquadratic extension over $\mathbb{Q}$ with subfields $\mathbb{Q}(\sqrt{p}), \mathbb{Q}(\sqrt{r})$, and k, it can be verified that the prime ideal $2\mathbb{Z}$ of $\mathbb{Q}$ has two prime factors in K. In turn, these factors are the only ramified primes in the extension K_1/K. Since $A(K)$ is trivial, the genus formula for K_1/K provides the upper bound: $\text{rank}_2 A(K_1) \leq 1$.

As stated in Theorem 6.2.1, the 2-Hilbert class field of $k_1 = \mathbb{Q}(\sqrt{2}, \sqrt{pr})$ is $L(k_1) = \mathbb{Q}(\sqrt{2}, \sqrt{p}, \sqrt{r}, \sqrt{p_1})$. We note that the field K_1 is an unramified extension of k_1 and it is properly contained in $L(k_1)$. Therefore, $L(k_1)/K_1$ is an unramified quadratic extension and thus, $\text{rank}_2 A(K_1) \geq 1$. Integrating this with the previous argument, we obtain $\text{rank}_2 A(K_1) = 1$. □

Inspired by Kumawaka's lemma (cf. [50, Lemma 2.1]), we formulated Lemma 4.3.1 for a bigger class of fields. In this work, we adapt those arguments for the biquadratic extension $K_n = \mathbb{Q}_n(\sqrt{p}, \sqrt{r})/\mathbb{Q}_n$. We note that this extension does not involve layers from the cyclotomic $\mathbb{Z}_2$-extension of K other than K_n.



Lemma 6.4.3. *Let $K = \mathbb{Q}(\sqrt{p}, \sqrt{r})$ where p and r satisfy Condition (6.1). Let K_n be the n^{th}-layer of K in the $\mathbb{Z}_2$-extension of K. Suppose $\text{Gal}(K_n/\mathbb{Q}_n(\sqrt{p})) = \langle\tau\rangle$ and $\text{Gal}(K_n/\mathbb{Q}_n(\sqrt{r})) = \langle\sigma\rangle$. Then, the following hold for $n \geq 1$.*

1. $\#A(K_n) = \#A(K_n)^{\tau+1} \cdot \#A(K_n)^{\langle\sigma\tau\rangle} = 2 \cdot \#A(K_n)^{\tau+1}$.

2. $\#A(\mathbb{Q}_n(\sqrt{p})) \leq \#A(K_n) \leq 2 \cdot \#A(\mathbb{Q}_n(\sqrt{p}))$.

Proof. From Theorem 6.2.3, $\#A(\mathbb{Q}_n(\sqrt{r})) = 1$ for every $n \geq 0$, and we deduce from Proposition 1.7.6 that σ acts as inverse on $A(K_n)$. This leads to the equality $A(K_n)^{\sigma\tau-1} = A(K_n)^{\tau+1}$, where the subgroups $A(K_n)^{\sigma\tau-1}$ and $A(K_n)^{\tau+1}$ are defined in Lemma 4.3.1.

(1). From the exact sequence

$$1 \longrightarrow A(K_n)^{\langle\sigma\tau\rangle} \longrightarrow A(K_n) \longrightarrow A(K_n)^{\sigma\tau-1} \longrightarrow 1,$$

we obtain $\#A(K_n) = \#A(K_n)^{\langle\sigma\tau\rangle} \cdot \#A(K_n)^{\sigma\tau-1} = \#A(K_n)^{\langle\sigma\tau\rangle} \cdot \#A(K_n)^{\tau+1}$. We apply genus formula for K_n/k_n as $\mathrm{Gal}(K_n/k_n) = \langle\sigma\tau\rangle$. As this extension is unramified, and $\#A(k_n) = 4$ for all $n \geq 1$ (from Theorem 6.2.1), $\#A(K_n)^{\langle\sigma\tau\rangle} \leq 2^{-1} \cdot 4 = 2$ irrespective of the action of τ. We now look at two possibilities:

Case 1. τ **acts as inverse on** $A(K_n)$: If $[\mathfrak{P}]^\tau = [\mathfrak{P}]^{-1}$ for every $[\mathfrak{P}] \in A(K_n)$, then $A(K_n)^{\tau+1} = \{id\}$, and hence, $\#A(K_n) = \#A(K_n)^{\langle\sigma\tau\rangle}$ and thus $\#A(K_n) \leq 2$. But from Lemma 6.4.2, $\mathrm{rank}_2 A(K_1) = 1$ implies $\mathrm{rank}_2 A(K_n) \geq 1$, and $\#A(K_n) \geq 2$. Therefore, in this case, $\#A(K_n) = 2 = 2 \cdot \#A(K_n)^{\tau+1}$.

Case 2. τ **does not act as inverse on** $A(K_n)$: In this case, $A(K_n)^{\tau+1}$ will be a non-trivial subgroup of $A(K_n)$. Since $A(K_n)$ is an abelian 2-group, so is $A(K_n)^{\tau+1}$. Therefore, by Cauchy's theorem on finite groups, there exists $[\mathfrak{q}] \in A(K_n)^{\tau+1}$ of order 2. It is clear that $[\mathfrak{q}]^\tau = [\mathfrak{q}]$, and $[\mathfrak{q}]^{\sigma\tau} = ([\mathfrak{q}]^{-1})^\tau = [\mathfrak{q}]^\tau = [\mathfrak{q}]$. This implies $[\mathfrak{q}] \in A(K_n)^{\langle\sigma\tau\rangle}$, and that $\#A(K_n)^{\langle\sigma\tau\rangle} \geq 2$. From the lines before Case 1, it is apparent that $\#A(K_n)^{\langle\sigma\tau\rangle} \leq 2$, and hence, $\#A(K_n)^{\langle\sigma\tau\rangle} = 2$. This proves that $\#A(K_n) = 2 \cdot \#A(K_n)^{\tau+1}$.

(2). Let N be the norm map from $A(K_n)$ to $A(\mathbb{Q}_n(\sqrt{p}))$. Due to Theorem 1.5.6, the map N is surjective, as the extension $K_n/\mathbb{Q}_n(\sqrt{p})$ is ramified at primes above 2 and r. This produces the first inequality $\#A(\mathbb{Q}_n(\sqrt{p})) \leq \#A(K_n)$. We now observe the kernel of N by taking an element $[\mathfrak{P}] \in Ker(N)$. By Corollary 1.7.5, we may choose $\mathfrak{P}$ to be a prime ideal in K_n lying above a split prime $\mathfrak{p}$ in $\mathbb{Q}_n(\sqrt{p})$. Now, $\mathfrak{p} \subseteq \mathfrak{P}\mathfrak{P}^\tau \cap \mathcal{O}_{\mathbb{Q}_n(\sqrt{p})} = \langle\alpha\rangle$, where $\alpha \in \mathcal{O}_{\mathbb{Q}_n(\sqrt{p})} \setminus \{0\}$. If α is a unit, then $1 \in \mathfrak{P}\mathfrak{P}^\tau$, which is not possible. Hence, α is not a unit, and $\mathfrak{p} = \langle\alpha\rangle$, as $\mathfrak{p}$ is maximal in $\mathcal{O}_{\mathbb{Q}_n(\sqrt{p})}$. Therefore, $\mathfrak{p}\mathcal{O}_{K_n} = \mathfrak{P}\mathfrak{P}^\tau$ is principal, and thus, $[\mathfrak{P}]^{1+\tau} = id$. Hence, $Ker(N) \subseteq T := \{[\mathfrak{P}] \in A(K_n) : [\mathfrak{P}]^{1+\tau} = id\}$, and $\#A(K_n)^{\tau+1} = \#(A(K_n)/T) \leq \#(A(K_n)/Ker(N)) = \#A(\mathbb{Q}_n(\sqrt{p}))$. From part 1,

$\#A(K_n) = 2 \cdot \#A(K_n)^{\tau+1} \leq 2 \cdot \#A(\mathbb{Q}_n(\sqrt{p}))$. □

Remark 6.4.4. *From Lemma 6.4.3, we observe that $A(K_n)^{\langle\sigma\tau\rangle} \cong \mathbb{Z}/2\mathbb{Z}$. Therefore, there exists $[\mathfrak{a}]$ of order 2 in $A(K_n)$ such that $A(K_n)^{\langle\sigma\tau\rangle} = \{id, [\mathfrak{a}]\}$. If $[\mathfrak{q}] \in A(K_n)$ is of order two such that $[\mathfrak{q}] \in A(K_n)^{\tau+1}$, then from Case 2 of Lemma 6.4.3, $[\mathfrak{q}] \in A(K_n)^{\langle\sigma\tau\rangle}$. Therefore, $[\mathfrak{q}] = [\mathfrak{a}]$. This implies that $A(K_n)^{\tau+1}$ can have at most one element of order 2, and if it does, then it must be $[\mathfrak{a}]$. Hence, $A(K_n)^{\tau+1}$ is cyclic of order $\#A(K_n)/2$.*

Suppose $[\mathfrak{P}] \neq [\mathfrak{a}] \in A(K_n)$ is another element of order 2, and let $H = \{id, [\mathfrak{P}]\}$ be another subgroup of $A(K_n)$. Then, H and $A(K_n)^{\tau+1}$ intersect trivially. Consequently, $\#(H \cdot A(K_n)^{\tau+1}) = \#A(K_n)$, and hence, $H \cdot A(K_n)^{\tau+1} = A(K_n)$. Since by Remark 6.4.4 $A(K_n)^{\tau+1}$ is cyclic, the group $A(K_n) = H \cdot A(K_n)^{\tau+1}$ can have at most three elements of order 2. This implies that $\text{rank}_2 A(K_n) \leq 2$ for all $n \geq 0$. We shall now see that in fact, the rank is always 1 for $n \geq 1$.

6.4.1 Proof of Theorem 6.1.1

From Theorem 6.2.1, since $A(k_n) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ for every $n \geq 1$, $K_n \subset L(k_n) = \mathbb{Q}_n(\sqrt{p}, \sqrt{r}, \sqrt{p_1}) \subseteq \tilde{L}(k_n)$ for every n. Since K_n/k_n is unramified, $\tilde{L}(K_n) = \tilde{L}(k_n)$. Thus, we have the tower of field extensions:

$$\mathbb{Q} \subset \mathbb{Q}_1 \subset \mathbb{Q}_2 \subset k_2 \subset \mathfrak{K}_1,\ \mathfrak{K}_2,\ \mathfrak{K}_3 \subset L(k_2) \subset L(K_2) \subseteq \tilde{L}(k_2) = \tilde{L}(K_2),$$

where, $\mathfrak{K}_1 = \mathbb{Q}(\sqrt{pr}, \sqrt{p_1})$, $\mathfrak{K}_2 = \mathbb{Q}(\sqrt{pr}, \sqrt{p_2})$, and $\mathfrak{K}_3 = K_2$. Let $\tilde{G}_2 = \text{Gal}(\tilde{L}(k_2)/k_2)$. If $\tilde{G}_2$ is of order 4, then $\tilde{L}(k_2) = L(k_2)$, and $\tilde{L}(K_2) = L(K_2) = L(k_2)$ must be a cyclic extension of K_2, and we are done. If not, then Theorem 6.2.1 implies that $\tilde{G}_2/\tilde{G}_2' \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Thus, $\tilde{G}_2$ can have only 3 abelian quotients of order 2, and hence it has three subgroups of index two, and they are $\mathfrak{G}_i = \text{Gal}(\tilde{L}(k_2)/\mathfrak{K}_i)$, $i = 1, 2, 3$. By group theory and Theorem 6.2.5, it can be seen that the possibilities of the subgroups $\mathfrak{G}_i$ of $\tilde{G}_2$ are $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2^r\mathbb{Z}$ $(r \in \{1, 2, m-1\})$, $D_{2^{m-1}}$, and $Q_{2^{m-1}}$ (cf. [58, Pages 27, 28]) for some $m \geq 3$. As $\mathfrak{K}_i/k_2$ is unramified for each i, $\tilde{L}(\mathfrak{K}_i) = \tilde{L}(k_2)$. Hence, the largest abelian quotient of $\mathfrak{G}_i$ will correspond to the maximal, abelian unramified 2-extension of $\mathfrak{K}_i$, that is, $A(\mathfrak{K}_i) = \mathfrak{G}_i/\mathfrak{G}_i'$. Again using Theorem 6.2.5, $\mathfrak{G}_i/\mathfrak{G}_i'$ is either $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/2^r\mathbb{Z}$ $(r \in \{1, 2, m-1\})$. Out of these, if $\tilde{G}_2 \cong Q_8$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, then all the $A(\mathfrak{K}_i)$'s

are cyclic and isomorphic to each other. In particular, $A(K_2) = A(\mathfrak{K}_3)$ is cyclic.

If $\tilde{G}_2$ is not isomorphic to Q_8 or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, then it must be isomorphic to one of $D_{2^m}(m \geq 3)$, $Q_{2^m}(m > 3)$, or $S_{2^m}(m > 3)$. In that case, the subgroups of index 2 can be dihedral, quaternion, or cyclic. Therefore, there exist $i_1 \neq i_2 \neq i_3 \in \{1, 2, 3\}$ such that $A(\mathfrak{K}_{i_1}) \cong A(\mathfrak{K}_{i_2}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, and $A(\mathfrak{K}_{i_3})$ is a cyclic 2-group. Consider p_1, p_2 as defined in Lemma 6.4.2, and let a and b be integers such that $p_1 = a + b\sqrt{2}$, and $p_2 = a - b\sqrt{2}$. The minimal polynomial of $\sqrt{p_1}$ over $\mathbb{Q}$ is given by $f(x) := (x^2 - a)^2 - 2b^2$. Suppose α is a root of f. Substituting α^2 with t in $f(\alpha) = 0$, we note that t can take the values p_1 as well as p_2. Therefore, α can assume the values $\sqrt{p_1}, -\sqrt{p_1}, \sqrt{p_2}$, and $-\sqrt{p_2}$. Since $\pm\sqrt{p_2} \notin \mathfrak{K}_1$, $\mathfrak{K}_1$ is not a Galois extension of $\mathbb{Q}$, and similarly, $\mathfrak{K}_2$ is also not a Galois extension of $\mathbb{Q}$. But, $\mathfrak{K}_1$ and $\mathfrak{K}_2$ are isomorphic as field extensions over $\mathbb{Q}$ as $\pm\sqrt{p_1}$ and $\pm\sqrt{p_2}$ are all conjugates over $\mathbb{Q}$. As a result, the class groups of $\mathfrak{K}_1$ and $\mathfrak{K}_2$, and in particular, $A(\mathfrak{K}_1)$ and $A(\mathfrak{K}_2)$ must be isomorphic. This implies that $A(\mathfrak{K}_3) = A(K_2)$ is always cyclic. From Lemma 6.4.2, $A(K_1)$ is cyclic, and from Theorem 1.8.5, $A(K_n)$ is cyclic for all $n \geq 1$. Thus, $X(K_\infty)$ is a cyclic module.

From Part 2 of Lemma 6.4.3, we recall that $\#A(K_n) \leq 2 \cdot \#A(\mathbb{Q}_n(\sqrt{p}))$. Also, from Theorem 6.2.4, the λ-invariant of $\mathbb{Q}(\sqrt{p})$ is 0 implies $\#A(\mathbb{Q}_n(\sqrt{p}))$ is bounded independent of n, as n grows. Combining both, we conclude that $\#A(K_n)$ is bounded as n tends to infinity. Thus, the Iwasawa λ-invariant of K is equal to 0. □

Proof of Corollary 6.1.2

Suppose $n_0 \geq 0$ is the stage such that $\#A(\mathbb{Q}_n(\sqrt{p})) = \#A(\mathbb{Q}_{n_0}(\sqrt{p}))$ for all $n \geq n_0$. Then, it is straightforward from Lemma 6.4.3 and Theorem 1.8.5, that $\#A(K_n) = \#A(K_{n_0+1})$ for all $n \geq n_0+1$. The inequality $\#A(K_n) \leq 2 \cdot \#A(\mathbb{Q}_n(\sqrt{p}))$ yields $\#X(K_\infty) \leq 2^{n_0+1} \cdot \#X(\mathbb{Q}_\infty(\sqrt{p}))$. □

Proof of Corollary 6.1.3

Let $S = \{p\}$ and $\Sigma = \phi$ be the empty set. Then, $A_\Sigma(\mathbb{Q}_n(\sqrt{r})) = A(\mathbb{Q}_n(\sqrt{r})) = \{id\}$ from Theorem 6.2.3, and $\text{rank}_2 A_\Sigma(K_n) = 1$ from Theorem 6.1.1. The quadratic extension $K_n/\mathbb{Q}_n(\sqrt{r})$ is ramified at all primes in $S \setminus \Sigma = S$, and unramified outside S. Theorem 3.1

of [61] states that if $F/\mathfrak{f}$ is a quadratic extension unramified outside S and ramified at all primes in $S \setminus \Sigma$ with $A_\Sigma(\mathfrak{f}) = \{id\}$, then $\text{rank}_2 A_S(\mathfrak{f}) = 1 + \text{rank}_2 A_\Sigma(F)$. Therefore, it is immediate that $\text{rank}_2 A_{\{p\}}(\mathbb{Q}_n(\sqrt{r})) = 1 + \text{rank}_2 A_\Sigma(K_n) = 1 + \text{rank}_2 A(K_n) = 2$. □

Remark 6.4.5. *As $A(K_n)$ is cyclic for each n, by Burnside's basis theorem, $\tilde{L}(K_n) = L(K_n)$. Thus, $\tilde{L}(k_n) = \tilde{L}(K_n) = L(K_n)$. This also implies that $L(K_\infty) = \tilde{L}(K_\infty)$ is the maximal unramified 2-extension of k_∞, which clearly is a finite extension of k_∞.*

6.5 An equivalent criteria for $\#A(K_n) = \#A(\mathbb{Q}_n(\sqrt{p}))$

In view of part 1 of Lemma 6.4.3, it is imperative to understand the action of τ on $A(K_n)$, where $\text{Gal}(K_n/\mathbb{Q}_n(\sqrt{p})) = \langle \tau \rangle$. Firstly, we note an elementary consequence of Lemma 6.4.3.

Proposition 6.5.1. *For $\text{Gal}(K_n/\mathbb{Q}_n(\sqrt{p})) = \langle \tau \rangle$, τ acts on $A(K_n)$ as inverse if and only if $\#A(K_n) = 2$.*

Proof. As given in Case 1 of Lemma 6.4.3, τ acting as inverse on $A(K_n)$ implies that $A(K_n)^{\tau+1} = \{id\}$ and $\#A(K_n) = 2$. Conversely, suppose $A(K_n) = \{id, [\mathfrak{b}]\}$. If $[\mathfrak{b}]^\tau = id$, then $\mathfrak{b}^\tau$ must be principal, which also implies that $\mathfrak{b}$ is principal, which is a contradiction. Therefore, $[\mathfrak{b}]^\tau = [\mathfrak{b}] = [\mathfrak{b}]^{-1}$. □

Suppose $A(K_n) = \langle [\mathfrak{b}] \rangle$. If $\#A(K_n) = 2$, then from Proposition 6.5.1, τ acts as inverse on $A(K_n)$. This is equivalent to $[\mathfrak{b}]^\tau = [\mathfrak{b}]$, because the order of $[\mathfrak{b}]$ is equal to 2. Otherwise, if $\#A(K_n) \geq 4$, then $\#A(K_n)^{\tau+1} = \#A(K_n)/2$, and $A(K_n)$ is cyclic together imply that $A(K_n)^{\tau+1} = \langle\ [\mathfrak{b}]^2\ \rangle$. Since every element of $A(K_n)^{\tau+1}$ is fixed by τ, and $A(K_n)$ is a Galois module, we have $([\mathfrak{b}]^\tau)^2 = ([\mathfrak{b}]^2)^\tau = [\mathfrak{b}]^2$. For a finite cyclic 2-group G, the map $x \mapsto x^2$ has exactly two elements in the kernel, namely the identity and the element of order 2. Therefore, if $([\mathfrak{b}]^\tau)^2 = [\mathfrak{b}]^2$, then $[\mathfrak{b}]^\tau = [\mathfrak{b}]$ or $[\mathfrak{b}]^\tau = [\mathfrak{b}] \cdot [\mathfrak{a}]$, where $o([\mathfrak{a}]) = 2$.

Remark 6.5.2. *We recall from Lemma 6.4.3 that $\text{Gal}(K_n/\mathbb{Q}_n(\sqrt{r})) = \langle \sigma \rangle$, and it acts as inverse on $A(K_n)$. From the above discussion, it is readily available that $[\mathfrak{b}]^{\sigma\tau} = ([\mathfrak{b}]^{-1})^\tau = ([\mathfrak{b}]^\tau)^{-1} = [\mathfrak{b}]^{-1}$ or $[\mathfrak{b}]^{-1} \cdot [\mathfrak{a}]$.*

Let K/F be an unramified quadratic extension with $\text{Gal}(K/F) = \langle \sigma \rangle$. If j is the lifting map between the respective class groups, then $\#Ker(j) = 2 \cdot [E(F) : N_{K/F}(E(K))]$. The

second factor $[E(F) : N_{K/F}(E(K))]$ can be seen in Equation (1.5) of Theorem 1.4.3. Thus, $\#Ker(j)$ will be a nontrivial power of 2, say 2^r. As a result, $Ker(j)$ and $Ker(j) \cap N_{K/F}(\mathcal{C}l_K)$ must be contained in $A(F)$. Hence, it is sufficient to consider $Ker(j) \cap N_{K/F}(A(K))$ for extensions of degrees of powers of 2. Furthermore, from Equation (6.2), there exists $s \geq 0$ such that $[{}_\nu\mathcal{C}l_K : \mathcal{C}l_K^{1-\sigma}] = \big(\#Ker(j) \cap N_{K/F}(\mathcal{C}l_K)\big) = 2^s$. This implies that for every $[x] \in {}_\nu\mathcal{C}l_K$, there exists $[y] \in \mathcal{C}l_K$ such that $[x]^{2^s} = [y]^{1-\sigma}$. If $[x]$ belongs to the odd part of $\mathcal{C}l_K$ (that is, $[x] \notin A(K)$), then there exists an odd $t \geq 0$ such that $[x]^t = id$. As t and 2^s are relatively prime, there exist integers x_0 and y_0 such that $x_0 2^s + y_0 t = 1$. Therefore,

$$[x] = [x]^{x_0 2^s + y_0 t} = [x]^{x_0 2^s} = ([y]^{1-\psi})^{x_0} = ([y]^{x_0})^{1-\psi},$$

which means that $[x]$ belongs to ${\mathcal{C}l_K}^{1-\sigma}$. This demonstrates that the odd part of ${}_\nu\mathcal{C}l_K$ is contained in ${\mathcal{C}l_K}^{1-\sigma}$. The reverse containment is clear as ${\mathcal{C}l_K}^{1-\sigma} \subseteq {}_\nu\mathcal{C}l_K$. Therefore, the odd part of the subgroups ${}_\nu\mathcal{C}l_K$ and ${\mathcal{C}l_K}^{1-\sigma}$ are equal. Hence, it is enough to consider the even part of the class group to evaluate $[{}_\nu\mathcal{C}l_K : {\mathcal{C}l_K}^{1-\sigma}]$, that is,

$$[{}_\nu\mathcal{C}l_K : {\mathcal{C}l_K}^{1-\sigma}] = [{}_\nu A(K_n) : A(K)^{1-\sigma}] = \#\left(Ker(j) \cap N_{K/F}(A(K))\right),$$

where ${}_\nu A(K_n) := A(K_n)^2 = A(K_n)^{\tau+1}$. We now prove the following result, which will help us realize the action of τ on $A(K_n)$ from the possibilities stated prior to Remark 6.5.2.

Lemma 6.5.3. *For $n \geq 1$, $\mathrm{Gal}(K_n/\mathbb{Q}_n(\sqrt{p})) = \langle\tau\rangle$, τ acts as identity on $A(K_n)$. Hence, $\sigma\tau$ acts as the inverse on $A(K_n)$.*

Proof. Let $A(K_n) = \langle[\mathfrak{b}]\rangle$. By Proposition 6.5.1, if $\#A(K_n) = 2$, then τ acts as inverse. However, the order of $[\mathfrak{b}]$ is equal to 2 implies $[\mathfrak{b}] = [\mathfrak{b}]^{-1} = [\mathfrak{b}]^\tau$.

If $\#A(K_n) = 4$, then $[\mathfrak{b}]^\tau = [\mathfrak{b}] \cdot [\mathfrak{a}]$ is the same as $[\mathfrak{b}]^\tau = [\mathfrak{b}]^{-1}$, and $\#A(K_n)^{\tau+1} = 1$. This is a contradiction to part 1 of Lemma 6.4.3, and thus, $[\mathfrak{b}]^\tau = [\mathfrak{b}]$.

If $\#A(K_n) \geq 8$, then, $\mathrm{Gal}(L(K_n)/k_n)$ is a nonabelian group of order at least 16. By Remark 6.4.5 it is obvious that $\mathrm{Gal}(L(K_n)/k_n) = \mathrm{Gal}(\tilde{L}(k_n)/k_n) \neq Q_8,\ (2,2)$. This rejects Cases 1 and 2 of Theorem 6.2.6. Suppose $[\mathfrak{b}]^\tau = [\mathfrak{b}] \cdot [\mathfrak{a}]$. Then by Remark 6.5.2, $[\mathfrak{b}]^{\sigma\tau} = [\mathfrak{b}]^{-1} \cdot [\mathfrak{a}]$. We consider the unramified quadratic extension K_n/k_n and define $\nu = 1 + \sigma\tau$. For $[x] \in A(K_n)$, there exists an $s \geq 0$, such that $[x] = [\mathfrak{b}]^s$, and $[x]^{\sigma\tau} = ([\mathfrak{b}]^s)^{\sigma\tau} = [\mathfrak{b}]^{-s} \cdot [\mathfrak{a}]^s$. Thus,

$$[x]^{\sigma\tau} = \begin{cases} [x]^{-1} & \text{if } s \text{ is even,} \\ [x]^{-1} \cdot [\mathfrak{a}] & \text{if } s \text{ is odd.} \end{cases}$$

Consequently, every even power of $[\mathfrak{b}]$ will belong to ${}_\nu A(K_n) := \{[x] \in A(K_n) : [x]^\nu = id\}$, and conversely. Therefore, ${}_\nu A(K_n) = A(K_n)^2 = A(K_n)^{\tau+1}$. Next, σ acts as the inverse implies $A(K_n)^{1-\sigma\tau} = A(K_n)^{\tau+1}$. Thus, we obtain

$$[{}_\nu A(K_n) : A(K_n)^{1-\sigma\tau}] = \#(Ker(j) \cap N_{K_n/k_n}(A(K_n))) = 1,$$

where we let j to be the lifting map from $A(k_n)$ to $A(K_n)$. This means that if $[\mathfrak{b}]^\tau = [\mathfrak{b}] \cdot [\mathfrak{a}]$, then K_n/k_n satisfies Taussky Condition (B). Appealing to Theorem 6.2.6, we find that Case 3 (a) holds, and $\mathrm{Gal}(\tilde{L}(k_n)/k_n)$ is a semi-dihedral group of order at least 16. For this n, and the cyclotomic $\mathbb{Z}_2$-extension of the field k_n, we have $(k_n)_\infty = k_\infty$ and $X((k_n)_\infty) = X(k_\infty) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Since $\mathrm{Gal}(\tilde{L}(k_n)/k_n)$ is semidihedral, from Theorem 6.2.7, $\mathrm{Gal}(\tilde{L}((k_n)_\infty)/(k_n)_\infty) = \mathrm{Gal}(\tilde{L}(k_\infty)/k_\infty)$ must be semidihedral. But this contradicts Theorem 6.2.8. Therefore, if $\#A(K_n) \geq 8$, then $[\mathfrak{b}]^\tau = [\mathfrak{b}]$. □

6.5.1 Proof of Theorem 6.1.4

If $n = 0$, then from Lemma 6.4.2 and the paragraph before Proposition 6.4.1, $\#A(K_0) = \#A(\mathbb{Q}_0(\sqrt{p}))$. For any n, we know that $\mathrm{Gal}(L(K_n)/K_n) \cong A(K_n)$ is an abelian extension and $\mathrm{Gal}(K_n/\mathbb{Q}_n(\sqrt{p})) = \langle\tau\rangle$ is of order 2. Since $K_n/\mathbb{Q}_n(\sqrt{p})$ is a quadratic extension and $L(K_n)$ is the 2-Hilbert class field of K_n, $L(K_n)/\mathbb{Q}_n(\sqrt{p})$ is a Galois extension. As τ acts as 1 on $\mathrm{Gal}(L(K_n)/K_n)$ from Lemma 6.5.3, $L(K_n)/\mathbb{Q}_n(\sqrt{p})$ is a finite abelian extension.

We now refer to Theorem 6.3.1 for the ramified extension $K_n/\mathbb{Q}_n(\sqrt{p})$ for $n \geq 1$. With the notation employed in Theorem 6.3.1, for the extension $K_n/\mathbb{Q}_n(\sqrt{p})$, we have $\ell = 2$, $N = 1$, $\psi = \tau$, and $m(K_n) = 1$ (from Lemma 6.5.3). For these values, $s = 0$, $m = 1$, and $e = 1$. Therefore, Theorem 6.3.1 for $K_n/\mathbb{Q}_n(\sqrt{p})$ can be restated as: $[x] \in A(\mathbb{Q}_n(\sqrt{p}))$ capitulates in $A(K_n)$ if there exists $[y] \in A(K_n)$ of order 2 such that $N_{K_n/\mathbb{Q}_n(\sqrt{p})}([y]) = [x]$.

Suppose $\#A(K_n) = \#A(\mathbb{Q}_n(\sqrt{p}))$. Then, since $N_{K_n/\mathbb{Q}_n(\sqrt{p})}$ is surjective, it must be an isomorphism. As $n \geq 1$, $A(\mathbb{Q}_n(\sqrt{p}))$ contains an element of order 2, say $[x]$. Let $[y] \in A(K_n)$ be the pre-image of $[x]$ under $N_{K_n/\mathbb{Q}_n(\sqrt{p})}$. Then, the order of $[y]$ must be equal to 2. From the previous paragraph, it is clear that $[x]$ capitulates in $A(K_n)$.

Conversely, suppose some non-trivial ideal class in $A(\mathbb{Q}_n(\sqrt{p}))$ capitulates in $A(K_n)$. Then, the kernel of the lifting map $j : A(\mathbb{Q}_n(\sqrt{p})) \to A(K_n)$ must contain some $[x] \in A(\mathbb{Q}_n(\sqrt{p}))$ of order 2 that capitulates in $A(K_n)$. Let $[y] \in A(K_n)$ be a class such that $N_{K_n/\mathbb{Q}_n(\sqrt{p})}([y]) = [x]$. Applying Equation (1.7) and Lemma 6.5.3 on $[x]$ and $[y]$, we observe:

$$j \circ N_{K_n/\mathbb{Q}_n(\sqrt{p})}[y] = [y]^{1+\tau} \Rightarrow j[x] = id = [y]^2.$$

Therefore, the order of $[y]$ is at most 2. But as $[x]$ is non-trivial, the order of $[y]$ must be precisely equal to 2. This further means that the unique element of order 2 in $A(K_n)$ (as $A(K_n)$ is cyclic) maps to a non-trivial element of $A(\mathbb{Q}_n(\sqrt{p}))$. From part 2 of Lemma 6.4.3, it is immediate that the kernel of $N_{K_n/\mathbb{Q}_n(\sqrt{p})}$ can have at most 2 elements. Thus, in this case, the kernel of $N_{K_n/\mathbb{Q}_n(\sqrt{p})}$ must be trivial. From this, we realize that the norm map $N_{K_n/\mathbb{Q}_n(\sqrt{p})}$ is an isomorphism from $A(K_n)$ to $A(\mathbb{Q}_n(\sqrt{p}))$, and hence, the order of these two groups must be equal. □

Proof of Corollary 6.1.5

The field $L(K_n)$ is unramified over K_n, and K_n is ramified over $\mathbb{Q}_n(\sqrt{p})$ at primes above 2 and r. Hence, $L(K_n)$ is also ramified over $\mathbb{Q}_n(\sqrt{p})$ at primes above 2 and r, each with ramification index 2. Therefore, $L(K_n)$ must be contained in the maximal abelian extension of $\mathbb{Q}_n(\sqrt{p})$ unramified outside primes above 2 and r. The field $L(k_n) = K_n(\sqrt{p_1}) = \mathbb{Q}_n(\sqrt{p}, \sqrt{r}, \sqrt{p_1})$ is a biquadratic extension of $\mathbb{Q}_n(\sqrt{p})$. Now, $\mathrm{Gal}(L(K_n)/\mathbb{Q}_n(\sqrt{p}))$ contains a biquadratic quotient namely, $\mathrm{Gal}(L(k_n)/\mathbb{Q}_n(\sqrt{p}))$. Thus, $\mathrm{Gal}(L(K_n)/\mathbb{Q}_n(\sqrt{p}))$ must have rank at least 2, and hence the result. □

6.6 Order of $A(K_1)$

We first identify the behaviour of the ideal $r\mathcal{O}_{\mathbb{Q}_1}$ in certain extensions of $\mathbb{Q}_1$ which will be essential in the proof of Theorem 6.1.6.

Lemma 6.6.1. *Let r and p be prime numbers satisfying Condition (6.1) and p_1, p_2 be totally positive prime elements in $\mathbb{Q}_1$ such that $p = p_1 \cdot p_2$ in $\mathbb{Q}_1$. Then, the following hold:*

1. *If $r \equiv 3 \pmod 8$, then the prime ideal $r\mathcal{O}_{\mathbb{Q}_1}$ is inert in the extension $\mathbb{Q}_1(\sqrt{p_i})/\mathbb{Q}_1$, for $i = 1, 2$.*

2. *If* $r \equiv 7 \pmod 8$ *and* $r\mathcal{O}_{\mathbb{Q}_1} = \langle r_1 \rangle \cdot \langle r_2 \rangle$ *in* $\mathbb{Q}_1$*, then exactly one of* $\langle r_1 \rangle$ *and* $\langle r_2 \rangle$ *is inert in* $\mathbb{Q}_1(\sqrt{p_1})/\mathbb{Q}_1$ *(and similarly in* $\mathbb{Q}_1(\sqrt{p_2})/\mathbb{Q}_1$*). Also, if* $\langle r_1 \rangle$ *is inert in* $\mathbb{Q}_1(\sqrt{p_1})$*, then it must split in* $\mathbb{Q}_1(\sqrt{p_2})$*.*

Proof. (1). Let $r \equiv 3 \pmod 8$. Since $p \equiv 1 \pmod 4$, from Condition (6.1), $\left(\frac{r}{p}\right) = -1$. This indicates that r is not a square modulo p. As $p \equiv 1 \pmod 8$, the ideal $p\mathcal{O}_{\mathbb{Q}_1}$ can be expressed as $\langle p_1 \rangle \cdot \langle p_2 \rangle$, with $\mathcal{O}_{\mathbb{Q}_1}/\langle p_i \rangle \cong \mathbb{Z}/p\mathbb{Z}$ (for $i = 1, 2$). Therefore, r is not a square modulo p_i in $\mathcal{O}_{\mathbb{Q}_1}$. Using the generalization of Legendre and Jacobi symbols given by Definition 1.6.2, Equation (1.9), and Proposition 1.6.3, we obtain $\left(\frac{r}{p_i}\right) = -1$. The extension $\mathbb{Q}_1(\sqrt{p_i})/\mathbb{Q}_1$ is quadratic, with the minimal polynomial of $\sqrt{p_i}$ being $f(x) = x^2 - p_i$. Since $r \equiv 3 \pmod 8$, the ideal $r\mathcal{O}_{\mathbb{Q}_1}$ is prime in $\mathbb{Q}_1$. Now, whether $r\mathcal{O}_{\mathbb{Q}_1}$ splits or remains inert in $\mathbb{Q}_1(\sqrt{p_i})$ depends on the factorization of f modulo $r\mathcal{O}_{\mathbb{Q}_1}$ in $\mathcal{O}_{\mathbb{Q}_1}$ (by Theorem 1.2.7). If p_i is not a square modulo $r\mathcal{O}_{\mathbb{Q}_1}$, then $r\mathcal{O}_{\mathbb{Q}_1}$ is inert in $\mathbb{Q}_1(\sqrt{p_i})/\mathbb{Q}_1$. Thus, we need to evaluate $\left(\frac{p_i}{r}\right)$.

We produce a proof for p_1, as a similar proof would hold for p_2 as well. Our aim is to use Hecke's quadratic reciprocity stated in Theorem 1.6.4. Since $\mathbb{Q}_1/\mathbb{Q}$ is a real quadratic extension, $R = 2$, $x = p_1, y = r$, $(x_1, y_1) = (p_1, r)$, and $(x_2, y_2) = (p_2, r)$. As p_i's are totally positive and $r > 0$, $s(x_1, y_1) = s(x_2, y_2) = 0$. Also, from the proof of Proposition 5.3.3, we find that modulo 4, p_i's are congruent to 1, or $3 + 2\sqrt{2} = (1 + \sqrt{2})^2$. Therefore, from Theorem 1.6.4, we have $\left(\frac{p_1}{r}\right) = (-1)^0 \cdot (-1)^0 \cdot (-1) = -1$. Due to Proposition 1.6.3, p_1 is not a square modulo $r\mathcal{O}_{\mathbb{Q}_1}$ in $\mathbb{Q}_1$. Hence, $r\mathcal{O}_{\mathbb{Q}_1}$ is inert in $\mathbb{Q}_1(\sqrt{p_1})/\mathbb{Q}_1$.

(2). Let $r \equiv 7 \pmod 8$. Then, there exits $r_1, r_2 \in \mathbb{Q}_1$ such that $r\mathcal{O}_{\mathbb{Q}_1}$ can be factorized as $r\mathcal{O}_{\mathbb{Q}_1} = \langle r_1 \rangle \cdot \langle r_2 \rangle$. In this case, $\mathbb{Z}/r\mathbb{Z} \cong \mathcal{O}_{\mathbb{Q}_1}/\langle r_i \rangle$ for $i = 1, 2$. By Definition 1.6.2 and Equation (1.9),

$$\left(\frac{p}{r}\right) = \left(\frac{p}{r_i}\right) = \left(\frac{p_1 p_2}{r_i}\right) = -1.$$

Hence, for each i, exactly one of $\left(\frac{p_1}{r_i}\right)$ and $\left(\frac{p_2}{r_i}\right)$ must be equal to -1, and the other symbol must be equal to 1. We furnish proof for $i = 1$ as the other case can be dealt with similarly. Without loss of generality, let $\left(\frac{p_1}{r_1}\right) = -1$ (this implies that $\langle r_1 \rangle$ is inert in $\mathbb{Q}_1(\sqrt{p_1})/\mathbb{Q}_1$). In $\mathbb{Q}_1$, the conjugates of r_1 are r_1 and r_2, and the conjugates of p_1 are p_1 and p_2. Again applying Theorem 1.6.4 on p_1 and r_1, we obtain $\left(\frac{r_1}{p_1}\right) = -1$. Further, by multiplicativity of the Jacobi symbol, we have

$$-1 = \left(\frac{r}{p}\right) = \left(\frac{r_1 r_2}{p_1}\right) = -1 \cdot \left(\frac{r_2}{p_1}\right).$$

Finally by Theorem 1.6.4, $\left(\frac{r_2}{p_1}\right) = \left(\frac{p_1}{r_2}\right) = 1$. This means that if $\langle r_1 \rangle$ is inert in $\mathbb{Q}_1(\sqrt{p_1})$, then $\langle r_2 \rangle$ must be a split prime in $\mathbb{Q}_1(\sqrt{p_1})$. Also, $\left(\frac{p}{r}\right) = -1$ implies that definitely, one of the ideals $\langle r_1 \rangle$ and $\langle r_2 \rangle$ must be inert in $\mathbb{Q}_1(\sqrt{p_1})$. □

As p_1 and p_2 are totally positive in $\mathbb{Q}_1$ and congruent to squares modulo 4, from Theorem 1.6.4, $\left(\frac{p_1}{p_2}\right) = \left(\frac{p_2}{p_1}\right)$. Therefore, the prime ideal $\langle p_1 \rangle$ remains inert in $\mathbb{Q}_1(\sqrt{p_2})/\mathbb{Q}_1$ if and only if $\langle p_2 \rangle$ remains inert in $\mathbb{Q}_1(\sqrt{p_1})/\mathbb{Q}_1$. The next lemma is a consequence of this assumption.

Lemma 6.6.2. *Let $r \equiv 3 \pmod 8$, and suppose that the prime ideal $\langle p_1 \rangle$ of $\mathbb{Q}_1$ is inert in $\mathbb{Q}_1(\sqrt{p_2})/\mathbb{Q}_1$. If $T_2 := \mathbb{Q}_1(\sqrt{rp_1}, \sqrt{p_2})$, then $\operatorname{rank}_2(A(T_2)) \leq 1$.*

Proof. For simplicity, we shall use F to denote the field $\mathbb{Q}_1(\sqrt{p_2})$ in this proof. Since $\#A(\mathbb{Q}_1(\sqrt{p})) = 2$, by Burnside's basis theorem, $\#A(\mathbb{Q}_1(\sqrt{p}, \sqrt{p_1})) = 1$. Now, $p_1\mathcal{O}_F$ is ramified in $\mathbb{Q}_1(\sqrt{p}, \sqrt{p_1})/F$. By Theorem 1.5.6, the norm map between class groups of these fields must be surjective, and hence $\#A(F) = 1$. We note from Lemma 5.3.2 that the only prime ramified in $F/\mathbb{Q}_1$ is $\langle p_2 \rangle$. So, if we appeal to Equation (1.5) for this extension, then we obtain $1 = \#A(\mathbb{Q}_1) \times \frac{2^{1-1}}{\left[E(\mathbb{Q}_1) : N_{F/\mathbb{Q}_1}(E(F))\right]}$. Therefore, every unit of $\mathbb{Z}[\sqrt{2}] = \mathcal{O}_{\mathbb{Q}_1}$ is the norm of some unit of $\mathcal{O}_F$. In particular, there exists $u \in \mathcal{O}_F$ such that its norm over $\mathbb{Q}_1$ is $1 + \sqrt{2}$.

It follows from our assumption, part 1 of Lemma 6.6.1, and Proposition 5.3.3 that the primes of F ramified in T_2 are $p_1\mathcal{O}_F$, $r\mathcal{O}_F$, and ℓ, respectively, where ℓ is the unique prime ideal above 2. Consequently, applying Equation (1.4) for T_2/F produces

$$2^{\operatorname{rank}_2 A(T_2)} = \frac{2^{3-1}}{\left[E(F) : E(F) \cap N_{T_2/F}(T_2^\times)\right]} \leq 2^2.$$

Suppose $\left[E(F) : E(F) \cap N_{T_2/F}(T_2^\times)\right] = 1$. Then, there exists $\alpha \in T_2^\times$, such that its norm over F is equal to u, where u is defined in the previous paragraph. In that case, $N_{T_2/\mathbb{Q}_1}(\alpha) = N_{F/\mathbb{Q}_1}(u) = 1 + \sqrt{2}$. Moreover, $N_{T_2/\mathbb{Q}_1}(\alpha) = N_{k_1/\mathbb{Q}_1}(N_{T_2/k_1}(\alpha)) = 1 + \sqrt{2}$, as $T_2 = \mathbb{Q}_1(\sqrt{rp_1}, \sqrt{p_2}) = \mathbb{Q}_1(\sqrt{rp}, \sqrt{p_2}) = k_1(\sqrt{p_2})$. However, as $r \equiv 3 \pmod 8$, this is a contradiction to Proposition 5.4.3 which asserts that $1 + \sqrt{2}$ is not a norm

in the extension $\mathbb{Q}_1(\sqrt{d})/\mathbb{Q}_1$ if d has a prime factor congruent to 3 (mod 4). Thus, $\left[E(F) : E(F) \cap N_{T_2/F}(T_2^{\times})\right] \geq 2$, and $\text{rank}_2(A(T_2)) \leq 1$. □

Let a, b be positive integers such that $p_1 = a+b\sqrt{2}$ and $p_2 = a-b\sqrt{2}$, so that $p = a^2-2b^2$. This means that $p_1 \equiv 2a \pmod{p_2}$. As $\mathcal{O}_{\mathbb{Q}_1}/\langle p_i \rangle \cong \mathbb{Z}/p\mathbb{Z}$, 2 is a square modulo p implies that 2 is a square modulo p_2 in $\mathbb{Q}_1$. Therefore, $\left(\frac{p_1}{p_2}\right) = -1$ if and only if $\left(\frac{a}{p_2}\right) = -1$, which is equivalent to $\left(\frac{a}{p}\right) = -1$. Also, $\left(\frac{2}{p}\right)_4 = -1$ means that 2 is not a fourth power modulo p. Hence, the square root of 2 modulo p is not a square itself. Now, $a^2 \equiv 2b^2 \pmod{p}$ implies $a \equiv \pm tb \pmod{p}$, where $t^2 \equiv 2 \pmod{p}$. Since -1 is also a square modulo p, $\left(\frac{a}{p}\right) = -1$ is equivalent to $\left(\frac{b}{p}\right) = 1$.

6.6.1 Proof of Theorem 6.1.6

From the discussion in the previous paragraph, it is evident that if $p = a^2 - 2b^2$, then, $\left(\frac{a}{p}\right) = -1$ if and only if $\left(\frac{p_1}{p_2}\right) = \left(\frac{p_2}{p_1}\right) = -1$, i.e., the prime ideal $\langle p_1 \rangle$ of $\mathbb{Q}_1$ is inert in $\mathbb{Q}_1(\sqrt{p_2})/\mathbb{Q}_1$. From Lemma 6.4.3, it is direct that $2 \leq \#A(K_1) \leq 4$. We suppose that $\#A(K_1) = 4$. Then, from Theorem 6.1.4, $L(K_1)$ must be an abelian extension of $\mathbb{Q}_1(\sqrt{p})$ of degree 8. We observe that $\mathbb{Q}_1(\sqrt{p}) \subset K_1 \subset L(K_1)$, where $L(K_1)/K_1$ is cyclic of degree 4. On the other hand, $\mathbb{Q}_1(\sqrt{p}, \sqrt{r}, \sqrt{p_1})/\mathbb{Q}_1(\sqrt{p}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ is a subextension of $L(K_1)/\mathbb{Q}_1(\sqrt{p})$. Putting these together, we infer that $L(K_1)/\mathbb{Q}_1(\sqrt{p}) \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

A consequence of $\#A(K_1) = 4$ is that $L(k_1) \subsetneq L(K_1)$ and we have the field extension $k_1 \subset K_1 \subset L(k_1) \subset L(K_1) \subset L(L(k_1))$ By Burnside's basis theorem,

$$L(L(k_1)) \supset L(K_1) = \tilde{L}(K_1) = \tilde{L}(k_1) \supset L(L(k_1)).$$

Therefore, $L(K_1) = L(L(k_1))$. We now refer to the extension:

$$\mathbb{Q}_1 \subset \mathbb{Q}_1(\sqrt{p}) \subset K_1, \mathbb{Q}_1(\sqrt{p}, \sqrt{p_1}) \subset L(k_1) \subset L(K_1).$$

Since $L(K_1)$ is the 2-Hilbert class field of $L(k_1)$, it must be a Galois extension of degree 4 over $\mathbb{Q}_1(\sqrt{p_1}, \sqrt{p})$. Then, $L(k_1)/\mathbb{Q}_1(\sqrt{p_1}, \sqrt{p})$ is a subextension of $L(K_1)/\mathbb{Q}_1(\sqrt{p}, \sqrt{p_1})$ ramified at primes above 2 and r, whereas $L(K_1)/L(k_1)$ is unramified. Summing up, by Layer theorem (Theorem 1.2.9), $L(K_1)/\mathbb{Q}_1(\sqrt{p}, \sqrt{p_1})$ cannot be a cyclic extension of degree 4. Hence, $L(K_1)/\mathbb{Q}_1(\sqrt{p_1}, \sqrt{p})$ has to be an extension of type $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Thus, there exist fields F_1, F_2 different from $L(k_1)$ such that

$$\mathbb{Q}_1(\sqrt{p_1},\sqrt{p}) \subset F_1, F_2 \subset L(K_1).$$

Likewise, as $L(k_1)/\mathbb{Q}_1(\sqrt{r},\sqrt{p_1})$ is a quadratic extension ramified at the prime(s) above p_2, $L(K_1)/\mathbb{Q}_1(\sqrt{r},\sqrt{p_1})$ is of the form $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$. Therefore, there exist intermediate fields H_1 and H_2 distinct from $L(k_1)$ such that

$$\mathbb{Q}_1(\sqrt{r},\sqrt{p_1}) \subset H_1, H_2 \subset L(K_1).$$

Throughout this proof, the fields F_1, F_2, H_1, and H_2 will be fixed.

Our assumption $\#A(K_1) = 4$ also yields that $L(K_1)/k_1$ is an unramified, non-abelian extension of degree 8. That way, $L(K_1)/\mathbb{Q}_1$ is a Galois, non-abelian extension of degree 16. From the previous paragraphs, we infer that $\mathrm{Gal}(L(K_1)/\mathbb{Q}_1)$ has the following properties:

- It has at least two subgroups of type $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$ (namely, $\mathrm{Gal}(L(K_1)/\mathbb{Q}_1(\sqrt{p},\sqrt{p_1}))$ and $\mathrm{Gal}(L(K_1)/\mathbb{Q}_1(\sqrt{r},\sqrt{p_1}))$).
- It has a subgroup of type $\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$ (corresponding to $\mathrm{Gal}(L(K_1)/\mathbb{Q}_1(\sqrt{p}))$).
- It has a quotient of the form $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$ (with respect to $\mathbb{Q}_1(\sqrt{p},\sqrt{r},\sqrt{p_1})/\mathbb{Q}_1$).
- There are least 7 subextensions of degree 2 over $\mathbb{Q}_1$ contained in $L(K_1)$. These are $\mathbb{Q}_1(\sqrt{p})$, $\mathbb{Q}_1(\sqrt{r})$, $k_1 = \mathbb{Q}_1(\sqrt{pr})$, $\mathbb{Q}_1(\sqrt{p_1})$, $\mathbb{Q}_1(\sqrt{p_2})$, $\mathbb{Q}_1(\sqrt{rp_1})$, and $\mathbb{Q}_1(\sqrt{rp_2})$. Therefore, $\mathrm{Gal}(L(K_1)/\mathbb{Q}_1)$ has at least 7 quotients of order 2.

None of the groups mentioned in Remark 6.2.9 can be isomorphic to $\mathrm{Gal}(L(K_1)/\mathbb{Q}_1)$ as their properties stated therein do not match with our current observations. The groups of order 16 that are remaining to be pondered upon are $Q_8\oplus\mathbb{Z}/2\mathbb{Z}$, $D_8 \curlyvee \mathbb{Z}/4\mathbb{Z}$ (the central product of D_8 and $\mathbb{Z}/4\mathbb{Z}$), and $D_8\oplus\mathbb{Z}/2\mathbb{Z}$. Let $\mathfrak{G} = \mathrm{Gal}(L(K_1)/\mathbb{Q}_1)$. We deal with the possibility of $\mathfrak{G}$ being equal to each of the aforementioned groups.

Case 1. $\mathfrak{G} = Q_8\oplus\mathbb{Z}/2\mathbb{Z}$: In this case, $\mathfrak{G}$ has exactly three subgroups of order 2, all of which are normal. Thus, by Galois correspondence, there exist fields M_i $(i = 1, 2, 3)$ such that for each i, $\mathbb{Q}_1 \subset M_i \subset L(K_1)$, $[L(K_1) : M_i] = 2$, and $M_i/\mathbb{Q}_1$ is Galois. One of these is $L(k_1)$, and we fix $M_3 = L(k_1)$. We already have five fields, namely F_1, F_2, H_1, H_2, and $L(k_1)$ above which $L(K_1)$ is quadratic. Since $\mathfrak{G}$ has only three subgroups of order 2, some of these fields must be equal. Clearly, $F_1 \neq F_2 \neq L(k_1)$, and $H_1 \neq H_2 \neq L(k_1)$. Therefore, without loss of generality, $M_1 = F_1 = H_1$ and $M_2 = F_2 = H_2$. By definition, $\mathbb{Q}_1(\sqrt{p_1},\sqrt{p}) \subset F_1$ and $\mathbb{Q}_1(\sqrt{r},\sqrt{p_1}) \subset H_1$. That way, M_1 must contain $\mathbb{Q}_1(\sqrt{p_1},\sqrt{p},\sqrt{r}) = M_3$ which is not possible. A similar contradiction occurs with M_2 as well. Therefore, $\mathfrak{G} \neq Q_8\oplus\mathbb{Z}/2\mathbb{Z}$.

Case 2. $\mathfrak{G} = D_8 \curlyvee \mathbb{Z}/4\mathbb{Z}$: The group $\mathfrak{G}$ has only one normal subgroup of order 2. Since $L(k_1)/\mathbb{Q}_1$ is Galois, we note that F_1 and F_2 cannot be Galois over $\mathbb{Q}_1$. Thus, F_1 and F_2 are isomorphic field extensions over $\mathbb{Q}_1$ (as their compositum $L(K_1)$ is Galois over $\mathbb{Q}_1$) with isomorphism θ. Then, θ is also an automorphism of $\mathbb{Q}_1(\sqrt{p}, \sqrt{p_1})$ that fixes $\mathbb{Q}_1$. We break this case into two subcases depending on modulo 8 conditions on r.

(1). When $r \equiv 3 \pmod 8$: Since $p \equiv 1 \pmod 8$ and $\left(\frac{p}{r}\right) = -1$, the prime ideals $\sqrt{2}\mathcal{O}_{\mathbb{Q}_1}$ and $r\mathcal{O}_{\mathbb{Q}_1}$ split in $\mathbb{Q}_1(\sqrt{p})$, where they can be factorized as $\ell_1 \cdot \ell_2$ and $\mathfrak{r}_1 \cdot \mathfrak{r}_2$, respectively. Next, from Proposition 5.3.3 and Lemma 6.6.1, we gather that for $i = 1, 2$, ℓ_i and $\mathfrak{r}_i$ remain inert in $\mathbb{Q}_1(\sqrt{p_1}, \sqrt{p})/\mathbb{Q}_1(\sqrt{p})$. We denote these primes ideals in $\mathbb{Q}_1(\sqrt{p_1}, \sqrt{p})$ as $\overline{\ell_i}$ and $\overline{\mathfrak{r}_i}$ for $i = 1, 2$. Given that $\#A(\mathbb{Q}_1(\sqrt{p}, \sqrt{p_1})) = 1$, the extensions $F_i/\mathbb{Q}_1(\sqrt{p}, \sqrt{p_1})$ must be ramified at some prime. Since the primes above 2 and r are the only ones that are ramified in $L(K_1)/\mathbb{Q}_1(\sqrt{p_1}, \sqrt{p})$, without loss of generality, we may assume that $\overline{\mathfrak{r}_1}$ is ramified in $F_1/\mathbb{Q}_1(\sqrt{p}, \sqrt{p_1})$. Let $\widetilde{\mathfrak{r}_1}$ be the prime above $\overline{\mathfrak{r}_1}$ in $F_1/\mathbb{Q}_1(\sqrt{p}, \sqrt{p_1})$. Then, $\theta(\widetilde{\mathfrak{r}_1})$ will be the prime above $\theta(\overline{\mathfrak{r}_1})$ in $F_2/\mathbb{Q}_1(\sqrt{p}, \sqrt{p_1})$. Here, $\theta(\overline{\mathfrak{r}_1})$ is the conjugate of $\overline{\mathfrak{r}_1}$ in $\mathbb{Q}_1(\sqrt{p}, \sqrt{p_1})$. But, $\mathfrak{r}_1$ is inert in $\mathbb{Q}_1(\sqrt{p_1}, \sqrt{p})/\mathbb{Q}_1(\sqrt{p})$ implies $\theta(\overline{\mathfrak{r}_1}) = \overline{\mathfrak{r}_1}$ in $\mathbb{Q}_1(\sqrt{p}, \sqrt{p_1})$. Therefore, $\theta(\widetilde{\mathfrak{r}_1})$ will be the prime above $\overline{\mathfrak{r}_1}$ in $F_2/\mathbb{Q}_1(\sqrt{p}, \sqrt{p_1})$. Since F_1 and F_2 are isomorphic, this implies that $\overline{\mathfrak{r}_1}$ is ramified in F_2 as well. Therefore, $\overline{\mathfrak{r}_1}$ is ramified in F_1, F_2, and $L(k_1)$, and consequently, it must be totally ramified in $L(K_1)/\mathbb{Q}_1(\sqrt{p_1}, \sqrt{p})$. This is not possible as $L(K_1)/L(k_1)$ is an unramified extension. On similar lines, we can also show that the primes $\overline{\mathfrak{r}_2}, \overline{\ell_1}$, and $\overline{\ell_2}$ cannot be ramified in $F_1/\mathbb{Q}_1(\sqrt{p}, \sqrt{p_1})$. But, this is a contradiction as some prime has to ramify in $F_1/\mathbb{Q}_1(\sqrt{p}, \sqrt{p_1})$.

(2). When $r \equiv 7 \pmod 8$: For $i = 1, 2$, $L(K_1)/\mathbb{Q}_1(\sqrt{p_i})$ is a Galois extension of degree 8. The subgroups of order 8 of $\mathfrak{G}$ can be D_8, Q_8, or $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. We have $\mathbb{Q}_1(\sqrt{p_i}) \subseteq \mathbb{Q}_1(\sqrt{p_i}, \sqrt{r})$, $\mathbb{Q}_1(\sqrt{p_i}, \sqrt{p}) \subset L(K_1)$, where $L(K_1)/\mathbb{Q}_1(\sqrt{p_i}, \sqrt{r})$ and $L(K_1)/\mathbb{Q}_1(\sqrt{p_i}, \sqrt{p})$ are Galois extensions of the type $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Consequently, $\mathrm{Gal}(L(K_1)/\mathbb{Q}_1(\sqrt{p_i})) \cong D_8$ for $i = 1, 2$, with F_1 and F_2 being isomorphic, non-Galois extensions of $\mathbb{Q}_1(\sqrt{p_i})$. We recall r_1 and r_2 defined in part (2) of Lemma 6.6.1, and fix $\left(\frac{p_1}{r_1}\right) = -1$ without loss of generality. Then, from part (2) of Lemma 6.6.1, $r_1\mathcal{O}_{\mathbb{Q}_1}$ is inert in $\mathbb{Q}_1(\sqrt{p_1})/\mathbb{Q}_1$ and $r_2\mathcal{O}_{\mathbb{Q}_1}$ splits in $\mathbb{Q}_1(\sqrt{p_1})/\mathbb{Q}_1$. In $\mathbb{Q}_1(\sqrt{p_1})/\mathbb{Q}_1$, let $\widetilde{r_1}$ be the prime ideal above $r_1\mathcal{O}_{\mathbb{Q}_1}$, and $r_2\mathcal{O}_{\mathbb{Q}_1(\sqrt{p_1})} = r_{21} \cdot r_{22}$. As $\mathbb{Q}_1(\sqrt{p_1}, \sqrt{p})/\mathbb{Q}_1$ is a biquadratic extension, we deduce that in the extension $\mathbb{Q}_1(\sqrt{p_1}, \sqrt{p})/\mathbb{Q}_1(\sqrt{p_1})$, we have the factorizations: $\widetilde{r_1} = \overline{r_{11}} \cdot \overline{r_{12}}$, $r_{21} = \overline{r_{21}}$, and $r_{22} = \overline{r_{22}}$. For each $i, j \in \{1, 2\}$, $\overline{r_{ij}}$ is ramified in the extension $L(k_1)/\mathbb{Q}_1(\sqrt{p_1}, \sqrt{p})$.

Since $L(K_1)/L(k_1)$ is an unramified extension, each $\overline{r_{ij}}$ has ramification index 2 in the biquadratic extension $L(K_1)/\mathbb{Q}_1(\sqrt{p_1},\sqrt{p})$. If F_2 is the inertia field of $\overline{r_{21}}$, then $\overline{r_{21}}$ must be ramified in $F_1/\mathbb{Q}_1(\sqrt{p_1},\sqrt{p})$. Repeating the arguments with the isomorphism θ presented in the last part of the subcase $r \equiv 3 \pmod 8$, we obtain that $\overline{r_{21}}$ must also be ramified in $F_2/\mathbb{Q}_1(\sqrt{p_1},\sqrt{p})$, which is a contradiction. Therefore, $\mathfrak{G} \neq D_8 \curlyvee \mathbb{Z}/4\mathbb{Z}$.

Case 3. $\mathfrak{G} = D_8 \oplus \mathbb{Z}/2\mathbb{Z}$: Again, we break this case into subcases depending on the modulo 8 conditions on r.

(1). When $r \equiv 3 \pmod 8$: The subgroups of order 8 of $\mathfrak{G}$ are of the type $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, and D_8. As $\#A(K_1) = 4$, in this case, $L(K_1)/k_1$ must be nonabelian and its Galois group must be isomorphic to D_8. The group D_8 has exactly one cyclic subgroup of order 4, and here it corresponds to the extension $L(K_1)/K_1$. The quadratic subextensions of k_1 other than K_1 are $T_1 = \mathbb{Q}_1(\sqrt{pr},\sqrt{p_1})$, and $T_2 = \mathbb{Q}_1(\sqrt{pr},\sqrt{p_2}) = \mathbb{Q}_1(\sqrt{p_1 r},\sqrt{p_2})$. From the structure of subgroups of D_8, and due to Galois correspondence, $L(K_1)/T_i$ $(i = 1, 2)$ is an unramified extension of type $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. This implies $\text{rank}_2 A(T_i) \geq 2$. But this is a contradiction to Lemma 6.6.2 due to our initial assumption that $p = a^2 - 2b^2$ with $\left(\frac{a}{p}\right) = -1$.

(2). When $r \equiv 7 \pmod 8$: The group $D_8 \oplus \mathbb{Z}/2\mathbb{Z}$ has four subgroups isomorphic to D_8, two of the form $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ and one subgroup of the type $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. We have already shown that $\text{Gal}(L(K_1)/\mathbb{Q}_1(\sqrt{p})) \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, and from subcase (2) of the case $\mathfrak{G} = D_8 \curlyvee \mathbb{Z}/4\mathbb{Z}$, we note that $\text{Gal}(L(K_1)/\mathbb{Q}_1(\sqrt{p_i})) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Thus, $\text{Gal}(L(K_1)/\mathbb{Q}_1(\sqrt{rp_i})) \cong D_8$ for $i = 1, 2$. From Condition (6.1), the ideal $p_2\mathcal{O}_{\mathbb{Q}_1}$ is inert in $\mathbb{Q}_1(\sqrt{r})/\mathbb{Q}_1$. From the discussion before Lemma 6.6.2, $\left(\frac{a}{p}\right) = -1$ implies that $p_2\mathcal{O}_{\mathbb{Q}_1}$ is inert in $\mathbb{Q}_1(\sqrt{p_1})/\mathbb{Q}_1$ as well. As $\mathbb{Q}_1(\sqrt{r},\sqrt{p_1})/\mathbb{Q}_1$ is a biquadratic extension, $p_2\mathcal{O}_{\mathbb{Q}_1}$ splits as the product $p_{21} \cdot p_{22}$ in $\mathbb{Q}_1(\sqrt{rp_1})/\mathbb{Q}_1$, and the ideals p_{21} and p_{22} remain inert in $\mathbb{Q}_1(\sqrt{r},\sqrt{p_1})/\mathbb{Q}_1(\sqrt{rp_1})$. Let $\overline{p_{21}}$ and $\overline{p_{22}}$ be the prime ideals of $\mathbb{Q}_1(\sqrt{r},\sqrt{p_1})$ above p_{21} and p_{22}, respectively. As $\text{Gal}(L(K_1)/\mathbb{Q}_1(\sqrt{rp_1})) \cong D_8$, the fields H_1 and H_2 defined earlier in this proof must be isomorphic, non-Galois extensions over $\mathbb{Q}_1(\sqrt{rp_1})$. Suppose that H_2 is the inertia field of $\overline{p_{21}}$ in the extension $L(K_1)/\mathbb{Q}_1(\sqrt{r},\sqrt{p_1})$. With reasons similar to those discussed in both the subcases of Case 2, we obtain a contradiction, and that way, $\mathfrak{G} \neq D_8 \oplus \mathbb{Z}/2\mathbb{Z}$.

We find that $\mathfrak{G}$ can be none of $Q_8 \oplus \mathbb{Z}/2\mathbb{Z}$, $D_8 \curlyvee \mathbb{Z}/4\mathbb{Z}$, and $D_8 \oplus \mathbb{Z}/2\mathbb{Z}$. Hence, we conclude

that our assumption was wrong and $\#A(K_1) = 2$ if $p = a^2 - 2b^2$ with $\left(\frac{a}{p}\right) = -1$. □

6.6.2 An alternate condition for $\#A(K_1) = 2$

We have seen numerous instances that depict how the decomposition of certain prime ideals has an effect on the order of the 2-class group. Analogous to Lemma 4.2.2, we prove the following result:

Proposition 6.6.3. *Let ℓ_1 and ℓ_2 be prime ideals in $\mathbb{Q}(\sqrt{p})$ so that $2\mathcal{O}_{\mathbb{Q}(\sqrt{p})} = \ell_1 \cdot \ell_2$. If ℓ_1 and ℓ_2 are principal, then $\#A(K_1) = 2$.*

Proof. Since $r \equiv 3 \pmod 4$ and $p \equiv 1 \pmod 8$, $2\mathbb{Z}$ ramifies in $k/\mathbb{Q}$ and splits in $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$. Let $\mathfrak{l}$ be the prime ideal in k above $2\mathbb{Z}$. Then, $\mathfrak{l}$ splits in K/k, and hence must be principal in k, as K is the 2-Hilbert class field of k. Thus, there exists $\ell \in k$ such that $\mathfrak{l} = \ell\mathcal{O}_k$, and $(\ell\mathcal{O}_k)^2 = 2\mathbb{Z}$. Let ℓ_1 and ℓ_2 be the prime ideals of $\mathbb{Q}(\sqrt{p})$ such that $2\mathcal{O}_{\mathbb{Q}(\sqrt{p})} = \ell_1 \cdot \ell_2$. In this scenario, there exist prime ideals L_1, L_2 in K such that $L_i^2 = \ell_i\mathcal{O}_K$ for $i = 1, 2$, and $L_1 \cdot L_2 = \ell\mathcal{O}_K$. From our assumption, $[L_1]^2 = [L_2]^2 = id$. Therefore, by Lemma 6.4.2, $[L_i] \in A(K) = \{id\}$, which further implies that L_1 and L_2 are principal in K. Since K_1/K is ramified at primes above 2, there exist ideals $\widetilde{L_i}$ such that $(\widetilde{L_i})^2 = L_i\mathcal{O}_{K_1}$ for $i = 1, 2$. Furthermore, the order of $[\widetilde{L_i}]$ is at most 2 as L_i is principal for each i. If $\tilde{\mathfrak{l}}$ is the prime above $\mathfrak{l}$ in k_1/k, then from Proposition 5.3.3, $\tilde{\mathfrak{l}}$ remains inert in $k_1(\sqrt{p_1})/k_1$. Thus, the ideals $\widetilde{L_1}$ and $\widetilde{L_2}$ remain inert in the unramified extension $K_1(\sqrt{p_1})/K_1$, and thus are not principal in K_1. Adapting the arguments based on Nakayama's lemma presented in Lemma 4.2.2 on the extension $K_1(\sqrt{p_1})/K_1$, we conclude $\#A(K_1) = 2$. □

Theorem 6.1.6 and Proposition 6.6.3 highlight the importance of finding and studying solutions to certain diophantine equations. The prime ideal ℓ_1 is principal in $\mathbb{Q}(\sqrt{p})$ if and only if there exists a solution in integers to the equation $x^2 - py^2 = \pm 8$. For primes $p \equiv 9 \pmod{16}$ and $\left(\frac{2}{p}\right)_4 = -1$ such that $p \leq 10,000$, using PariGP, it can be seen that the prime ideals ℓ_i are principal in $\mathbb{Q}(\sqrt{p})$ except for the values $p = 761$, 1129, 2153, 2713, 2777, 4441, 4649, 4729, 4889, 5273, 5417, 7673, 9049, 9833.

It can also be verified that for all $p \leq 10,000$ of the form $p \equiv 9 \pmod{16}$ and $\left(\frac{2}{p}\right)_4 = -1$, if a and b are integers such that $a^2 - 2b^2 = p$, then indeed $\left(\frac{a}{p}\right) = -1$. This observation

leads to the following question:

Question: Let p be a prime such that $p \equiv 9 \pmod{16}$ and $\left(\frac{2}{p}\right)_4 = -1$. If a and b are integers such that $a^2 - 2b^2 = p$, is it always true that $\left(\frac{a}{p}\right) = -1$?

An affirmative answer to this question will facilitate an unconditional proof for $\#A(K_1) = 2$ (from Theorem 6.1.6). Another consequence would be the capitulation of a nontrivial ideal class in the extension $K_1/\mathbb{Q}_1(\sqrt{p})$ (due to Theorem 6.1.4). Although this condition is sufficient to ensure that $\#A(K_1) = \#A(\mathbb{Q}_1(\sqrt{p})) = 2$, there can still be an increase in the order of $A(K_2)$. To illustrate this, we enlist the orders of $A(K_2)$ and $A(\mathbb{Q}_2(\sqrt{p}))$ for small values of r and p satisfying Condition (6.1) in the following tables.

Table 6.1: Orders of $A(\mathbb{Q}_2(\sqrt{p}))$ and $A(K_2)$ for $r = 3$

p	$\#A(\mathbb{Q}_2(\sqrt{p}))$	$\#A(K_2)$
41	4	4
137	4	4
521	2	4
569	2	4
761	4	4
809	2	4
857	2	4
953	2	4

Table 6.2: Orders of $A(\mathbb{Q}_2(\sqrt{p}))$ and $A(K_2)$ for $r = 7$

p	$\#A(\mathbb{Q}_2(\sqrt{p}))$	$\#A(K_2)$
41	4	4
313	4	4
409	2	4
521	2	4
761	4	4
857	2	4

We note that both the possibilities $\#A(K_2) = \#A(\mathbb{Q}_2(\sqrt{p}))$ and $\#A(K_2) = 2 \cdot \#A(\mathbb{Q}_2(\sqrt{p}))$ can occur. Even for $r = 11, 19$, and 23, it can be seen that $\#A(K_2) = 4$ for every $p \leq 1000$ that satisfies Condition (6.1). Therefore, it would also be interesting to see what factors govern the growth of $\#A(K_2)$.

Scope of future work

1. There are several families of real quadratic fields $K = \mathbb{Q}(\sqrt{d})$ where $d \geq 0$ has at most 3 prime factors with different conditions on d for which Greenberg's conjecture has not been verified for $\ell = 2$. We would like to continue investigating those fields with different techniques. In light of Chapter 6, we would like to pursue more bi-quadratic fields to understand how their Iwasawa modules are related with the ones corresponding to their subfields. Also, we would like to work on imaginary quadratic fields and CM fields with the objective of examining the Iwasawa invariants.

2. Mizusawa studied some extensions of $\mathbb{Q}_\infty$ unramified outside certain primes (cf. [61]), where $\mathbb{Q}_\infty$ is the $\mathbb{Z}_2$-extension of $\mathbb{Q}$. One of the consequences of his work is the verification of Greenberg's conjecture for some abelian extensions of $\mathbb{Q}$. Understanding ray class fields and images of units in local fields and finite fields are some of the pre-requisites. A similar problem can be considered for finite extensions of $\mathbb{Q}$. Corollary 6.1.3 and Corollary 6.1.5 are some results aimed in this direction.

3. Let $K = \mathbb{Q}(\sqrt{p^2+2})$ such that p^2+2 is square-free and K is p-rational. Since p is unramified in $K/\mathbb{Q}$, it must be ramified in K_n/K for all $n \geq 1$ where K_n is the n-th layer in the cyclotomic $\mathbb{Z}_p$-extension of K. Since p does not divide the class number of K, by [80, Proposition 13.22], we infer that the Iwasawa λ invariant for the cyclotomic $\mathbb{Z}_p$-extension of K is equal to 0 if $p \equiv 3, 5 \pmod 8$. Similarly, the λ-invariant for the cyclotomic $\mathbb{Z}_p$-extension of $K = \mathbb{Q}(\sqrt{p^2-2})$ is 0 if $p \equiv 5, 7 \pmod 8$. Recently, in [72], Qi and Stokes studied Greenberg's conjecture on Iwasawa invariants for non-p-rational fields. In this spirit, we would like to study possible connections between Iwasawa invariants and p-rationality of various number fields.

Bibliography

[1] Anand, J. Chattopadhyay, and B. Roy. On sums of polynomial-type exceptional units in $\mathbb{Z}/n\mathbb{Z}$. *Arch. Math. (Basel)*, 114(3):271–283, 2020.

[2] J. Assim and Z. Bouazzaoui. Half-integral weight modular forms and real quadratic p-rational fields. *Funct. Approx. Comment. Math.*, 63(2):201–213, 2020.

[3] A. Azizi, M. M. Chems-Eddin, and A. Zekhnini. On the rank of the 2-class group of some imaginary triquadratic number fields. *Rend. Circ. Mat. Palermo (2)*, 70(3):1751–1769, 2021.

[4] A. Azizi and A. 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(7):2741–2752, 2001.

[5] A. Azizi, A. Zekhnini, and M. Taous. On the strongly ambiguous classes of some biquadratic number fields. *Math. Bohem.*, 141(3):363–384, 2016.

[6] R. Barbulescu and J. Ray. Numerical verification of the Cohen-Lenstra-Martinet heuristics and of Greenberg's p-rationality conjecture. *J. Théor. Nombres Bordeaux*, 32(1):159–177, 2020.

[7] E. Benjamin, F. Sanborn, and C. Snyder. Capitulation in unramified quadratic extensions of real quadratic number fields. *Glasgow Math. J.*, 36(3):385–392, 1994.

[8] Y. Benmerieme and A. Movahhedi. Multi-quadratic p-rational number fields. *J. Pure Appl. Algebra*, 225(9):Paper No. 106657, 17, 2021.

[9] W. Bosma and P. Stevenhagen. On the computation of quadratic 2-class groups. *J. Théor. Nombres Bordeaux*, 8(2):283–313, 1996.

[10] K. Boulajhaf and A. Mouhib. Cyclicity of the 2-decomposed unramified Iwasawa module. *J. Number Theory*, 263:234–254, 2024.

[11] E. Brown and C. J. Parry. The 2-class group of certain biquadratic number fields. *J. Reine Angew. Math.*, 295:61–71, 1977.

[12] A. Brumer. On the units of algebraic number fields. *Mathematika*, 14:121–124, 1967.

[13] C. Chevalley. Sur la théorie du corps de classes dans les corps finis et les corps locaux (thése). *J. Faculty of Sciences Tokyo*, 2:365–476, 1933.

[14] N. Childress. *Class field theory*. Springer Science & Business Media, 2008.

[15] D. Clausen. Classifying all groups of order 16. page 15. URL: http://buzzard.ups.edu/courses/2012spring/projects/clausen-groups-16-ups-434-2012.pdf.

[16] K. Conrad. Groups of order 16. page 4. URL: https://kconrad.math.uconn.edu/blurbs/grouptheory/group16.pdf.

[17] G. Cornell. Relative genus theory and the class group of l-extensions. *Trans. Amer. Math. Soc.*, 277(1):421–429, 1983.

[18] D. S. Dummit and R. M. Foote. *Abstract algebra*. John Wiley & Sons, Inc., Hoboken, NJ, third edition, 2004.

[19] P. D. T. A. Elliott. *Probabilistic number theory I: Mean-value theorems*, volume 239. Springer Science & Business Media, 2012.

[20] S. Essahel and A. Mouhib. Fields $\mathbb{Q}(i, \sqrt{2}, \sqrt{p_1}, \ldots, \sqrt{p_n})$ with cyclic 2-class group. *Acta Math. Hungar.*, 170(2):499–509, 2023.

[21] B. Ferrero and L. C. Washington. The Iwasawa invariant μ_p vanishes for abelian number fields. *Ann. of Math. (2)*, 109(2):377–395, 1979.

[22] T. Fukuda. Remarks on $\mathbb{Z}_p$-extensions of number fields. *Proc. Japan Acad. Ser. A Math. Sci.*, 70(8):264–266, 1994.

[23] T. Fukuda and K. Komatsu. On the Iwasawa λ-invariant of the cyclotomic $\mathbb{Z}_2$-extension of a real quadratic field. *Tokyo J. Math.*, 28(1):259–264, 2005.

[24] R. Fuller. *Roy Fuller's notes from Langlands' course on class field theory, Spring 1964*. URL: https://personal.math.ubc.ca/~cass/fuller/fuller.html.

[25] P. Furtwängler. Über das verhalten der ideale des grundkörpers im klassenkörper. *Monatshefte für Mathematik und Physik*, 27:1–15, 1916.

[26] D. Gorenstein. *Finite groups*. Harper & Row, Publishers, New York-London, 1968.

[27] G. Gras. Sur les l-classes d'idéaux dans les extensions cycliques relatives de degré premier l. I, II. *Ann. Inst. Fourier (Grenoble)*, 23(3):1–48; ibid. 23 (1973), no. 4, 1–44, 1973.

[28] G. Gras. Remarks on K_2 of number fields. *J. Number Theory*, 23(3):322–335, 1986.

[29] G. Gras. *Class field theory, from theory to practice*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2003. From theory to practice, Translated from the French manuscript by Henri Cohen.

[30] G. Gras. Les θ-régulateurs locaux d'un nombre algébrique: conjectures p-adiques. *Canad. J. Math.*, 68(3):571–624, 2016.

[31] G. Gras. Invariant generalized ideal classes—structure theorems for p-class groups in p-extensions. *Proc. Indian Acad. Sci. Math. Sci.*, 127(1):1–34, 2017.

[32] G. Gras. On p-rationality of number fields. Applications—PARI/GP programs. In *Publications mathématiques de Besançon. Algèbre et théorie des nombres. 2019/2*, volume 2019/2 of *Publ. Math. Besançon Algèbre Théorie Nr.*, pages 29–51. Presses Univ. Franche-Comté, Besançon, 2019.

[33] G. Gras. Algebraic norm and capitulation of p-class groups in ramified cyclic p-extensions. *arXiv preprint arXiv:2211.12279*, 2022.

[34] G. Gras. On the λ-stability of p-class groups along cyclic p-towers of a number field. *Int. J. Number Theory*, 18(10):2241–2263, 2022.

[35] R. Greenberg. On the Iwasawa invariants of totally real number fields. *Amer. J. Math.*, 98(1):263–284, 1976.

[36] R. Greenberg. Galois representations with open image. *Ann. Math. Qué.*, 40(1):83–119, 2016.

[37] D. R. Heath-Brown. Power-free values of polynomials. *Q. J. Math.*, 64(1):177–188, 2013.

[38] H. Ichimura and H. Sumida. On the Iwasawa invariants of certain real abelian fields. *Tohoku Math. J. (2)*, 49(2):203–215, 1997.

[39] Y. Iizuka. On the class number divisibility of pairs of imaginary quadratic fields. *J. Number Theory*, 184:122–127, 2018.

[40] K. Iwasawa. On Γ-extensions of algebraic number fields. *Bull. Amer. Math. Soc.*, 65:183–226, 1959.

[41] K. Iwasawa. On $\mathbf{Z}_l$-extensions of algebraic number fields. *Ann. of Math. (2)*, 98:246–326, 1973.

[42] G. J. Janusz. *Algebraic Number Fields*. Academic Press New York and London, 1973.

[43] J.-F. Jaulent and T. Nguyen Quang Do. Corps p-rationnels, corps p-réguliers, et ramification restreinte. *J. Théor. Nombres Bordeaux*, 5(2):343–363, 1993.

[44] H. Kisilevsky. Some results related to Hilbert's Theorem 94. *J. Number Theory*, 2:199–206, 1970.

[45] H. Kisilevsky. Number fields with class number congruent to 4 mod 8 and Hilbert's theorem 94. *J. Number Theory*, 8(3):271–279, 1976.

[46] J. Koperecz. Triquadratic p-rational fields. *J. Number Theory*, 242:402–408, 2023.

[47] J. S. Kraft and R. Schoof. Computing Iwasawa modules of real quadratic number fields. volume 97, pages 135–155. 1995. Special issue in honour of Frans Oort.

[48] S. Krishnamoorthy and S. K. Pasupulati. Note on the p-divisibility of class numbers of an infinite family of imaginary quadratic fields. *Glasg. Math. J.*, 64(2):352–357, 2022.

[49] T. Kubota. über den bizyklischen biquadratischen Zahlkörper. *Nagoya Math. J.*, 10:65–85, 1956.

[50] N. 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(4):931–958, 2021.

[51] S. Kuroda. Über den dirichletschen körper. *J. Fac. Sci. Imp. Univ. Tokyo Sec. I.*, 4:383–406, 1943.

[52] M. H. Le. Upper bounds for class numbers of real quadratic fields. *Acta Arith.*, 68(2):141–144, 1994.

[53] F. Lemmermeyer. Class field towers. *Preprint*, 111, 2010.

[54] H-W. Leopoldt. Zur Arithmetik in abelschen Zahlkörpern. *J. Reine Angew. Math.*, 209:54–71, 1962.

[55] S. Louboutin. Explicit upper bounds for values at $s = 1$ of Dirichlet L-series associated with primitive even characters. *J. Number Theory*, 104(1):118–131, 2004.

[56] S. Louboutin. The Brauer-Siegel theorem. *J. London Math. Soc. (2)*, 72(1):40–52, 2005.

[57] Y. Mizusawa. On the Iwasawa invariants of $\mathbb{Z}_2$-extensions of certain real quadratic fields. *Tokyo J. Math.*, 27(1):255–261, 2004.

[58] Y. Mizusawa. *A Study of Iwasawa Theory on Class Field Towers.* PhD thesis, Waseda University, 2004.

[59] Y. Mizusawa. On unramified Galois 2-groups over $\mathbb{Z}_2$-extensions of real quadratic fields. *Proc. Amer. Math. Soc.*, 138(9):3095–3103, 2010.

[60] Y. Mizusawa. A note on semidihedral 2-class field towers and $\mathbb{Z}_2$-extensions. *Ann. Math. Qué.*, 38(1):73–79, 2014.

[61] Y. Mizusawa. Tame pro-2 Galois groups and the basic $\mathbb{Z}_2$-extension. *Trans. Amer. Math. Soc.*, 370(4):2423–2461, 2018.

[62] Y. Mizusawa. On metabelian 2-class field towers over $\mathbb{Z}_2$-extensions of real quadratic fields. *Canad. Math. Bull.*, 65(3):795–805, 2022.

[63] A. Mouhib. The structure of the unramified abelian Iwasawa module of some number fields. *Pacific J. Math.*, 323(1):173–184, 2023.

[64] A. Mouhib and A. Movahhedi. Sur le 2-groupe de classes des corps multiquadratiques réels. *J. Théor. Nombres Bordeaux*, 17(2):619–641, 2005.

[65] A. Mouhib and A. Movahhedi. On the p-class tower of a $\mathbf{Z}_p$-extension. *Tokyo J. Math.*, 31(2):321–332, 2008.

[66] A. Mouhib and A. Movahhedi. Cyclicity of the unramified Iwasawa module. *Manuscripta Math.*, 135(1-2):91–106, 2011.

[67] A. Movahhedi. *Sur les p-extensions des corps p-rationnels*. PhD thesis, Universit Paris Diderot, 1988.

[68] A. Movahhedi. Sur les p-extensions des corps p-rationnels. *Math. Nachr.*, 149:163–176, 1990.

[69] A. Movahhedi and T. Nguyen Quang Do. Sur l'arithmétique des corps de nombres p-rationnels. In *Séminaire de Théorie des Nombres, Paris 1987–88*, volume 81 of *Progr. Math.*, pages 155–200. Birkhäuser Boston, Boston, MA, 1990.

[70] Y. Nishino. On the Iwasawa invariants of the cyclotomic $\mathbb{Z}_2$-extensions of certain real quadratic fields. *Tokyo J. Math.*, 29(1):239–245, 2006.

[71] M. Ozaki and H. Taya. On the Iwasawa λ_2-invariants of certain families of real quadratic fields. *Manuscripta Math.*, 94(4):437–444, 1997.

[72] P. Qi and M. Stokes. On the non p-rationality invariants of certain real quadratic fields. *arXiv preprint arXiv:2408.03836*, 2024.

[73] L. Rédei and H. Reichardt. Die durch vier teilbaren invarianten der klassengruppe der quadratischen zahlkörper. *J. reine angew. Math.*, 170:59–74, 1933.

[74] M. Rosen. Two theorems on Galois cohomology. *Proc. Amer. Math. Soc.*, 17:1183–1185, 1966.

[75] J.-P. Serre. *Corps locaux*, volume No. VIII of *Publications de l'Université de Nancago*. Hermann, Paris, 1968. Deuxième édition.

[76] R. Sharifi. *Iwasawa Theory.* URL: https://www.math.ucla.edu/~sharifi/iwasawa.pdf.

[77] O. Taussky. A remark on the class field tower. *Journal of the London Mathematical Society*, 1(2):82–85, 1937.

[78] O. Taussky. A remark concerning Hilbert's theorem 94. *J. Reine Angew. Math.*, 239/240:435–438, 1970.

[79] F. Terada. On a generalization of the principal ideal theorem. *Tohoku Mathematical Journal, Second Series*, 1(3):229–269, 1949.

[80] L. C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.

[81] G. Yamamoto. On the vanishing of Iwasawa invariants of absolutely abelian p-extensions. *Acta Arith.*, 94(4):365–371, 2000.

[82] X. Zhang. A simple construction of genus fields of abelian number fields. *Proc. Amer. Math. Soc.*, 94(3):393–395, 1985.

Publications

Publications from Thesis work

1. J. Chattopadhyay, H. Laxmi, and A. Saikia, *On the p-rationality of consecutive quadratic fields*, J. Number Theory, **248** (2023), 14–26.

2. J. Chattopadhyay, H. Laxmi, and A. Saikia, *Structure of 2-class groups in the $\mathbb{Z}_2$-extensions of certain real quadratic fields*, Res. Number Theory, **9** (2023), 14 pages.

3. H. Laxmi and A. Saikia, *$\mathbb{Z}_2$-extension of real quadratic fields with $\mathbb{Z}/2\mathbb{Z}$ as 2-class group at each layer*, Ramanujan J., **64** (2024), 1285–1301.

4. H. Laxmi and A. Saikia, *Unramified Iwasawa module of $\mathbb{Z}_2$-extension of certain quadratic fields with a bounded quotient*, arXiv:2404.05190, (2024), 10 pages, Communicated.

5. H. Laxmi and A. Saikia, *Stability of 2-class groups in $\mathbb{Z}_2$-extension of certain real biquadratic fields*, arXiv:2501.12782, (2025), 19 pages, Communicated.