# On Euclidean ideal classes in abelian extensions

*By*

**Jyothsnaa S.**

**MATH10201405001**

**The Institute of Mathematical Sciences, Chennai**

***A thesis submitted to the***

***Board of Studies in Mathematical Sciences***

***In partial fulfillment of requirements***

***for the Degree of***

**DOCTOR OF PHILOSOPHY**

***of***

**HOMI BHABHA NATIONAL INSTITUTE**

**May, 2019**

# Homi Bhabha National Institute

## Recommendations of the Viva Voce Committee

As members of the Viva Voce Committee, we certify that we have read the dissertation prepared by Jyothsnaa S. entitled "On Euclidean ideal classes in abelian extensions" and recommend that it may be accepted as fulfilling the thesis requirement for the award of Degree of Doctor of Philosophy.

________________________________________ Date: May 27, 2019
Chairman - P. Sankaran

________________________________________ Date: May 27, 2019
Guide/Convenor - S. Gun

________________________________________ Date: May 27, 2019
Examiner - B. Sury

________________________________________ Date: May 27, 2019
Member 1 - V. Kodiyalam

________________________________________ Date: May 27, 2019
Member 2 - A. Mukhopadhyay

________________________________________ Date: May 27, 2019
Member 3 - P. Rath

Final approval and acceptance of this thesis is contingent upon the candidate's submission of the final copies of the thesis to HBNI.

I hereby certify that I have read this thesis prepared under my direction and recommend that it may be accepted as fulfilling the thesis requirement.

**Date: May 27, 2019**

**Place: Chennai** Guide

# STATEMENT BY AUTHOR

This dissertation has been submitted in partial fulfillment of requirements for an advanced degree at Homi Bhabha National Institute (HBNI) and is deposited in the Library to be made available to borrowers under rules of the HBNI.

Brief quotations from this dissertation are allowable without special permission, provided that accurate acknowledgement of source is made. Requests for permission for extended quotation from or reproduction of this manuscript in whole or in part may be granted by the Competent Authority of HBNI when in his or her judgement the proposed use of the material is in the interests of scholarship. In all other instances, however, permission must be obtained from the author.

Jyothsnaa S.

# DECLARATION

I hereby declare that the investigation presented in the thesis has been carried out by me. The work is original and has not been submitted earlier as a whole or in part for a degree / diploma at this or any other Institution / University.

Jyothsnaa S.

# LIST OF PUBLICATIONS ARISING FROM THE THESIS

## Journal

1. On existence of Euclidean ideal classes in real cubic and quadratic fields with cyclic class groups, Sanoli Gun and Jyothsnaa Sivaraman, *to appear in Michigan Math. J.*

2. Existence of Euclidean ideal classes beyond certain rank, Jyothsnaa Sivaraman, *to appear in J. Ramanujan Math. Soc.*

3. On Euclidean ideal classes in certain abelian extensions, Jean-Marc Deshouillers, Sanoli Gun and Jyothsnaa Sivaraman, *to appear in Math. Z.*

Jyothsnaa S.

*To my Teachers.*

# ACKNOWLEDGEMENTS

I would like to begin by thanking my advisor, Prof. Sanoli Gun, wholeheartedly. Without her unfailing support, both emotional and academic, I cannot imagine this thesis coming to fruition. She has played a major role in not just my Ph.D. but also my induction into research. For this, I am infinitely grateful.

I would also like to thank Prof. Purusottam Rath for all his guidance. I have known Prof. Rath since my undergraduate days, and without his support I would never have been able to enter and hold my ground in research. For his time and patience, I will always remain indebted.

Next, I must thank Prof. Jean-Marc Deshouillers who taught me that mathematics is all about arguments and counters. He truly taught me what it means to enjoy mathematics.

I further take this opportunity to thank Prof. Joseph Oesterlé. I am especially thankful for the fact that he kindly indulged all my mathematical queries, however basic they might be. Without his help, I am sure I would have been lost.

I would also like to thank Prof. M. Ram Murty. His work has served as the starting point for all the ideas that appear in this thesis. Further, without his encouraging words I would not have had the courage to move forward and take the next step towards completing my Ph.D.

I also wish to thank Prof. V. Kumar Murty for all the discussions and interesting lectures on algebraic number theory. Through the years these discussions have streamlined my thoughts about this problem on Euclidean ideal classes.

I wish to thank all the faculty members of IMSc who taught me during my coursework: Prof. V. S. Sunder, Prof. Jaya Iyer, Prof. K. Srinivas, Prof. Vijay Kodiyalam and Prof. D. S. Nagaraj. Their courses, discussions and questions have played a major role in shaping my mathematical ideas.

I am immensely glad that I had the opportunity to interact and learn from such distinguished mathematicians and for that I have to thank IMSc : the institution, the faculty and its administration.

I believe that I also owe a lot to the Chennai Mathematical Institute, where I had the chance to interact with a few faculty members over the course of the last few years. In particular, I would like to thank Prof. Sunder Sobers (who is now at IMSc) and Prof. Shiva Shankar for their courses which laid the foundation to my mathematical career.

I would also like to thank Abhishek T. Bharadwaj and Biplab Paul for taking time out to discuss with me. I would like to thank all my batchmates, friends and colleagues who have made my time here both stimulating and memorable.

Finally I would like to thank my parents for facilitating my education and supporting me in all my endeavours.

# Contents

# Synopsis

## Introduction

The study of growth and distribution of class numbers of number fields constitutes a venerable theme in number theory. The origin of this theory can be traced to Gauss's Disquisitiones Arithmeticae [11].

One is immediately led to the following questions (and meta questions) listed presumably in decreasing order of difficulty:

- Are there infinitely many real quadratic number fields with class number 1?
- Whether the distribution of class numbers/$p$-torsion elements in class groups is more uniform among the lower degree number fields, say among quadratic and cubic fields?
- Whether the ring of integers of number fields with class number 1 are "generic" or "special"?

In this thesis we will introduce an open problem pertaining to the last question, witness its extension to the second question and finally state our results in this context. The first question of course still remains far from our reach. As we shall see, these seemingly algebraic questions force or lead us to deep arithmetic and analytic issues which are intricately linked to the distribution of prime ideals in number fields. Hence, they naturally lead us to the Holy Grail: the Riemann hypothesis, not just over rationals, but over number fields.

We begin by addressing the last question: Is the ring of integers of a number field of class number one "generic" or "special"? By "special" we refer to the property of being a Euclidean domain. It is known that any Euclidean domain is a principal ideal domain. *But does the converse hold?* As it turns out, this question needs to be addressed in a case wise fashion. It follows from the work of Motzkin [28] that in the case of imaginary quadratic fields there exist fields whose rings of integers are principal ideal domains but not Euclidean domains. But for fields where the ring of integers has infinitely many units this appears not to be the case. In fact Weinberger in 1972 [36] proved, under the extended Riemann hypothesis, that if the ring of integers has infinitely many units, it is a principal ideal domain if and only if it is a Euclidean domain. A lot of work has gone into trying to make this result unconditional, for instance [4], [18], [19] and [31], to cite a few. However we are more interested in non trivial class groups which brings us to question two.

In order to address the second question, we observe that working with Euclidean domains is no longer enough. If our principal motivation is to study class groups, then we need to generalise the idea of Euclidean domains. In his seminal paper of 1979, Lenstra did exactly this. He introduced the notion of Euclidean ideal classes (see [26]) in order to study cyclic class groups.

In this paper, Lenstra proves, under the extended Riemann hypothesis, that if the ring of integers of a number field has infinitely many units, then it has a Euclidean ideal class if and only if the class group is cyclic. There are some partial unconditional results towards this question by Graves and Murty [14] when the unit rank (rank of the free part of $\mathcal{O}_{\mathbf{K}}^{\times}$) of a number field is at least 4. This thesis centers around improvements that can be made on these results. In the next section we will look at the preliminaries required to expand on our results in the above context.

# Preliminaries

A field extension $\mathbf{K}$ of $\mathbb{Q}$ of finite degree inside $\mathbb{C}$ is called a number field. If this extension is Galois over $\mathbb{Q}$ and the Galois group of $\mathbf{K}$ over $\mathbb{Q}$ is abelian, we say that the field $\mathbf{K}$ is an abelian number field. The set of all elements of $\mathbf{K}$ which are solutions of monic polynomials over $\mathbb{Z}$ form a ring and this ring is called the ring of integers of $\mathbf{K}$, denoted by $\mathcal{O}_{\mathbf{K}}$. Any finitely generated $\mathcal{O}_{\mathbf{K}}$ submodule of $\mathbf{K}$ is called a fractional ideal. One can define the notion of product of two fractional ideals. Under this operation, it is well known that every non-zero fractional ideal of $\mathcal{O}_{\mathbf{K}}$ is invertible. Therefore the set of all non-zero fractional ideals of $\mathcal{O}_{\mathbf{K}}$ forms a group under multiplication with $\mathcal{O}_{\mathbf{K}}$ acting as unity. This brings us to the notion of class groups. Consider the quotient group of non-zero fractional ideals modulo the subgroup of non-zero principal fractional ideals. This is known as the class group of $\mathcal{O}_{\mathbf{K}}$ (note that this notion can be defined more generally for Dedekind domains). In case of $\mathcal{O}_{\mathbf{K}}$ the cardinality of this group is known to be finite and it is called the class number of $\mathcal{O}_{\mathbf{K}}$. The class number can be considered as a measure for the deviation of $\mathcal{O}_{\mathbf{K}}$ from being a principal ideal domain. The ring $\mathcal{O}_{\mathbf{K}}$ is a principal ideal domain if and only if it has class number 1.

We are interested in studying these class groups. We will do so by studying what are known as "Euclidean ideal classes". In order to describe Euclidean ideal classes, we begin with the notion of Euclidean domains.

**Definition 0.0.1.** *An integral domain $R$ is said to be Euclidean if there exists a function*

$$\phi : R \setminus \{0\} \to \mathbb{N} \cup \{0\}$$

*such that given any $b \neq 0$ and $a$ in $R$, there exist $q$ and $r$ in $R$ such that $a = bq + r$,* *where either $r = 0$ or $\phi(r) < \phi(b)$. Here $\mathbb{N}$ is used to denote the set of all positive integers. We will refer to such functions as Euclidean functions.*

We comment here that if $\phi$ is a Euclidean function on $R$, then there exists a Euclidean function $\tilde{\phi}$ on $R$ such that for any $a \in R \setminus \{0\}$,

$$\tilde{\phi}(a) = \tilde{\phi}(au) \text{ for all units } u \text{ of } R.$$

Further it is well known that if a ring is a Euclidean domain then it is a principal ideal domain. Using these facts we can redefine Euclidean domains in the following way.

**Definition 0.0.2.** *Let $R$ be an integral domain, $E$ be the monoid of all non-zero integral ideals of $R$ and $\mathbb{N}$ the set of all positive integers. Suppose that $\psi$ is a map from $E$ to $\mathbb{N}$. We say that $R$ is Euclidean for $\psi$ if $R$ is a principal ideal domain and for each non-zero ideal $\mathfrak{b}$ of $E$ and any $x \in R\mathfrak{b}^{-1} \setminus R$, there exists $y \in R$ such that*

$$\psi(\mathfrak{b}(x - y)) < \psi(\mathfrak{b}).$$

However, in 1979, Lenstra generalised this notion of Euclidean domains. In this thesis, we will only consider the definition in the case of Dedekind domains for ease of exposition.

**Definition 0.0.3.** *Let $R$ be a Dedekind domain, $E$ be the set of all non-zero integral ideals of $R$ and $\mathbb{N}$, the set of all positive integers. Suppose that $\psi$ is a map from $E$ to $\mathbb{N}$. We say that a non-zero fractional ideal $\mathfrak{a}$ of $R$ is Euclidean for $\psi$ if for each non- zero ideal $\mathfrak{b}$ of $E$ and any $x \in \mathfrak{a}\mathfrak{b}^{-1} \setminus \mathfrak{a}$, there exists $y \in \mathfrak{a}$ such that*

$$\psi\left(\mathfrak{a}^{-1}\mathfrak{b}(x - y)\right) < \psi(\mathfrak{b}).$$

*Further we say that the class of $\mathfrak{a}$ in the class group of $R$ is a Euclidean ideal class.*

Lenstra was also able to prove that if a Euclidean ideal class exists then the class group is always cyclic. This gives us a generalisation of Euclidean domains which correspond to non trivial class groups. In fact Lenstra defined the idea of Euclidean ideal classes for integral domains and showed that if an integral domain has a Euclidean ideal class, it is automatically a Dedekind domain with cyclic class group. However we will restrict ourselves to the rings of integers of number fields.

So the existence of a Euclidean ideal class is a sufficient condition for the class group to be cyclic. *We would like to know if this is also necessary.* This question was also addressed by Lenstra in the same paper, albeit conditionally, as mentioned earlier in the introduction.

Lenstra proved, under the extended Riemann hypothesis, that if the unit rank of $\mathcal{O}_{\mathbf{K}}$ is at least 1 then $\mathcal{O}_{\mathbf{K}}$ has a Euclidean ideal class if and only if it has cyclic class group. The main subject of this thesis is to explore the possibilities of making this statement unconditional.

# Our results

## Large unit rank

In 2013, Graves and Murty, in [14], proved the following.

**Theorem 0.0.4** ([14])**.** *Suppose that $\mathbf{K}$ is a number field with unit rank at least 4 and the Hilbert class field $H(\mathbf{K})$ is abelian over $\mathbb{Q}$. Also suppose that the conductor of $H(\mathbf{K})$ is $f$ and $\mathbb{Q}(\zeta_f)$ over $\mathbf{K}$ is cyclic. Then $\mathbf{K}$ has a Euclidean ideal class.*

This was done using techniques developed in [13] and [19]. In a joint work with Deshouillers and Gun [6], we were able to extend this to number fields whose unit rank is 3. We prove the following.

**Theorem 0.0.5** ([6])**.** *Suppose that* $\mathbf{K}$ *is a number field with unit rank at least* 3 *and the Hilbert class field* $H(\mathbf{K})$ *is abelian over* $\mathbb{Q}$*. Also suppose that the conductor of* $H(\mathbf{K})$ *is* $f$ *and* $\mathbb{Q}(\zeta_f)$ *over* $\mathbf{K}$ *is cyclic. Then* $\mathbf{K}$ *has a Euclidean ideal class.*

Under the conjecture of Elliott and Halberstam, we can derive the following.

**Theorem 0.0.6** ([6])**.** *Let* $\mathbf{K}$ *be a number field such that the Hilbert class field* $H(\mathbf{K})$ *is abelian over* $\mathbb{Q}$ *and the Galois group* $Gal(\mathbb{Q}(\zeta_f)/\mathbf{K})$ *is cyclic where* $f$ *is the conductor of* $H(\mathbf{K})$*. Now if the Elliott and Halberstam conjecture is true and the unit rank of* $\mathbf{K}$ *is at least* 2*, then* $\mathbf{K}$ *has a Euclidean ideal class.*

The main idea in proving Theorem 0.0.5 was to strengthen the sieve lemma in [14] by interjecting the use of "well factorable" weights as introduced by Iwaniec [24] and the use of a theorem of Bombieri, Friedlander and Iwaniec [2] to estimate the error term in the sieve. This helps us decrease the bound on the rank from 4 to 3 by improving the "Level of distribution." Note however that even the Elliott-Halberstam conjecture does not give us the result for the case of rank 1 whilst the result for unit rank one is known under the extended Riemann hypothesis. We observe here that our result is actually stronger than Theorem 0.0.5, as seen below.

**Theorem 0.0.7** ([6])**.** *Let* $\mathbf{K}$ *be a number field with unit rank at least* 3 *and suppose that its Hilbert class field* $H(\mathbf{K})$ *is abelian over* $\mathbb{Q}$*. Further let* $\mathbb{Q}(\zeta_d)$ *be the maximal cyclotomic subextension inside* $\mathbf{K}$*. Consider the diagram*

$$\begin{tikzcd}
\mathbb{Q}(\zeta_f) \arrow[d, dash] \arrow[dd, dash, bend left=50, "G_1"] \arrow[dddd, dash, bend right=60, "G_3"'] \\
H(\mathbf{K}) \arrow[d, dash] \arrow[d, dash, bend right=60, "G_2"'] \\
\mathbf{K} \arrow[d, dash] \\
\mathbb{Q}(\zeta_d) \arrow[d, dash] \\
\mathbb{Q}
\end{tikzcd}$$

*Let $G_3$ be the Galois group of $\mathbb{Q}(\zeta_f)$ over $\mathbb{Q}$. Then*

$$G_3 = \{\sigma_a \ : \ 1 \leq a \leq n, \quad (a, f) = 1\},$$

*where $\sigma_a : \mathbb{Q}(\zeta_f) \to \mathbb{Q}(\zeta_f)$ is such that $\sigma_a(\zeta_f) = \zeta_f^a$. If $G_1$ is the Galois group of $\mathbb{Q}(\zeta_f)$ over $\mathbf{K}$, $G_2$ the Galois group of $H(\mathbf{K})$ over $\mathbf{K}$, the class group of $\mathcal{O}_\mathbf{K}$ is cyclic and*

$$\big\{\sigma_a \in G_1 \ : \ G_2 = \langle \sigma_a|_{H(\mathbf{K})} \rangle\big\} \bigcap \left\{\sigma_a \in G_3 \ : \ a \equiv 1 \bmod d, \ \ \left(\frac{a-1}{d}, \ \frac{f}{d}\right) = 1\right\} \neq \emptyset,$$

*then it has a Euclidean ideal class. Here the notation $G_2 = \langle \sigma_a|_{H(\mathbf{K})} \rangle$ means that $\sigma_a|_{H(\mathbf{K})}$ generates $G_2$.*

Note that our theorem will provide alternate proofs for statements such as the following result of Hsu.

**Theorem 0.0.8** ([23]). *Let $q, k, r \equiv 1 \bmod 4$, $q, k, r \geq 29$ be distinct rational primes. If $\mathbf{K}$ is of the form $\mathbb{Q}(\sqrt{q}, \sqrt{kr})$ and if the class number of $\mathcal{O}_\mathbf{K}$ is $2$, then $\mathbf{K}$ has a non-principal Euclidean ideal.*

This concludes our section on number fields with large unit rank.

## Small unit rank

We also made some progress on the subject of number fields with lower unit rank. Before we state our results, we introduce a few notations. Let $\mathbf{K}_1, \mathbf{K}_2$ and $\mathbf{K}_3$ be number fields with Hilbert class fields $\mathbf{H}(\mathbf{K}_1), \mathbf{H}(\mathbf{K}_2)$ and $\mathbf{H}(\mathbf{K}_3)$ respectively, all abelian over $\mathbb{Q}$. Also let $f_1, f_2$ and $f_3$ be their conductors, i.e. $\mathbb{Q}(\zeta_{f_1}), \mathbb{Q}(\zeta_{f_2})$ and $\mathbb{Q}(\zeta_{f_3})$ be the smallest cyclotomic fields containing $\mathbf{H}(\mathbf{K}_1), \mathbf{H}(\mathbf{K}_2)$ and $\mathbf{H}(\mathbf{K}_3)$ respectively. Set $f$ to be the least common multiple of $16, f_1, f_2, f_3$ if $\mathbf{K}_1, \mathbf{K}_2, \mathbf{K}_3$ are real quadratic and the least common multiple of $16, f_1, f_2$ if $\mathbf{K}_1, \mathbf{K}_2$ are real cubic. However, in case of Theorem 0.0.11, we set $f$ to be the least common multiple of $16, f_1$ and $f_2$. Further, $\mathbf{F} := \mathbb{Q}(\zeta_f)$. In this set up, we have the following theorems.

**Theorem 0.0.9** ([15])**.** *Let $\mathbf{K}_1, \mathbf{K}_2$ be distinct real cubic fields with prime class numbers and $\mathbf{H}(\mathbf{K}_1), \mathbf{H}(\mathbf{K}_2), \mathbf{F}, f$ be as above. Also let $G$ be the Galois group of $\mathbf{F}$ over $\mathbf{K}_1\mathbf{K}_2$, $G_\ell$ be the Galois group of $\mathbf{F}$ over $\mathbb{Q}(\zeta_\ell)$, where either $\ell$ is an odd prime dividing $f$ or $\ell = 4$ and Gal$(\mathbf{F}/\mathbf{H}(\mathbf{K}_i))$ be the Galois group of $\mathbf{F}/\mathbf{H}(\mathbf{K}_i)$ for $i = 1, 2$. If*

$$G \not\subset \bigcup_\ell G_\ell \bigcup \ \mathit{Gal}(\mathbf{F}/\mathbf{H}(\mathbf{K}_1)) \bigcup \ \mathit{Gal}(\mathbf{F}/\mathbf{H}(\mathbf{K}_2)),$$

*then at least one of $\mathbf{K}_1, \mathbf{K}_2$ has a Euclidean ideal class.*

We also have an analogous result in the quadratic case.

**Theorem 0.0.10** ([15])**.** *Let $\mathbf{K}_1, \mathbf{K}_2$ and $\mathbf{K}_3$ be distinct real quadratic fields with prime class numbers and $\mathbf{H}(\mathbf{K}_1)$, $\mathbf{H}(\mathbf{K}_2)$, $\mathbf{H}(\mathbf{K}_3), \mathbf{F}$, $f$ be as above. Also let $G$ be the Galois group of $\mathbf{F}$ over $\mathbf{K}_1\mathbf{K}_2\mathbf{K}_3$, $G_\ell$ be the Galois group of $\mathbf{F}$ over $\mathbb{Q}(\zeta_\ell)$, where either $\ell$ is an odd prime dividing $f$ or $\ell = 4$ and Gal$(\mathbf{F}/\mathbf{H}(\mathbf{K}_i))$ be the Galois group of $\mathbf{F}/\mathbf{H}(\mathbf{K}_i)$ for $i = 1, 2, 3$. If*

$$G \not\subset \bigcup_\ell G_\ell \bigcup \ \mathit{Gal}(\mathbf{F}/\mathbf{H}(\mathbf{K}_1)) \bigcup \ \mathit{Gal}(\mathbf{F}/\mathbf{H}(\mathbf{K}_2)) \bigcup \ \mathit{Gal}(\mathbf{F}/\mathbf{H}(\mathbf{K}_3)),$$

*then at least one of $\mathbf{K}_1, \mathbf{K}_2, \mathbf{K}_3$ has a Euclidean ideal class.*

Now if we assume the Elliott and Halberstam conjecture, we can strengthen Theorem 0.0.10 in the following manner.

**Theorem 0.0.11** ([15])**.** *Let $\mathbf{K}_1$ and $\mathbf{K}_2$ be distinct real quadratic fields with prime class numbers and $\mathbf{H}(\mathbf{K}_1)$, $\mathbf{H}(\mathbf{K}_2), \mathbf{F}$ and $f$ be as above. Also let $G$ be the Galois group of $\mathbf{F}$ over $\mathbf{K}_1\mathbf{K}_2$, $G_\ell$ be the Galois group of $\mathbf{F}$ over $\mathbb{Q}(\zeta_\ell)$, where either $\ell$ is an odd prime dividing $f$ or $\ell = 4$ and Gal$(\mathbf{F}/\mathbf{H}(\mathbf{K}_i))$ be the Galois group of $\mathbf{F}/\mathbf{H}(\mathbf{K}_i)$*

*for $i = 1, 2$. If*

$$G \not\subset \bigcup_{\ell} G_\ell \bigcup \ Gal(\mathbf{F}/\mathbf{H}(\mathbf{K}_1)) \bigcup \ Gal(\mathbf{F}/\mathbf{H}(\mathbf{K}_2)),$$

*then at least one of $\mathbf{K}_1, \mathbf{K}_2$ has a Euclidean ideal class provided the Elliott and Halberstam conjecture holds.*

Further using Theorem 0.0.10 we obtain the following corollary.

**Corollary 0.0.12** ([15])**.** *Let $p_1, q_1, p_2, q_2, p_3, q_3$ be six distinct primes which are congruent to $1 \bmod 4$. For $j \in \{1, 2, 3\}$, if each $\mathbf{K}_j := \mathbb{Q}(\sqrt{p_j q_j})$ has class number $2$, then at least one of them has a Euclidean ideal class.*

An analogous corollary holds for the cubic case. In this work, we use the techniques of Narkiewicz [31] and the sieve of Heath-Brown [20] as seen in his work on Artin's primitive root conjecture. Even though Narkiewicz's work was with respect to Euclidean domains we were able to generalise the same and apply it to the case of Euclidean ideal classes.

## Bound on unit rank

During our study of these results, we realised that the linear sieve which is used repeatedly to prove the above theorems can be replaced by a modified version of Brun's sieve [1], provided we compromise on the effectiveness of the bound on the unit rank. Using this new idea, we provide a short proof of the following fact.

Given a number field $\mathbf{K}$ with unit rank at least $r$, under certain conditions, $\mathbf{K}$ will have a Euclidean ideal class if its class group is cyclic. More precisely, our theorem is the following.

**Theorem 0.0.13** ([34])**.** *Let $\mathbf{K}$ be a number field and $H(\mathbf{K})$ its Hilbert class field. Suppose that the Hilbert class field is abelian over $\mathbb{Q}$. Let $f$ be the smallest even* *positive integer such that* $\mathbb{Q}(\zeta_f)$ *contains* $H(\mathbf{K})$*. Further, suppose that the Galois group of* $\mathbb{Q}(\zeta_f)$ *over* $\mathbf{K}$ *is cyclic. Then there exists a natural number* $r$ *such that if* $\mathbf{K}$ *has unit rank at least* $r$*, it has a Euclidean ideal class.*

With this we conclude our synopsis of all the results that will appear in this thesis.

# Notations

| **Symbol** | **Description** |
|---|---|
| $\emptyset$ | The empty set. |
| $\mathbb{N}$ | The set of natural numbers. |
| $\mathbb{Z}$ | The ring of rational integers. |
| $\mathbb{Q}$ | The field of rational numbers. |
| $\mathbb{R}$ | The field of real numbers. |
| $\mathbb{C}$ | The field of complex numbers. |
| $\Re(s)$ | The real part of the complex number $s$. |
| $\mathbf{K}$ | A number field. |
| $\mathcal{O}_{\mathbf{K}}$ | The ring of integers associated to $\mathbf{K}$. |
| $H(\mathbf{K})$ | The Hilbert class field of $\mathbf{K}$. |
| $\zeta_n$ | An $n$-th primitive root of unity in $\mathbb{C}$. |
| $\mathbb{Q}(\zeta_n)$ | The $n$-th cyclotomic field. |
| $\varphi(n)$ | The Euler-totient function. |
| $\mu(n)$ | The Möbius function. |
| $\mathfrak{N}(\mathfrak{a})$ | The absolute norm of an ideal $\mathfrak{a}$. |
| $Li(x)$ | The logarithmic integral from 2 to $x$. |

We also use the following notations frequently.

1. For $f, g : \mathbb{R} \to \mathbb{R}$ with $g(x) > 0$ for all $x \in \mathbb{R}$, we shall say $f = o(g)$ if

$$\lim_{x \to +\infty} \frac{|f(x)|}{g(x)} = 0.$$

2. For $f, g : \mathbb{R} \to \mathbb{R}$ with $g(x) > 0$, for all $x \in \mathbb{R}$, we shall say $g(x) \gg f(x)$ if

$$\frac{|f(x)|}{g(x)} \leq M$$

for some positive constant $M$ and all $x \geq x_0$ for some $x_0$.

# Chapter 1

# Introduction

## 1.1 Euclidean domains

The Euclidean algorithm was first introduced by the Greek mathematician Euclid (300 B.C.) in his book *Elements*. In fact, it seems to have been independently discovered by Chinese and Indian mathematicians such as Aryabhata who discussed the linear equation $ax + by = c$ in his treatise Aryabhatiya [35]. The primary usage of this algorithm is to find the greatest common divisor of two integers. We recall that this algorithm only depends on the property of the set of integers which allows us to divide a number by another non-zero number and produce a remainder with smaller absolute value than the divisor. It was observed that the concept of such an algorithm can be generalized to integral domains where certain "Euclidean functions" can be defined.

**Definition 1.1.1.** *An integral domain $R$ is said to be a Euclidean domain if there exists a function*

$$\phi : R \setminus \{0\} \to \mathbb{N} \cup \{0\}$$

*with the following property. Given any $a$ and $b \neq 0$ in $R$, there exist $q$ and $r$ in*

*$R$ such that $a = bq + r$, where either $r = 0$ or $\phi(r) < \phi(b)$. We will refer to such functions as Euclidean functions.*

It is known that the remainder and quotient are both unique if and only if the domains under consideration are fields or the ring of univariate polynomials over a field [25]. Some authors insist on an extra condition that for any $a \in R$ and $b \in R \backslash \{0\}$, $\phi(ab) \geq \phi(b)$. For the sake of completeness, we note that this second condition can be dispensed with. Indeed, given the existence of a Euclidean function on an integral domain it is possible to construct another function which is Euclidean and satisfies this extra condition. For example, given the existence of a Euclidean function, we claim that the following function will satisfy both conditions,

$$\begin{aligned} \tilde{\phi}: \quad & R \setminus \{0\} \to \mathbb{N} \cup \{0\} \\ & r \to \min_{\phi} \phi(r). \end{aligned}$$

where $\phi$ ranges over all Euclidean functions on $R$.

**Proposition 1.1.2.** *The map $\tilde{\phi}$ is a Euclidean function on $R$ such that $\tilde{\phi}(ab) \geq \tilde{\phi}(b)$ for all $a \in R$ and $b \in R \backslash \{0\}$.*

*Proof.* We first prove that this map is Euclidean. Observe that, given any non-zero $b$, there exists a function $\phi$ for which $\phi(b) = \tilde{\phi}(b)$. Now for any $a \in R$, there exist $q$ and $r$ such that $a = bq + r$ and $\phi(r) < \phi(b)$ when $r \neq 0$. But this implies that $\tilde{\phi}(r) \leq \phi(r) < \phi(b) = \tilde{\phi}(b)$. Therefore, we know that $\tilde{\phi}$ is a Euclidean function.

It remains to check whether $\tilde{\phi}(ab) \geq \tilde{\phi}(b)$ for any $a \in R$ and $b$ in $R \backslash \{0\}$. To prove this, we suppose otherwise. Then, there exist $a$ and $b (\neq 0)$ such that $\tilde{\phi}(ab) < \tilde{\phi}(b)$. Now let $\phi'$ be defined as follows:

$$\phi'(c) = \begin{cases} \tilde{\phi}(c); & c \neq b \\ \tilde{\phi}(ab); & c = b. \end{cases}$$

We will now show that $\phi'$ is a Euclidean function, thereby contradicting the minimality of $\tilde{\phi}$ at $b$. This will be done in a case-wise fashion.

- **Case 1:** If $c \notin \{b, 0\}$ then for any $d \in R$, there exist $q$ and $r$ in $R$ such that $d = cq + r$ with either $r = 0$ or $\tilde{\phi}(r) < \tilde{\phi}(c)$. If $r = 0$, the condition of the Euclidean function is already satisfied. Otherwise there are two cases based on whether $r$ is equal to $b$ or not. If $r \neq b$,

  $$\phi'(r) = \tilde{\phi}(r) < \tilde{\phi}(c) = \phi'(c).$$

  Otherwise $r = b$ and, again, we have

  $$\phi'(r) = \phi'(b) = \tilde{\phi}(ab) < \tilde{\phi}(b) = \tilde{\phi}(r) < \tilde{\phi}(c) = \phi'(c).$$

- **Case 2:** Suppose that $c = b$. In this case we will divide by $ab$ instead of $c$. For any $d$ in $R$, there exist $q$ and $r$ in $R$ such that $d = abq + r$ where either $r = 0$ or $\tilde{\phi}(r) < \tilde{\phi}(ab) < \tilde{\phi}(b)$. If $r = 0$ the case is trivial as seen above. Otherwise, if $0 \neq r = b$ then $b \mid d$ in which case the remainder on division by $c$ is 0 and condition for a Euclidean function is automatically satisfied. But if $r \neq b$, then

  $$\phi'(r) = \tilde{\phi}(r) < \tilde{\phi}(ab) = \phi'(b).$$

This proves that $\phi'$ is a Euclidean function such that $\phi'(b) < \tilde{\phi}(b)$. Hence the contradiction. □

We now give few examples of Euclidean domains below.

**Example 1.1.3.** *The ring $\mathbb{Z}[\sqrt{2}]$ is Euclidean as seen by the following map:*

$$\begin{aligned} \phi \quad : \quad & \mathbb{Z}[\sqrt{2}] \to \mathbb{N} \cup \{0\} \\ & a + \sqrt{2}b \to |a^2 - 2b^2|. \end{aligned}$$

*Proof.* Let $\alpha = a + \sqrt{2}b$ and $\beta = c + \sqrt{2}d \neq 0$. Consider the element $\alpha/\beta$ in the fraction field of $\mathbb{Z}[\sqrt{2}]$, namely $\mathbb{Q}[\sqrt{2}]$. We rewrite this element as shown below:

$$\begin{aligned} \frac{\alpha}{\beta} &= m + \sqrt{2}n; \quad m, n \in \mathbb{Q} \\ &= ||m|| + \sqrt{2}||n|| + m' + \sqrt{2}n', \end{aligned}$$

where $||m||$ denotes the integer closest to $m$ and $||n||$ denotes integer closest to $n$. One immediately observes that,

$$\beta(m' + \sqrt{2}n') \in \mathbb{Z}[\sqrt{2}].$$

Further $\phi(m' + n'\sqrt{2}) < \frac{3}{4} < 1$. Therefore $\phi(\beta(m' + \sqrt{2}n')) < \phi(\beta)$, thus completing the proof of our claim. □

Note that the similar arguments may be applied to several other rings such as $\mathbb{Z}[i]$, $\mathbb{Z}[\omega]$ where $\omega$ is a primitive cube root of unity, etc. to establish the existence of a Euclidean function. But such a question of existence of a Euclidean function may also be answered without explicitly finding the map. One such non trivial example is the following.

**Example 1.1.4.** *The ring $\mathbb{Z}[\sqrt{14}]$ is a Euclidean domain.*

For a proof of the above claim, we refer the reader to [18]. This is more subtle and involves deep theorems such as those of Bombieri, Friedlander and Iwaniec on primes in arithmetic progressions [2] and the linear sieve with well factorable weights [24].

## 1.2 The work of Motzkin

A venerable problem in number theory is determining how many number fields have class number one. In other words how many number fields have rings of integers which are principal ideal domains. But as it turns out, to prove that the ring of integers is a principal ideal domain it is often easy to prove the same by showing that it is a Euclidean domain. But to prove that the ring of integers is Euclidean, it is sufficient to show the existence of a Euclidean function. Sometimes it is the absolute norm map which works as a Euclidean function, as seen in the case of $\mathbb{Z}[\sqrt{2}]$. But this need not always be the case.

The ring of integers of a number field which is Euclidean for the norm map is said to be norm Euclidean. Not every Euclidean number field is norm-Euclidean. However, if the ring of integers is not norm-Euclidean, it may still be Euclidean with respect to a different Euclidean function. In fact, the rings of integers of number fields may be divided into the following categories:

1. Those that are not Euclidean, such as the ring of integers of $\mathbb{Q}(\sqrt{-5})$, given by $\mathbb{Z}[\sqrt{-5}]$ (reference to a proof provided below);
2. Those that are Euclidean but not norm-Euclidean, such as the ring of integers of $\mathbb{Q}(\sqrt{69})$, given by $\mathbb{Z}\left[\frac{1+\sqrt{69}}{2}\right]$ (see [3] for a proof);
3. Those that are norm-Euclidean, such as $\mathbb{Z}[\sqrt{2}]$.

The problem of classifying number fields into these categories has been a subject of interest for a very long time. One of the first results in this direction was given by Dedekind in *Vorlesungen über Zahlentheorie* ("Lectures on Number Theory"), in the year 1863, based on the lectures of Dirichlet. In these notes, he proved that the rings of integers of certain quadratic fields are norm-Euclidean and showed the existence of principal ideal domains which are not norm-Euclidean.

**Theorem 1.2.1** (Dirichlet and Dedekind [7])**.** *For $d \in \{-1, -2, -3, -7, -11, 2, 3, 5, 13\}$, the ring of integers of $\mathbb{Q}(\sqrt{d})$ is norm-Euclidean. The ring of integers of $\mathbb{Q}(\sqrt{d})$ is a principal ideal domain but not norm-Euclidean for $d = -19$.*

It is also known that the ring of integers of $\mathbb{Q}(\sqrt{d})$ is a principal ideal domain and not norm-Euclidean for $d \in \{-43, -67, -163\}$. Further a result of Heilbronn [21] shows that there are only finitely many norm Euclidean real quadratic fields. In fact the complete list is now known.

The next question, of course, is whether it is possible for a domain to be Euclidean but not norm-Euclidean. This was addressed in a paper of Motzkin, published in 1949. Motzkin gave a new criterion to examine the property of an integral domain being Euclidean. He gave a constructive criterion for the existence of a Euclidean algorithm. First he introduced the concept of a product ideal and its derived set in the following manner.

**Definition 1.2.2.** *Given two subsets $S$ and $T$ of an integral domain $R$, define their product as,*

$$S \cdot T := \{st : s \in S, t \in T\}.$$

*A subset $S$ of an integral domain $R$ is called a product ideal if*

$$S \cdot (R \setminus \{0\}) \subseteq S.$$

*The derived set of a subset $S$ of $R$ is given by the set*

$$S' := \{a \in S : \exists\, b \in R \text{ such that } b + aR \subseteq S\}.$$

*Note that if $S$ is a product ideal then $S'$ is also a product ideal. Further one can inductively define the $n$-th derived set of $S$. It will henceforth be denoted by $S^{(n)}$.*

Having defined the notion of product ideals, Motzkin proved a criterion to show exactly when an integral domain is Euclidean. He showed that there exists a bijection between the set of all possible Euclidean functions on an integral domain and the set of certain sequences of product ideals. More precisely, he showed the following.

**Theorem 1.2.3** (Motzkin [28])**.** *In any integral domain $R$, the set of all Euclidean functions is in bijection with a sequence of product ideals $(P_i)_{i=0}^{\infty}$ satisfying the following properties:*

1. $P_0 = (R \setminus \{0\}) \supseteq P_1 \supseteq \dots$
2. $P_i' \subseteq P_{i+1}$
3. $\bigcap_{i=0}^{\infty} P_i = \emptyset$.

Motzkin also gave a natural notion of comparing two distinct Euclidean functions which exist on the same ring.

**Definition 1.2.4.** *Given two sequences of product ideals $(P_i)$ and $(Q_i)$ corresponding to two distinct algorithms, we say that the first algorithm is faster than the second if*

$$P_i \subseteq Q_i, \ \forall i \in \mathbb{N}.$$

Therefore, note that the 'fastest' or 'minimal' algorithm must correspond to the sequence,

$$P_0 \supseteq P_0' \supseteq \dots.$$

So in order to check if a ring is Euclidean, one might as well check if this uniquely defined fastest sequence gives rise to an algorithm. In other words, to check if a ring is Euclidean it suffices to check if $\bigcap_{n=1}^{\infty} P_0^{(n)} = \emptyset$, where $P_0^{(n)}$ denotes the $n$-th derived set of $P_0$. As a corollary, Motzkin was able to show the following.

**Corollary 1.2.5.** *For $d < 0$ and square free, the ring of integers of $\mathbb{Q}(\sqrt{d})$ is not Euclidean for any map unless*

$$d \in \{-1, -2, -3, -7, -11\}.$$

**Remark 1.2.6.** *Another interesting application of this criterion is that the ring $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ is not Euclidean for any map, not just the norm map. The same holds for the other three examples that appeared after Theorem 1.2.1.*

However Weinberger [36] observed that these definitions take a more natural interpretation if one looks at the complements of the product ideals.

**Lemma 1.2.7.** *For an integral domain $R$, let*

$$\begin{aligned} E_0 &= \{0\}; \\ E_i &= R \setminus P_0^{(i)}. \end{aligned}$$

*Then if $\bigcup_{i=0}^{\infty} E_i = R$, then $R$ is a Euclidean domain. Here $P_0^{(i)}$ is the $i$-th derived set of $P_0$ as defined above.*

Note that the converse of Lemma 1.2.7 also holds. That is, if $R$ is Euclidean, then $\bigcup_{i=0}^{\infty} E_i = R$. In this language, it is easy to check that the criterion based on the fastest algorithm translates in the following fashion.

**Lemma 1.2.8** (Weinberger [36])**.** *Let $R$ be an integral domain and let $E_0 = \{0\}$. We inductively define*

$$E_n = \{a \in R : E_{n-1} \to R/aR \text{ is onto}\} \cup E_{n-1}.$$

*The map indicated above is the restriction of the canonical projection of $R$ to $R/aR$ to $E_{n-1}$. Then if $\bigcup_{i=0}^{\infty} E_i = R$ then $R$ is a Euclidean domain.*

Under this interpretation it is easy to see that when $R$ is a Euclidean domain, one Euclidean function is given by the map

$$\phi(\alpha) = i \text{ if } \alpha \in E_i \setminus E_{i-1}.$$

Further it follows that

$$\phi(\alpha) = \phi(\alpha u) \quad \text{when } u \in R^{\times}. \tag{1.2.1}$$

## 1.3 Generalising the Euclidean algorithm

As we saw earlier, the ring of integers $\mathcal{O}_{\mathbf{K}}$ of an arbitrary number field $\mathbf{K}$ is not a principal ideal domain. It is however a Dedekind domain and in a Dedekind domain, we are only ensured of factorisation of ideals into a product of prime ideals. So if one has to produce a generalisation of the Euclidean algorithm, the first step would be to define a map on the set ideals as opposed to elements of $\mathcal{O}_{\mathbf{K}}$. The final observation from equation (1.2.1) lets us accomplish exactly that.

We can now see that our first definition of Euclidean domains can now be seen as a notion related to the set of ideals instead of elements. This was first observed by Lenstra [26]. Before we state this observation more precisely let us define the notion of inverse of a fractional ideal for a Dedekind domain. Let $\mathfrak{b}$ be a fractional ideal of an Dedekind domain $R$ and $F(R)$ be the fraction field of $R$, then

$$\mathfrak{b}^{-1} := \{x \in F(R) : x\mathfrak{b} \subseteq R\}.$$

We can now give the precise formulation of our observation.

**Definition 1.3.1.** *Let $R$ be an integral domain, $J$ be the set of all non-zero ideals of $R$. Suppose that $\psi$ is a map from $J$ to $\mathbb{N}$ . We say that $R$ is Euclidean for $\psi$ if $R$*

*is a principal ideal domain and for each $\mathfrak{b}$ in $J$ and any $x \in R\mathfrak{b}^{-1} \setminus R$, there exists $y \in R$ such that*

$$\psi(\mathfrak{b}(x-y)R) < \psi(\mathfrak{b}).$$

To prove that Definition 1.1.1 implies Definition 1.3.1 , we first observe, by the last comment of the previous section, that there exists a Euclidean map $\phi$ on $R$ such that

$$\phi(\alpha) = \phi(\alpha u), \quad u \in R^{\times}.$$

Without loss of generality, we will assume that $\phi$ denotes this specific Euclidean map. We now set $\psi(\mathfrak{b}) = \phi(b)$ and we put $a = bx$. Then there exists a $q$ such that

$$\phi(bx - bq) < \phi(b)$$

Thus for $y = q$, we have Definition 1.3.1. Conversely to prove that Definition 1.3.1 implies Definition 1.1.1, we set $\phi(b) = \psi(bR)$, then for any $a \in R$ we put $x = ab^{-1}$ and choose $y$ according to Definition 1.3.1 and put $q = y$. Therefore the equivalence of the definitions is now clear. We can now generalise the definition of Euclidean domains in the following manner. In this thesis, we will only consider the definition in the case of Dedekind domains for ease of exposition.

**Definition 1.3.2** (Lenstra [26]). *Let $R$ be a Dedekind domain, $J$ be the set of all non-zero integral ideals of $R$. Suppose that $\psi$ is a map from $J$ to $\mathbb{N}$ . We say that a non-zero fractional ideal $\mathfrak{a}$ of $R$ is Euclidean for $\psi$ if for each non- zero ideal $\mathfrak{b}$ of $J$ and any $x \in \mathfrak{a}\mathfrak{b}^{-1} \setminus \mathfrak{a}$, there exists $y \in \mathfrak{a}$ such that*

$$\psi\left(\mathfrak{a}^{-1}\mathfrak{b}(x-y)\right) < \psi(\mathfrak{b}).$$

Note that the last line of the above definition implies that the definition is invariant if $\mathfrak{a}$ is replaced by $\alpha\mathfrak{a}$ for some non-zero $\alpha$ in $R$ and this is in fact the case.

Therefore we can now state the following definition.

**Definition 1.3.3.** *If $R$ is a Dedekind domain and $\mathfrak{a}$ is a Euclidean ideal of $R$, then the class of $\mathfrak{a}$ in the class group of $R$ is called a Euclidean ideal class.*

**Remark 1.3.4.** *If $\mathbf{K}$ is a number field and $\mathcal{O}_{\mathbf{K}}$ its ring of integers with a Euclidean ideal class, then at times, by abuse of notation we shall say that $\mathbf{K}$ has a Euclidean ideal class.*

Before we go further, we would like to explain what makes this definition interesting. We know that any Euclidean domain is a Principal ideal domain. This means that the class group of a Euclidean domain is trivial. Therefore if one wants to study class groups, one must consider Dedekind domains with non trivial class groups and the first step towards this would be the case of Dedekind domains with cyclic class groups. It turns out that Dedekind domains with Euclidean ideal classes have cyclic class groups. We indicate a proof of the same below.

**Lemma 1.3.5** (Lenstra [26])**.** *Let $R$ be a Dedekind domain. If $\mathfrak{a}$ is a Euclidean ideal for $\psi$, then for any $\mathfrak{b} \in E$, there exists an $n \in \mathbb{N} \cup \{0\}$ such that*

$$[\mathfrak{b}] = [\mathfrak{a}]^n \textit{ for some } 0 \leq n \leq \psi(\mathfrak{b}).$$

*Proof.* We first observe that in a Dedekind domain every class of the class group contains an integral ideal. We can now prove this lemma by induction on the value of $\psi(\mathfrak{b})$. If $\psi(\mathfrak{b}) = 1$, then $\mathfrak{a}\mathfrak{b}^{-1} \setminus \mathfrak{a}$ must be empty. This implies that $\mathfrak{b} = R$. Therefore the lemma holds trivially for $n = 0$. Now suppose that $\psi(\mathfrak{b})$ is strictly greater than 0. For any $x \in \mathfrak{a}\mathfrak{b}^{-1} \setminus \mathfrak{a}$, there exists $y \in \mathfrak{a}$ such that $\psi\left(\mathfrak{a}^{-1}\mathfrak{b}(x - y)\right) < \psi(\mathfrak{b})$. By the induction hypothesis, we have

$$[\mathfrak{a}^{-1}\mathfrak{b}(x - y)] = [\mathfrak{a}]^m \text{ for some } 0 \leq m \leq \psi(\mathfrak{b}) - 1$$

This immediately implies that

$$[\mathfrak{b}] = [\mathfrak{a}]^n \text{ for some } 0 \leq n \leq \psi(\mathfrak{b}).$$

□

One would like to know about the converse. More precisely, one asks the following question.

Question : *If the class group of a Dedekind domain is cyclic, then does it contain a Euclidean ideal class?*

This is the very question that forms the central motivation towards this thesis. However, we only address this question in the context of rings of integers of number fields.

## 1.4 History

In the August of 1966, Hooley published a paper [22] proving, under the extended Riemann hypothesis, Artin's primitive root conjecture holds. A hallmark paper was published in 1971 by Samuel [33]. In this paper, Samuel listed various basic properties of Euclidean rings. But most notable of all, he pointed out the link between Artin's primitive root conjecture and the existence of Euclidean functions in number fields.

Shortly afterwards, in 1973, Weinberger [36] revamped Motzkin's criterion and used Hooley's method to link the existence of Euclidean functions in number fields with infinitely many units, to an extension of the Riemann hypothesis for Dedekind zeta functions for certain number fields. More precisely,

**Theorem 1.4.1** (Weinberger [36]). *Let* $\mathbf{K}$ *be an algebraic number field whose ring of integers is a principal ideal domain and has a fundamental unit* $\epsilon$. *Then the extended Riemann hypothesis implies the following :*

1. *Given any prime ideal* $\mathfrak{p}$ *of* $\mathcal{O}_{\mathbf{K}}$, *let* $Cl_{\mathfrak{p}}^{\mathbf{K}}$ *be the ray class group mod* $\mathfrak{p}$. *Then every class of* $Cl_{\mathfrak{p}}^{\mathbf{K}}$ *contains infinitely many prime ideals for which* $\epsilon$ *is a primitive root.*

2. *Every prime element of* $\mathcal{O}_{\mathbf{K}}$ *is in* $E_3$ *(defined as in Lemma 1.2.7) and therefore* $\mathcal{O}_{\mathbf{K}}$ *is Euclidean.*

Note that part 1 of Theorem 1.4.1 is essentially Artin's primitive root conjecture for number fields. In 1974, Queen [32] proved a statement analogous to Weinberger's in the function field setup. We however do not go into that for now. In 1977, Lenstra generalised the result of Weinberger to the set of $S$ integers where $|S| \geq 2$ and $S$ contains all the infinite places, for all global fields. This essentially combines the work of Weinberger and Queen but we state the number field version here for the sake of completeness.

**Theorem 1.4.2** (Lenstra [27]). *Let* $\mathbf{K}$ *be a number field and* $\mathcal{O}_{\mathbf{K}}$ *be its ring of integers. Also let* $S$ *be a set of places of* $\mathbf{K}$ *containing the infinite places. If* $\mathcal{O}_{\mathbf{K},S}$ *were to denote the ring of* $S$ *integers, with* $|S| \geq 2$, *and, if we assume that for every square free integer* $n$ *and every finite subset* $S' \subset S$, *the zeta-function of the field* $K(\zeta_n, (\mathcal{O}_{\mathbf{K},S'}^{\times})^{1/n})$ *satisfies the Riemann hypothesis for number fields, then* $\mathcal{O}_{\mathbf{K},S}$ *is Euclidean. Furthermore, its fastest algorithm* $\theta$ *is given by*

$$\theta(x) = \sum_{p \notin S} v_p(x) \cdot n_p, \qquad \forall\, x \in \mathcal{O}_{\mathbf{K},S}, \quad x \neq 0,$$

*where the sum is over all primes of* $K$ *which are not in* $S$, *and*

1. $n_p = 1$, *if the natural map from the unit group* $\mathcal{O}_{\mathbf{K},S}^{\times}$ *to the group of units of*

*the residue field is surjective.*

2. $n_p = 2$, *otherwise.*

Meanwhile, Cooke and Weinberger [5] proved that the extended Riemann hypothesis (defined in the preliminaries) implies that the natural density of primes $\mathfrak{p}$ of $\mathcal{O}_{\mathbf{K}}$, for which the map from $\mathcal{O}_{\mathbf{K}}^{\times}$ to $(\mathcal{O}_{\mathbf{K}}/\mathfrak{p})^{\times}$ is surjective, is positive. In particular, there are infinitely many primes in $E_2$ (defined in Lemma 1.2.7). In 1988, following Cooke and Weinberger, Narkiewicz was able to prove the following statement unconditionally, as a consequence of a more general result.

**Theorem 1.4.3** (Narkiewicz [29])**.** *If* $\mathbf{K} \neq \mathbb{Q}$ *is a real abelian algebraic number field, then there exist infinitely many totally split primes* $\mathfrak{p}$ *such that every non-zero residue class modulo* $\mathfrak{p}$ *contains infinitely many units, with the exception of at most two fields. If there are two exceptional fields (presumably fictitious), then both are necessarily quadratic. The lone (presumably fictitious) exceptional field is necessarily cubic.*

The proof of this theorem again follows from a special application of the lower bound sieve using the usual form of the Bombieri-Vinogradov theorem for rational primes.

For the rest of this chapter we will assume that $\mathcal{O}_{\mathbf{K}}$ is a principal ideal domain. In 1995, Clark and Murty were able to reformulate Motzkin's criterion purely in terms of the prime ideals of $\mathcal{O}_{\mathbf{K}}$. In 2004, Harper added to this variant a special application of the large sieve inequality. This application essentially gives us a quantitative condition under which $\mathcal{O}_{\mathbf{K}}$ is Euclidean. Before we go into the application, we need the following definition.

**Definition 1.4.4.** *Let* $B_1$ *denote the set of all primes* $\pi$ *of* $\mathcal{O}_{\mathbf{K}}$ *such that the natural map from* $\mathcal{O}_{\mathbf{K}}^{\times} \to (\mathcal{O}_{\mathbf{K}}/\pi\mathcal{O}_{\mathbf{K}})^{\times}$ *is surjective. Further, define*

$$B_1(x) := \{b \in B_1 : |\mathfrak{N}(b)| \leq x\}.$$

Having stated the above definition, we now present Harper's theorem.

**Theorem 1.4.5** (Harper [18]). *If $B_1(x) \gg \frac{x}{\log^2 x}$, then $\mathcal{O}_{\mathbf{K}}$ is Euclidean.*

In the same paper Harper published a proof of the fact that $\mathbb{Z}[\sqrt{14}]$ is Euclidean. The proof crucially depends on a lemma of Heath-Brown which in turn follows from Iwaniec's linear sieve with a bilinear error term as well as earlier work of Gupta and Murty [14]. In the same year, Harper and Murty published the following result for all abelian extensions of unit rank at least 3, using similar techniques. More precisely, they showed the following.

**Theorem 1.4.6** (Harper and Murty [19]). *Let $\mathbf{K}/\mathbb{Q}$ be an abelian extension of degree $n$ and let $r$ be the rank of the unit group of $\mathcal{O}_{\mathbf{K}}$. If $r \geq 3$, then $\mathcal{O}_{\mathbf{K}}$ is Euclidean if and only if it is a principal ideal domain.*

In 2007, Narkiewicz [31] generalised Harper and Murty's method to all real quadratic fields with at most two exceptions and all Galois cubic extensions with at most one exception. He showed that:

**Theorem 1.4.7** (Narkiewicz [31]). *Let $\mathbf{K}$ be a finite Galois extension of $\mathbb{Q}$ with $\mathcal{O}_{\mathbf{K}}$ having class number one.*

1. *If $\mathbf{K}$ is a real quadratic then $\mathcal{O}_{\mathbf{K}}$ is Euclidean, except for at most two fields.*
2. *If $\mathbf{K}$ is a cubic extension then $\mathcal{O}_{\mathbf{K}}$ is Euclidean, except for at most one field.*

With this we will conclude the history on the Euclidean domain front since these are the results we will be generalising in this thesis.

We can now look at the analogous work that has been carried out on the Euclidean ideal class front. The seminal work that started the study of Euclidean ideal classes was written by Lenstra ([26]) in the year 1979. Lenstra defined the notion of Euclidean ideal classes on integral domains and showed that if an integral domain has a Euclidean ideal class it is automatically a Dedekind domain with cyclic class group. However, as mentioned earlier, we will restrict our definitions and exposition to Dedekind domains and in particular to rings of integers of number fields. One of the most notable results of this paper is the following.

**Theorem 1.4.8** (Lenstra [26]). *Under the extended Riemann hypothesis, a number field with unit rank at least one has cyclic class group if and only if it has a Euclidean ideal class.*

There have been some works in trying to find a family of fields with Euclidean ideal classes such as in [23], [12], etc. But to the best of our knowledge there is only one which attempts at making the above theorem unconditional.

**Theorem 1.4.9** (Graves and Murty [14]). *Suppose that the unit rank of a number field* $\mathbf{K}$ *is at least* $4$ *and that the Hilbert class field of* $\mathbf{K}$ *is abelian over* $\mathbb{Q}$. *Further suppose that* $\mathbb{Q}(\zeta_f)/\mathbf{K}$ *is cyclic where* $f$ *is the conductor of the Hilbert class field. Then the class group of* $\mathbf{K}$ *is cyclic if and only if there is a Euclidean ideal class.*

The main objective of this thesis is to improve this result to unit rank 3 along the lines of the work of Harper and Murty and prove results analogous to that of Narkiewicz in Euclidean ideal class setup. In the next section we give a detailed summary of our results obtained in the context of Euclidean ideal classes.

## 1.5 Our results

### 1.5.1 Bound on unit rank

The first result that will be appearing in this thesis is about the existence of Euclidean ideal classes when the rank of the free part of $\mathcal{O}_{\mathbf{K}}$ is sufficiently large. From the section on history, one gathers that the unit rank plays an important role in the context of this problem of existence of Euclidean ideal classes. We first show that for a family of number fields, there exists a lower bound on the unit rank $r$ such that whenever the unit rank exceeds $r$, these number fields have Euclidean ideal classes. More precisely, we prove the following.

**Theorem 1.5.1** ([34]). *Let $\mathbf{K}$ be a number field and $H(\mathbf{K})$ its Hilbert class field. Suppose that the $H(\mathbf{K})$ is abelian over $\mathbb{Q}$. Let $f$ be the smallest even positive integer such that $H(\mathbf{K}) \subseteq \mathbb{Q}(\zeta_f)$. If the Galois group of $\mathbb{Q}(\zeta_f)$ over $\mathbf{K}$ is cyclic, then there exists a finite natural number $r$ such that if $\mathbf{K}$ has unit rank at least $r$, $\mathbf{K}$ has a Euclidean ideal class.*

The proof of this theorem will appear in Chapter 3.

### 1.5.2 Large unit rank

The next result is an improvement of Theorem 1.4.9. In a joint work with Deshouillers and Gun [6], we were able to extend the aforementioned result to number fields whose unit rank is 3. More precisely, we prove the following.

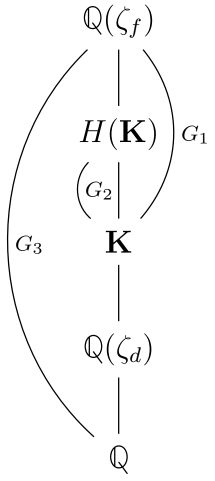
**Theorem 1.5.2** ([6]). *Suppose that $\mathbf{K}$ is a number field with unit rank at least $3$ and that the Hilbert class field $H(\mathbf{K})$ of $\mathbf{K}$ is abelian over $\mathbb{Q}$. Also suppose that the conductor of $\mathbf{K}$ is $f$ and $\mathbb{Q}(\zeta_f)$ over $\mathbf{K}$ is cyclic. Then $\mathbf{K}$ has a Euclidean ideal class.*

Now if we assume the conjecture of Elliott and Halberstam, we can derive a stronger result. In particular, we have the following theorem.

**Theorem 1.5.3** ([6]). *Let $\mathbf{K}$ be a number field such that the Hilbert class field $H(\mathbf{K})$ is abelian over $\mathbb{Q}$ and the Galois group $Gal(\mathbb{Q}(\zeta_f)/\mathbf{K})$ is cyclic where $f$ is the conductor of $\mathbf{K}$. Now if the Elliott and Halberstam conjecture is true and the unit rank of $\mathbf{K}$ is at least $2$, then $\mathbf{K}$ has a Euclidean ideal class.*

The detailed proof of this statement can be found in Chapter 4. We note here that our result is actually stronger than Theorem 1.5.2. The result in full generality is stated below.

**Theorem 1.5.4** ([6]). *Let* $\mathbf{K}$ *be a number field with unit rank at least* 3 *and suppose that its Hilbert class field* $H(\mathbf{K})$ *is abelian over* $\mathbb{Q}$. *Further let* $\mathbb{Q}(\zeta_d)$ *be the maximal cyclotomic subextension inside* $\mathbf{K}$. *Consider the diagram :*



*Let* $G_3$ *be the Galois group of* $\mathbb{Q}(\zeta_f)$ *over* $\mathbb{Q}$. *Then*

$$G_3 = \{\sigma_a \ : \ 1 \leq a \leq n, \quad (a, f) = 1\},$$

*where* $\sigma_a : \mathbb{Q}(\zeta_f) \to \mathbb{Q}(\zeta_f)$ *is such that* $\sigma_a(\zeta_f) = \zeta_f^a$. *If* $G_1$ *is the Galois group of* $\mathbb{Q}(\zeta_f)$ *over* $\mathbf{K}$, $G_2$ *the Galois group of* $H(\mathbf{K})$ *over* $\mathbf{K}$, *the class group of* $\mathbf{K}$ *is cyclic and*

$$\big\{\sigma_a \in G_1 \ : \quad G_2 = \langle \sigma_a|_{H(\mathbf{K})} \rangle\big\} \bigcap \left\{\sigma_a \in G_3 \ : \ a \equiv 1 \bmod d, \ \left(\frac{a-1}{d}, \ \frac{f}{d}\right) = 1\right\} \neq \phi,$$

*then it has a Euclidean ideal class. Here the notation* $G_2 = \langle \sigma_a|_{H(\mathbf{K})} \rangle$ *means that* $\sigma_a|_{H(\mathbf{K})}$ *generates* $G_2$.

This concludes our section on number fields with large unit rank.

### 1.5.3 Small unit rank

The next result we state is a partial generalisation of the work of Narkiewicz as stated in Theorem 1.4.7. This is a joint work with Gun. Before we state our results, we introduce few notations. Let $\mathbf{K}_1, \mathbf{K}_2$ and $\mathbf{K}_3$ be number fields with Hilbert class fields $\mathbf{H}(\mathbf{K}_1), \mathbf{H}(\mathbf{K}_2)$ and $\mathbf{H}(\mathbf{K}_3)$ respectively, all abelian over $\mathbb{Q}$. Also let $f_1, f_2$ and $f_3$ be their conductors, i.e. $\mathbb{Q}(\zeta_{f_1}), \mathbb{Q}(\zeta_{f_2})$ and $\mathbb{Q}(\zeta_{f_3})$ be the smallest cyclotomic fields containing $\mathbf{H}(\mathbf{K}_1), \mathbf{H}(\mathbf{K}_2)$ and $\mathbf{H}(\mathbf{K}_3)$ respectively. Set $f$ to be the least common multiple of $16, f_1, f_2, f_3$ if $\mathbf{K}_1, \mathbf{K}_2, \mathbf{K}_3$ are real quadratic and the least common multiple of $16, f_1, f_2$ if $\mathbf{K}_1, \mathbf{K}_2$ are real cubic. Further, $\mathbf{F} := \mathbb{Q}(\zeta_f)$. In this set up, we have the following theorems.

**Theorem 1.5.5** ([15]). *Let $\mathbf{K}_1, \mathbf{K}_2$ be distinct real cubic fields with prime class numbers and $\mathbf{H}(\mathbf{K}_1), \mathbf{H}(\mathbf{K}_2), \mathbf{F}, f$ be as above. Also let $G$ be the Galois group of $\mathbf{F}$ over $\mathbf{K}_1\mathbf{K}_2$, $G_\ell$ be the Galois group of $\mathbf{F}$ over $\mathbb{Q}(\zeta_\ell)$, where either $\ell$ is an odd prime dividing $f$ or $\ell = 4$ and $Gal(\mathbf{F}/\mathbf{H}(\mathbf{K}_i))$ be the Galois group of $\mathbf{F}/\mathbf{H}(\mathbf{K}_i)$ for $i = 1, 2$. If*

$$G \not\subset \bigcup_{\ell} G_\ell \bigcup \ Gal(\mathbf{F}/\mathbf{H}(\mathbf{K}_1)) \bigcup \ Gal(\mathbf{F}/\mathbf{H}(\mathbf{K}_2)),$$

*then at least one of $\mathbf{K}_1, \mathbf{K}_2$ has a Euclidean ideal class.*

We also have an analogous result in the quadratic case.

**Theorem 1.5.6** ([15]). *Let $\mathbf{K}_1, \mathbf{K}_2$ and $\mathbf{K}_3$ be distinct real quadratic fields with prime class numbers and $\mathbf{H}(\mathbf{K}_1)$, $\mathbf{H}(\mathbf{K}_2)$, $\mathbf{H}(\mathbf{K}_3), \mathbf{F}$, $f$ be as above. Also let $G$ be the Galois group of $\mathbf{F}$ over $\mathbf{K}_1\mathbf{K}_2\mathbf{K}_3$, $G_\ell$ be the Galois group of $\mathbf{F}$ over $\mathbb{Q}(\zeta_\ell)$, where either $\ell$ is an odd prime dividing $f$ or $\ell = 4$ and $Gal(\mathbf{F}/\mathbf{H}(\mathbf{K}_i))$ be the Galois group of $\mathbf{F}/\mathbf{H}(\mathbf{K}_i)$ for $i = 1, 2, 3$. If*

$$G \not\subset \bigcup_{\ell} G_\ell \bigcup \ Gal(\mathbf{F}/\mathbf{H}(\mathbf{K}_1)) \bigcup \ Gal(\mathbf{F}/\mathbf{H}(\mathbf{K}_2)) \bigcup \ Gal(\mathbf{F}/\mathbf{H}(\mathbf{K}_3)),$$

*then at least one of* $\mathbf{K}_1, \mathbf{K}_2, \mathbf{K}_3$ *has a Euclidean ideal class.*

Now if we assume the Elliott and Halberstam conjecture, we can strengthen Theorem 1.5.6.

**Theorem 1.5.7** ([15]). *Let* $\mathbf{K}_1$ *and* $\mathbf{K}_2$ *be distinct real quadratic fields with prime class numbers and* $\mathbf{H}(\mathbf{K}_1)$, $\mathbf{H}(\mathbf{K}_2), \mathbf{F}$ *and* $f$ *be as above. Also let* $G$ *be the Galois group of* $\mathbf{F}$ *over* $\mathbf{K}_1\mathbf{K}_2$, $G_\ell$ *be the Galois group of* $\mathbf{F}$ *over* $\mathbb{Q}(\zeta_\ell)$, *where either* $\ell$ *is an odd prime dividing* $f$ *or* $\ell = 4$ *and* $Gal(\mathbf{F}/\mathbf{H}(\mathbf{K}_i))$ *be the Galois group of* $\mathbf{F}/\mathbf{H}(\mathbf{K}_i)$ *for* $i = 1, 2$. *If*

$$G \not\subset \bigcup_{\ell} G_\ell \bigcup \ Gal(\mathbf{F}/\mathbf{H}(\mathbf{K}_1)) \bigcup \ Gal(\mathbf{F}/\mathbf{H}(\mathbf{K}_2)),$$

*then at least one of* $\mathbf{K}_1, \mathbf{K}_2$ *has a Euclidean ideal class provided the Elliott and Halberstam conjecture holds.*

Theorem 1.5.6 allows us to prove the following corollary.

**Corollary 1.5.8** ([15]). *Let* $p_1, q_1, p_2, q_2, p_3, q_3$ *be six distinct primes which are congruent to* $1 \bmod 4$. *For* $j \in \{1, 2, 3\}$, *if each* $\mathbf{K}_j := \mathbb{Q}(\sqrt{p_j q_j})$ *has class number* $2$, *then at least one of them has a Euclidean ideal class.*

As a concrete example, we can show that one of $\mathbb{Q}(\sqrt{221}), \mathbb{Q}(\sqrt{305})$ or $\mathbb{Q}(\sqrt{1073})$ has a Euclidean ideal class. Details about these results can be found in Chapter 5.

With this we conclude our section on the results that will appear in this thesis.

## 1.6 Organisation of the thesis

The second chapter will deal with some preliminaries required for our work. The third chapter will explore the effect of varying the sieves used in the context of this problem. The fourth chapter extends the result of Graves and Murty ([14]). Finally chapter five will deal with a generalisation of the theorem of Narkiewicz to Euclidean ideal classes ([31]).

# Chapter 2

# Preliminaries

In this chapter we set the notations and introduce the preliminaries required for this thesis. Throughout this thesis, $\mathbb{N}$ denotes the set of natural numbers, $\mathbb{Z}$ denotes the ring of rational integers, $\mathbb{Q}$ denotes the field of rational numbers and $\mathbb{C}$ denotes the field of complex numbers. This chapter is partitioned into three parts, namely the algebraic part (Section 2.1), the sieve-theoretic part (Section 2.2) and the arithmetic part (Section 2.3).

We begin with the first part.

## 2.1 Algebraic number theory

We start with definitions of some basic objects.

**Definition 2.1.1.** *A number field* $\mathbf{K}$ *is a field extension of* $\mathbb{Q}$ *inside* $\mathbb{C}$*, of finite degree.*

Some examples of number fields are $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-5})$, $\mathbb{Q}(2^{1/3})$, $\mathbb{Q}(\sqrt{-7}, \sqrt{17})$ and $\mathbb{Q}(\zeta_n)$ where $\zeta_n$ is a primitive $n$-th root of unity.

Analogous to the ring of integers $\mathbb{Z}$ in $\mathbb{Q}$, we can define a ring of "integral" elements for a number field $\mathbf{K}$. More precisely,

**Definition 2.1.2.** *An element $b$ in a number field $\mathbf{K}$ is said to be integral over $\mathbb{Z}$ if it satisfies a monic polynomial over $\mathbb{Z}$. The set of integral elements in $\mathbf{K}$ form a ring, and this ring is called the ring of integers of $\mathbf{K}$. We shall henceforth denote it by $\mathcal{O}_{\mathbf{K}}$.*

We now consider the rings of integers associated to the examples of number fields mentioned above. They are as follows: $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{-5}]$, $\mathbb{Z}[2^{1/3}]$, $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}, \frac{1+\sqrt{17}}{2}]$ and $\mathbb{Z}[\zeta_n]$. We will see some nice properties of $\mathcal{O}_{\mathbf{K}}$. However, before we state them, we need some technical definitions which we introduce now.

**Definition 2.1.3.** *Let $R$ be an integral domain and $F(R)$ its fraction field. Then a fractional ideal is any finitely generated $R$-submodule of $F(R)$.*

Let us consider the case when $R = \mathbb{Z}$, then $F(R) = \mathbb{Q}$. The modules $2\mathbb{Z}$ and $\frac{1}{2}\mathbb{Z}$ are both fractional ideals of $\mathbb{Z}$. We will now try to attribute structure to the set of all fractional ideals of the integral domain $R$.

**Definition 2.1.4.** *Given two $R$ submodules of $F(R)$, say $M$ and $N$, we define the product $MN$ as follows:*

$$MN := \left\{ \sum_{i=1}^{n} x_i y_i \;:\; x_i \in M, y_i \in N \right\}.$$

One can show that $MN$ is also a fractional ideal. Therefore the set of all fractional ideals of the integral domain $R$ form a monoid with $R$ acting as identity. This brings us naturally to the next definition.

**Definition 2.1.5.** *An $R$-submodule $M$ of $F(R)$ is said to be invertible if there exists another $R$-submodule $N$ of $F(R)$ such that $MN = R$.*

Having defined the notion of invertibility, we now consider the setup where the monoid of fractional ideals becomes invertible.

**Definition 2.1.6.** *An integral domain whose every non-zero fractional ideal is invertible is called a Dedekind domain.*

We note that such rings do exist. For example: $\mathbb{Z}[i]$, $\mathbb{F}_p[X]$ where $\mathbb{F}_p$ is the finite field of $p$ elements, etc. Let us briefly look at some properties of Dedekind domains.

1. Every non-zero fractional ideal of a Dedekind domain can be factorized into a finite product of prime ideals (possibly with negative exponents).

2. Given a number field $\mathbf{K}$, $\mathcal{O}_{\mathbf{K}}$ is a Dedekind domain and $\mathbf{K}$ is the fraction field of $\mathcal{O}_{\mathbf{K}}$. This gives us an infinite family of examples of Dedekind domains.

3. Every principal ideal domain is a Dedekind domain while the converse does not hold. For instance, $\mathbb{Z}[\sqrt{-5}]$ is a Dedekind domain but it is not a principal ideal domain.

4. (Dirichlet's unit theorem) The multiplicative group of units of $\mathcal{O}_{\mathbf{K}}$, denoted by $\mathcal{O}_{\mathbf{K}}^{\times}$, is a finitely generated abelian group. Further the rank of the free part of $\mathcal{O}_{\mathbf{K}}^{\times}$ is called the unit rank of $\mathcal{O}_{\mathbf{K}}$ (or by abuse of notation, unit rank of $\mathbf{K}$). If we consider a minimal generating set of the free part of $\mathcal{O}_{\mathbf{K}}^{\times}$, any element of this set is called a fundamental unit.

We would also like to state the definition of the Dedekind zeta function at this stage.

**Definition 2.1.7.** *Given a number field* $\mathbf{K}$*, we can associate to it a zeta function in the following manner. For* $s \in \mathbb{C}$*, let*

$$\zeta_{\mathbf{K}}(s) \;:=\; \sum_{\substack{\mathfrak{a}\neq(0);\\ \mathfrak{a} \textit{ integral ideal of } \mathcal{O}_{\mathbf{K}}}} \frac{1}{\mathfrak{N}(\mathfrak{a})^s} \quad \textit{in} \quad \Re(s) > 1$$

*where $\mathfrak{N}(\mathfrak{a})$ is used to denote the cardinality of $\mathcal{O}_{\mathbf{K}}/\mathfrak{a}$ (known as the absolute norm of the integral ideal $\mathfrak{a}$) and $\zeta_{\mathbf{K}}$ is called the Dedekind zeta function associated to the number field $\mathbf{K}$.*

It is known that the Dedekind zeta function has a meromorphic continuation to the entire complex plane.

**Conjecture 2.1.8** (Extended Riemann hypothesis)**.** *The zeroes of the above mentioned extension of $\zeta_{\mathbf{K}}$ in the strip $0 < \Re(s) < 1$ lie on the line $\Re(s) = \frac{1}{2}$.*

Now coming back to Dedekind domains, since the set of all fractional ideals forms an abelian group, we can talk about a structure on quotients of this abelian group. This brings us to the next subsection on class groups and ray class groups.

### 2.1.1 Class groups and ray class groups

The set of all non-zero fractional ideals of $\mathcal{O}_{\mathbf{K}}$ forms a group and the set of non-zero principal fractional ideals forms a subgroup. This brings us to the notion of class groups.

**Definition 2.1.9.** *The quotient group of the group of all non-zero fractional ideals of a Dedekind domain $R$ modulo the subgroup of non-zero principal fractional ideals is called the class group of $R$. This will be denoted by $Cl_R$. The cardinality of this group, if finite, is called the class number and is denoted by $h_R$.*

The class group of $R$ measures how far $R$ is from being a principal ideal domain. It is easy to see that a Dedekind domain is a principal ideal domain if and only if it has trivial class group. However another fundamental theorem of algebraic number theory states that even if $\mathcal{O}_{\mathbf{K}}$ is not a principal ideal domain it is, in some sense, not far from it. More precisely,

**Theorem 2.1.10.** *Given a number field* $\mathbf{K}$*, the class number of* $\mathcal{O}_{\mathbf{K}}$ *is finite.*

The study of growth of class numbers and the distribution of $p$-torsion elements in class groups corresponding to rings of integers of number fields is a subject of great interest to number theorists. In order to study such properties of class groups, we resort to the techniques of class field theory. Class field theory generalises the notion of class groups and connects them to Galois groups of abelian extensions of number fields. As a special case it allows us to study class groups as Galois groups of certain distinguished extensions. For the sake of completeness, we will provide below a short account of "ray class groups" and the theorems that associate them to Galois groups.

Let us begin with the definition of a modulus. For the following discussion, we fix a number field $\mathbf{K}$.

**Definition 2.1.11.** *A modulus* $\mathfrak{m}$ *of* $\mathbf{K}$ *is a formal product* $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ *where* $\mathfrak{m}_0$ *is a non-zero integral ideal of* $\mathcal{O}_{\mathbf{K}}$ *and* $\mathfrak{m}_\infty$ *is a subset (possibly empty) of the set of all real places on* $\mathbf{K}$ *(set of all embeddings of* $\mathbf{K}$ *into* $\mathbb{R}$ *). Further, we say that a prime ideal divides* $\mathfrak{m}$ *if it divides* $\mathfrak{m}_0$ *in the usual sense and that a real place divides* $\mathfrak{m}$ *if it belongs to* $\mathfrak{m}_\infty$*.*

Using this idea of modulus we generalise the idea of class groups in the following fashion.

**Definition 2.1.12.** *Given a modulus* $\mathfrak{m}$*, let* $I_{\mathfrak{m}}^{\mathbf{K}}$ *denote the set of all non-zero fractional ideals of the number field* $\mathbf{K}$ *co-prime to* $\mathfrak{m}_0$*. Suppose that*

$$\mathbf{K}_{\mathfrak{m},1} := \{\alpha \in \mathbf{K}^* \ : \ v_{\mathfrak{p}}(\alpha - 1) \geq e_{\mathfrak{p}},\ \sigma(\alpha) > 0\, \forall\, \sigma \in \mathfrak{m}_\infty\},$$

*where* $e_{\mathfrak{p}}$ *denotes the power of the prime ideal* $\mathfrak{p}$ *in the ideal* $\mathfrak{m}_0$ *for* $\mathfrak{p}|\mathfrak{m}_0$*,* $v_{\mathfrak{p}}(x)$ *is* *the power of* $\mathfrak{p}$ *appearing in the prime factorisation of* $x\mathcal{O}_{\mathbf{K}}$ *and*

$$P_{\mathfrak{m}}^{\mathbf{K}} := \{(\alpha) : \alpha \in \mathbf{K}_{\mathfrak{m},1}\}.$$

*Then* $Cl_{\mathfrak{m}}^{\mathbf{K}} := I_{\mathfrak{m}}^{\mathbf{K}}/P_{\mathfrak{m}}^{\mathbf{K}}$ *is known as the ray class group modulo* $\mathfrak{m}$.

**Remark 2.1.13.** *We observe that the group* $Cl_{\mathcal{O}_{\mathbf{K}}}^{\mathbf{K}} = Cl_{\mathcal{O}_{\mathbf{K}}}$.

Let us first compute the ray class group of the field $\mathbb{Q}$ corresponding to the modulus $(m)\mathfrak{m}_\infty$ for some $m \in \mathbb{Z} \setminus \{0\}$, where $\mathfrak{m}_\infty$ contains the unique real place corresponding to $\mathbb{Q}$.

We first note that

$$I_{(m)\mathfrak{m}_\infty}^{\mathbb{Q}} = \{(a/b) : (|a|, |m|) = (|b|, |m|) = 1\}$$

and

$$P_{(m)\mathfrak{m}_\infty}^{\mathbb{Q}} = \{(a/b) \in I_{(m)\mathfrak{m}_\infty}^{\mathbb{Q}} : \ a \equiv b \bmod m, \ a \text{ and } b \text{ are of the same sign } \}.$$

Now consider the following map:

$$\begin{array}{rcl} I_{(m)\mathfrak{m}_\infty}^{\mathbb{Q}} & \to & (\mathbb{Z}/(|m|\mathbb{Z}))^\times \\ (a/b) & \to & ab^{-1} \end{array}$$

where we choose a positive generator for $(a/b)$. This homomorphism is obviously surjective because for each $c \bmod |m|$ ($c$ chosen to be positive), we can just look at the ideal generated by $c$ on the left. Further, the kernel is exactly $P_{(m)\mathfrak{m}_\infty}^{\mathbb{Q}}$. So for a modulus with the infinite place the ray class group of $\mathbb{Q}$ is isomorphic to $(\mathbb{Z}/|m|\mathbb{Z})^\times$. Similarly for the modulus $\mathfrak{m} = (m)$ for some $m \in \mathbb{Z} \setminus \{0\}$, we consider the homomorphism from $I_{(m)}^{\mathbb{Q}}$to $(\mathbb{Z}/|m|\mathbb{Z})^\times/\{\pm 1\}$. This will show that the ray class group in this case is isomorphic to $(\mathbb{Z}/|m|\mathbb{Z})^{\times}/\{\pm 1\}$.

As mentioned earlier, class field theory helps us characterise abelian extensions of a number field $\mathbf{K}$ using ray class groups. But in order to demonstrate this phenomenon, we need to define ramified and split primes corresponding to arbitrary extensions of a number field $\mathbf{K}$ of finite degree over $\mathbf{K}$.

**Definition 2.1.14.** *Given a field extension of number fields $\mathbf{L}$ over $\mathbf{K}$, let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_{\mathbf{K}}$. Consider the factorisation of $\mathfrak{p}\mathcal{O}_{\mathbf{L}}$, the ideal generated by $\mathfrak{p}$ in $\mathcal{O}_{\mathbf{L}}$. Let*

$$\mathfrak{p}\mathcal{O}_{\mathbf{L}} = \mathfrak{q}_1^{e_1} \dots \mathfrak{q}_n^{e_n},$$

*where $\mathfrak{q}_i$ are prime ideals of $\mathcal{O}_{\mathbf{L}}$. We say that the prime ideals $\mathfrak{q}_i$ lie above the prime $\mathfrak{p}$. If any of the $e_i's$ are greater than one, the prime is said to be ramified. The dimension of $\mathcal{O}_{\mathbf{L}}/\mathfrak{q}_i$ as a $\mathcal{O}_{\mathbf{K}}/\mathfrak{p}$ vector space is called the residual degree or degree of $\mathfrak{q}_i$ with respect to the extension $\mathbf{L}/\mathbf{K}$ and is denoted by $f_i$. In addition if $e_i = f_i = 1$ for all $i$, we say that the prime ideal of $\mathbf{K}$ is totally split in $\mathbf{L}$ . A real place of $\mathbf{K}$ is said to ramify if it extends to an embedding of $\mathbf{L}$ into $\mathbb{C}$ such that the image is not contained in $\mathbb{R}$.*

We would now like to know if there is an easy way to find all the ramified primes of an extension $\mathbf{L}/\mathbf{K}$. This brings us to the next subsection : Discriminant.

### 2.1.2 Discriminant

Given an extension of number fields $\mathbf{L}/\mathbf{K}$, let $W = (w_1, \dots w_n)$ be a basis of $\mathbf{L}/\mathbf{K}$. We define the discriminant of $W$ in the following manner:

$$D_{\mathbf{L}/\mathbf{K}}(W) = det((\sigma_i w_j)_{\{i,j\}})^2$$

where $\sigma_i$ ranges over the distinct $\mathbf{K}$ embeddings of $\mathbf{L}$ into $\mathbb{C}$. We can now define the discriminant ideal of $\mathcal{O}_{\mathbf{L}}/\mathcal{O}_{\mathbf{K}}$ as follows.

**Definition 2.1.15.** *The $\mathcal{O}_{\mathbf{K}}$ module generated by all the $D_{\mathbf{L}/\mathbf{K}}(W)$ where $W$ ranges over all the bases of $\mathbf{L}/\mathbf{K}$ contained in $\mathcal{O}_{\mathbf{L}}$ is called the discriminant of $\mathcal{O}_{\mathbf{L}}/\mathcal{O}_{\mathbf{K}}$, denoted $d_{\mathbf{L}/\mathbf{K}}$.*

It is immediate that the discriminant is an ideal of $\mathcal{O}_{\mathbf{K}}$. But what is really interesting is that a prime ideal $\mathfrak{p}$ of $\mathcal{O}_{\mathbf{K}}$ ramifies in $\mathbf{L}$ if and only if it divides the discriminant.

**Example 2.1.16.** *Given a quadratic field $\mathbf{K} = \mathbb{Q}(\sqrt{d})$. One can show that*

$$d_{\mathbf{K}/\mathbb{Q}} = \begin{cases} (d) & \text{if } d \equiv 1 \bmod 4; \\ (4d) & \text{if } d \equiv 2, 3 \bmod 4. \end{cases}$$

Another useful example is the following.

**Example 2.1.17.** *For a cyclotomic field $\mathbf{K} = \mathbb{Q}(\zeta_n)$, the discriminant*

$$d_{\mathbf{K}/\mathbb{Q}} = \left( \frac{n^{\varphi(n)}}{\prod_{p|n} p^{\varphi(n)/(p-1)}} \right).$$

*where $\varphi$ is used to denote the Euler totient function.*

**Remark 2.1.18.** *We should, at this juncture, remark that the discriminant of a number field $\mathbf{K}$ over $\mathbb{Q}$ may also be defined as the discriminant of a $\mathbb{Z}$ basis of $\mathcal{O}_{\mathbf{K}}$. In this case, the discriminant becomes an integer. Further the ideal generated by this integer will coincide with the discriminant ideal as defined above.*

Another important property of discriminants which we will use later is the following.

**Theorem 2.1.19.** *Let* $\mathbf{L}_1$ *and* $\mathbf{L}_2$ *be two extensions of* $\mathbb{Q}$ *such that* $\mathbf{L}_1 \cap \mathbf{L}_2 = \mathbb{Q}$*. Further if the discriminants* $d_{\mathbf{L}_1}$ *and* $d_{\mathbf{L}_2}$ *are relatively prime, then* $d_{\mathbf{L}_1\mathbf{L}_2} = d_{\mathbf{L}_1}^{[\mathbf{L}_2:\mathbf{K}]} d_{\mathbf{L}_2}^{[\mathbf{L}_1:\mathbf{K}]}$.

Now that we have a way of finding ramified primes, the next step would be to do the same for split primes.

### 2.1.3 Artin symbol and its properties

Now we come to a key ingredient which associates a Galois element of the extension $\mathbf{L}$ of $\mathbf{K}$, provided $\mathbf{L}/\mathbf{K}$ is Galois, to a prime ideal of $\mathcal{O}_{\mathbf{K}}$.

**Theorem 2.1.20.** *Given a Galois extension* $\mathbf{L}/\mathbf{K}$ *of number fields, an unramified prime ideal* $\mathfrak{p}$ *in* $\mathcal{O}_{\mathbf{K}}$ *and a prime ideal* $\mathfrak{q}$ *above it in* $\mathcal{O}_{\mathbf{L}}$*, there is a unique Galois element* $\sigma$ *in the Galois group of* $\mathbf{L}/\mathbf{K}$ *such that*

$$\sigma(a) \equiv a^{\mathfrak{N}(\mathfrak{p})} \bmod \mathfrak{q} \quad \textit{for all } a \in \mathcal{O}_{\mathbf{L}}.$$

*Such an element is called the Artin symbol corresponding to* $\mathfrak{q}$ *and the extension* $\mathbf{L}/\mathbf{K}$*. It is denoted by* $\left(\frac{\mathbf{L}/\mathbf{K}}{\mathfrak{q}}\right)$*. Here* $\mathfrak{N}(\mathfrak{p})$ *denotes the absolute norm of the ideal* $\mathfrak{p}$*.*

One can show that for each prime $\mathfrak{p}$ in $\mathbf{K}$, the set of Artin symbols of the prime ideals above $\mathfrak{p}$ is a conjugacy class in the Galois group of $\mathbf{L}/\mathbf{K}$. If the extension is abelian, this conjugacy class is nothing but an element of the Galois group of $\mathbf{L}/\mathbf{K}$.

Therefore if $\mathbf{L}/\mathbf{K}$ is abelian, the Artin symbol of any prime above (in $\mathcal{O}_{\mathbf{L}}$) can be determined without ambiguity by the prime below (in $\mathcal{O}_{\mathbf{K}}$). From now onwards, we will only consider abelian extensions and by abuse of notation we will talk about $\left(\frac{\mathbf{L}/\mathbf{K}}{\mathfrak{p}}\right)$ where $\mathfrak{p}$ is a prime ideal in $\mathcal{O}_{\mathbf{K}}$. As an example let us compute the Artin symbol of a prime ideal in $\mathbb{Z}$ with respect to a cyclotomic field $\mathbb{Q}(\zeta_n)$.

**Example 2.1.21.** *Consider a prime $p \in \mathbb{Z}$ and the field $\mathbb{Q}(\zeta_n)$ such that $(p,n) = 1$. We know that the prime ideal $p\mathbb{Z}$ does not ramify in $\mathbb{Q}(\zeta_n)$, so the Artin symbol $\left(\frac{\mathbb{Q}(\zeta_n)/\mathbb{Q}}{p\mathbb{Z}}\right)$ is well defined. Let $\mathfrak{q}$ be any prime ideal above $p\mathbb{Z}$ in $\mathbb{Q}(\zeta_n)$. Consider the element $\sigma \in Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ which takes $\zeta_n$ to $\zeta_n^{|p|}$. An immediate application of the Binomial expansion will show that*

$$\sigma(a) \equiv a^{|p|} \bmod \mathfrak{q} \quad \textit{for all } a \in \mathbb{Z}[\zeta_n].$$

We state below two other notable properties of the Artin symbol.

**Lemma 2.1.22.** *Given an abelian extension of number fields $\mathbf{K} \subset \mathbf{F} \subset \mathbf{L}$ (i.e. $\mathbf{L}/\mathbf{K}$ is abelian) and a prime ideal $\mathfrak{p}$ in $\mathcal{O}_{\mathbf{K}}$,*

$$\left(\frac{\mathbf{L}/\mathbf{K}}{\mathfrak{p}}\right)\bigg|_{\mathbf{F}} = \left(\frac{\mathbf{F}/\mathbf{K}}{\mathfrak{p}}\right).$$

*Further, suppose that $\mathfrak{p}_0$ is a prime ideal above $\mathfrak{p}$ in $\mathcal{O}_{\mathbf{F}}$, then*

$$\left(\frac{\mathbf{L}/\mathbf{K}}{\mathfrak{p}}\right)^{f(\mathfrak{p}_0/\mathfrak{p})} = \left(\frac{\mathbf{L}/\mathbf{F}}{\mathfrak{p}_0}\right)$$

*where $f(\mathfrak{p}_0/\mathfrak{p})$ is the residual degree of the ideal $\mathfrak{p}_0$ with respect to the extension $\mathbf{F}$ over $\mathbf{L}$.*

*Proof.* Let $\mathfrak{P}$ be a prime ideal above $\mathfrak{p}$ in $\mathcal{O}_{\mathbf{L}}$ and $\mathfrak{P}_0 = \mathfrak{P} \bigcap \mathbf{F}$ and let $\sigma = \left(\frac{\mathbf{L}/\mathbf{K}}{\mathfrak{p}}\right)$. For any $a \in \mathcal{O}_{\mathbf{F}}$, we have, by the definition of the Artin symbol,

$$\sigma(a) - a^{\mathfrak{N}(\mathfrak{p})} \in \mathfrak{P}.$$

But this implies that

$$\sigma|_{\mathbf{F}}\,(a) - a^{\mathfrak{N}(\mathfrak{p})} \in \mathfrak{P}_0,$$

thereby proving the first assertion of our lemma. For the second assertion, let

$\sigma = \left(\frac{\mathbf{L}/\mathbf{K}}{\mathfrak{p}}\right)$, $\sigma_0 = \left(\frac{\mathbf{L}/\mathbf{F}}{\mathfrak{p}_0}\right)$ and $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_{\mathbf{L}}$ above $\mathfrak{p}$ and $\mathfrak{p}_0$. By the definition of Artin symbol, we now have for all $a \in \mathcal{O}_{\mathbf{L}}$,

$$\sigma(a) \equiv a^{\mathfrak{N}(\mathfrak{p})} \bmod \mathfrak{P} \qquad \text{and} \qquad \sigma_0(a) \equiv a^{\mathfrak{N}(\mathfrak{p}_0)} \bmod \mathfrak{P}.$$

We now obtain the second assertion from the fact that $\mathfrak{N}(\mathfrak{p})^{f(\mathfrak{p}_0/\mathfrak{p})} = \mathfrak{N}(\mathfrak{p}_0)$. □

Finally we state the result that motivates this subsection.

**Lemma 2.1.23.** *Given an extension of abelian number fields* $\mathbf{L}/\mathbf{K}$ *and a prime ideal* $\mathfrak{p}$ *in* $\mathcal{O}_{\mathbf{K}}$. *The prime ideal* $\mathfrak{p}$ *splits completely in* $\mathbf{L}$ *if and only if the Artin symbol* $\left(\frac{\mathbf{L}/\mathbf{K}}{\mathfrak{p}}\right)$ *is trivial in the Galois group.*

**Example 2.1.24.** *Using Lemma 2.1.23, it is easy to see that a prime* $p\mathbb{Z} \subset \mathbb{Z}$ *splits in* $\mathbb{Q}(\zeta_n)$ *if and only if* $|p| \equiv 1 \bmod n$.

With the above information on ramified and split primes, we will see now that class field theory allows us to characterise all abelian extensions of a number field $\mathbf{K}$.

### 2.1.4 Artin's map and reciprocity law

Having defined the Artin symbol, we can now look at the map that maps ideals from certain subgroups of the group of non-zero fractional ideals of $\mathbf{K}$ to the Galois groups of abelian extensions of $\mathbf{K}$.

**Definition 2.1.25.** *Given an abelian extension* $\mathbf{L}/\mathbf{K}$ *of number fields and a modulus* $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ *of* $\mathbf{K}$. *Suppose that every prime ideal of* $\mathcal{O}_{\mathbf{K}}$ *and real place of* $\mathbf{K}$ *which ramifies in* $\mathbf{L}$ *divides* $\mathfrak{m}$. *Then, we can define a map from* $I_{\mathfrak{m}}^{\mathbf{K}}$ *to* $Gal(\mathbf{L}/\mathbf{K})$ *in the* *following manner :*

$$\begin{array}{rcl} I_{\mathfrak{m}}^{\mathbf{K}} & \to & Gal(\mathbf{L}/\mathbf{K}) \\ \prod\limits_{\substack{\mathfrak{p}\nmid\mathfrak{m}_0 \\ \mathfrak{p} \text{ prime ideal of } \mathcal{O}_{\mathbf{K}}}} \mathfrak{p}^{n_{\mathfrak{p}}} & \to & \prod\limits_{\substack{\mathfrak{p}\nmid\mathfrak{m}_0 \\ \mathfrak{p} \text{ prime ideal of } \mathcal{O}_{\mathbf{K}}}} \left(\frac{\mathbf{L}/\mathbf{K}}{\mathfrak{p}}\right)^{n_{\mathfrak{p}}}. \end{array}$$

*Here $n_{\mathfrak{p}}$ is non-zero only for finitely many prime ideals in the product. This is known as the Artin map with respect to the modulus $\mathfrak{m}$ for the extension $\mathbf{L}/\mathbf{K}$. It is denoted by $\psi_{\mathfrak{m}}^{\mathbf{L}/\mathbf{K}}$.*

We would now like to prove that this map is in fact surjective. In order to do so, we require few definitions and deep theorems of class field theory. Let us begin with the definition of natural density of a set of primes.

**Definition 2.1.26.** *Let $S$ be a set of non-zero prime ideals of a number field $\mathbf{K}$. Then the limit*

$$d(S) = \lim_{x\to\infty} \frac{\{\mathfrak{p} \in S : \mathfrak{N}(\mathfrak{p}) \leq x\}}{\{\mathfrak{p} : \mathfrak{N}(\mathfrak{p}) \leq x\}},$$

*provided it exists, is called the natural density of $S$.*

A special case of the Chebotarev density theorem states the following.

**Theorem 2.1.27** (Chebotarev density theorem)**.** *Let $\mathbf{L}/\mathbf{K}$ be an abelian extension of number fields with Galois group $G$. For each $\sigma$ in $G$, let*

$$S(\sigma) := \left\{\mathfrak{p} \subseteq \mathcal{O}_{\mathbf{K}} \ : \ \mathfrak{p} \text{ prime ideal, unramified and } \left(\frac{\mathbf{L}/\mathbf{K}}{\mathfrak{p}}\right) = \sigma\right\},$$

*then*

$$d(S(\sigma)) = \frac{1}{|G|}.$$

As a corollary to the Chebotarev density theorem, one can show the following.

**Corollary 2.1.28.** *Consider an extension of abelian number fields* $\mathbf{L}/\mathbf{K}$*. Let* $e$ *be the trivial element in the Galois group of* $\mathbf{L}/\mathbf{K}$*. If* $d(S(e)) = 1$*, then* $\mathbf{L} = \mathbf{K}$*.*

We are now in a position to prove the surjectivity of the Artin map.

**Theorem 2.1.29.** *Given an abelian extension* $\mathbf{L}/\mathbf{K}$ *of number fields and a modulus* $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ *of* $\mathbf{K}$*. Suppose that every prime ideal of* $\mathcal{O}_{\mathbf{K}}$ *and real place of* $\mathbf{K}$ *which ramifies in* $\mathbf{L}$ *divides* $\mathfrak{m}$*, then* $\psi_{\mathfrak{m}}^{\mathbf{L}/\mathbf{K}}$ *is surjective.*

*Proof.* Let $H$ be the image of $\psi_{\mathfrak{m}}^{\mathbf{L}/\mathbf{K}}$. Let $\mathbf{F} = \mathbf{L}^H$, that is the subfield of $\mathbf{L}$ fixed by $H$. Therefore for each $\mathfrak{p}$ in $I_{\mathfrak{m}}^{\mathbf{K}}$, we have that $\psi_{\mathfrak{m}}^{\mathbf{L}/\mathbf{K}}(\mathfrak{p})$ acts trivially on $\mathbf{F}$. This implies that all but finitely many prime ideals of $\mathbf{K}$ split in $\mathbf{F}$. Thus the natural density of the set of all prime ideals of $\mathbf{K}$ which split in $\mathbf{F}$ is one. Therefore $\mathbf{F} = \mathbf{K}$ and the Artin map, $\psi_{\mathfrak{m}}^{\mathbf{L}/\mathbf{K}}$, is surjective. □

Another useful corollary to Theorem 2.1.27 is the following.

**Corollary 2.1.30.** *Let* $\mathbf{L}$ *and* $\mathbf{M}$ *be two finite abelian extensions of* $\mathbf{K}$*. If the set of prime ideals of* $\mathcal{O}_{\mathbf{K}}$ *which split in* $\mathbf{L}$ *were contained in the set of prime ideals which split in* $\mathbf{M}$*, then* $\mathbf{M} \subseteq \mathbf{L}$*.*

*Proof.* A prime ideal splits in $\mathbf{L}$ and $\mathbf{M}$ if and only if it splits in $\mathbf{LM}$. Therefore

$$\frac{1}{[\mathbf{LM} : \mathbf{K}]} \geq \frac{1}{[\mathbf{L} : \mathbf{K}]}.$$

This implies that $\mathbf{M} \subseteq \mathbf{L}$. □

We can now shift our attention to the kernel of the map from the subgroup of fractional ideals to the Galois group. This will lead us to what is known as Artin's reciprocity theorem.

**Definition 2.1.31.** *A subgroup* $H$ *of* $I_{\mathfrak{m}}^{\mathbf{K}}$ *which contains* $P_{\mathfrak{m}}^{\mathbf{K}}$ *is called a congruence subgroup.*

We can now state Artin's reciprocity law.

**Theorem 2.1.32** (Artin's reciprocity law)**.** *Let* $\mathbf{L}/\mathbf{K}$ *be an abelian extension of number fields. Then there exists a modulus* $\mathfrak{m}$ *such that*

1. *all the prime ideals of* $\mathcal{O}_{\mathbf{K}}$ *and real places of* $\mathbf{K}$ *which ramify in* $\mathbf{L}$ *divide* $\mathfrak{m}$*, and*

2. *the kernel of the Artin map,* $\psi_{\mathfrak{m}}^{\mathbf{L}/\mathbf{K}}$*, is a congruence subgroup of modulus* $\mathfrak{m}$*.*

The "smallest" such modulus (in terms of divisibility) is called the conductor of the extension $\mathbf{L}/\mathbf{K}$. Another important theorem of class field theory is the existence of the ray class field of modulus $\mathfrak{m}$.

**Theorem 2.1.33.** *Given a number field* $\mathbf{K}$ *and a modulus* $\mathfrak{m}$*, there exists a unique abelian extension* $\mathbf{L}$ *of* $\mathbf{K}$ *such that*

1. *all the prime ideals of* $\mathcal{O}_{\mathbf{K}}$ *and the real places of* $\mathbf{K}$ *which ramify in* $\mathbf{L}$ *divide* $\mathfrak{m}$*, and*

2. *the kernel of* $\psi_{\mathfrak{m}}^{\mathbf{L}/\mathbf{K}} = P_{\mathfrak{m}}^{\mathbf{K}}$*.*

*This is known as the ray class field of* $\mathbf{K}$ *corresponding to the modulus* $\mathfrak{m}$*. This field will be denoted by* $\mathbf{K}(\mathfrak{m})$*.*

For $\mathbf{K} = \mathbb{Q}$ and modulus $\mathfrak{m} = (m)\mathfrak{m}_\infty$, where $m \in \mathbb{Z} \setminus \{0\}$ and $\mathfrak{m}_\infty$ contains the unique real place of $\mathbb{Q}$, the ray class field is immediately seen to be $\mathbb{Q}(\zeta_{|m|})$ by Example 2.1.24 and Corollary 2.1.28. And for $\mathfrak{m} = (m)$, the split prime ideals correspond to the rational primes $\mathrm{p} \in \mathbb{N}$ which are either 1 mod $m$ or $-1$ mod $m$, which means that the ray class field is $\mathbb{Q}\left(\zeta_{|m|} + \frac{1}{\zeta_{|m|}}\right)$. By the above discussion and an application of Theorem 2.1.32, it is clear that any abelian extension of $\mathbb{Q}$ lies in a cyclotomic field. This is known as the *Kronecker-Weber Theorem.* Further the smallest $m \in \mathbb{N}$ for which $\mathbf{K} \subseteq \mathbb{Q}(\zeta_m)$ is called the conductor of $\mathbf{K}$. One can check that this will coincide with the notion of the conductor ideal of $\mathbf{K}/\mathbb{Q}$, up to the real place, as defined above. Coming now to the last subsection on the algebraic part, we would like to talk about a special kind of ray class field, namely the Hilbert class field.

### 2.1.5 Hilbert class field

In this section we will deal with a very special kind of ray class field known as the Hilbert class field. This will help us study the usual class group of a number field $\mathbf{K}$.

**Definition 2.1.34.** *The ray class field of* $\mathbf{K}$ *corresponding to* $\mathfrak{m} = \mathcal{O}_{\mathbf{K}}$ *is called the Hilbert class field of* $\mathbf{K}$*, denoted by* $H(\mathbf{K})$*.*

Note that if $\mathcal{O}_{\mathbf{K}}$ were a principal ideal domain, then $H(\mathbf{K}) = \mathbf{K}$. Using the definition of the Hilbert class field one can show the following.

**Theorem 2.1.35.** *The maximal unramified abelian extension of* $\mathbf{K}$ *is the Hilbert class field of* $\mathbf{K}$*.*

*Proof.* Since the modulus is trivial, the Hilbert class field is unramified. Further given any abelian unramified extension, it will be contained in $\mathbf{K}(\mathcal{O}_{\mathbf{K}})$ by Theorem 2.1.32 and Corollary 2.1.30. This implies that it must be contained in the Hilbert class field. □

An immediate corollary is the following.

**Corollary 2.1.36.** *The set of prime ideals which split in* $H(\mathbf{K})/\mathbf{K}$ *is exactly the set of principal ideals of* $\mathcal{O}_{\mathbf{K}}$*.*

We have already seen trivial examples of Hilbert class fields. Now let us look at one which requires some ramification theory to show that it is the Hilbert class field.

**Example 2.1.37.** *For* $\mathbf{K} = \mathbb{Q}(\sqrt{65})$, *the Hilbert class field is easy to compute using the theory of ramification. The class number of* $\mathbf{K}$ *is known to be* $2$. *Consider the following diagram :*

$$\begin{tikzcd}
 & \mathbb{Q}(\sqrt{13}, \sqrt{5}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{13}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{5}) \arrow[d, dash] & \mathbf{K} \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

*By Theorem 2.1.19, the only prime ideals that can ramify in* $\mathbb{Q}(\sqrt{13}, \sqrt{5})$ *are* $13\mathbb{Z}$ *and* $5\mathbb{Z}$. *However* $13\mathbb{Z}$ *does not ramify in* $\mathbb{Q}(\sqrt{5})$. *Therefore its ramification index in* $\mathbb{Q}(\sqrt{13}, \sqrt{5})$ *is* $2$. *The same argument holds for* $5\mathbb{Z}$. *This implies that* $\mathbb{Q}(\sqrt{13}, \sqrt{5})$ *over* $\mathbf{K}$ *is unramified. It is maximal simply because the class number of* $\mathbf{K}$ *is* $2$. *Therefore, the Hilbert class field of* $\mathbb{Q}(\sqrt{65})$ *is* $\mathbb{Q}(\sqrt{13}, \sqrt{5})$.

## 2.2 Sieve theory

In this section, we will look at some preliminaries pertaining to sieve theory. This will be divided into three sections in increasing order of complexity. The first section will talk about a modified version of the Brun's sieve (Section 2.2.1). The second about the lower bound linear sieve (Section 2.2.2) and the last about a combination of the lower and upper bound linear sieves (Section 2.2.3).

### 2.2.1 Modified Brun's sieve

The main theorem we state in this subsection is a modified version of Brun's sieve as stated in [1]. We begin with a few definitions. Let $\Sigma$ be a finite set of positive rational primes. Let

$$Pr_\Sigma(z) := \prod_{\substack{p<z \\ p\notin\Sigma}} p.$$

When $\Sigma = \emptyset$, the empty set, we denote the product by $Pr(z)$. Consider the linear forms $L_i(n) \ = \ a_i n + b_i$ where $a_i \neq 0$ and $b_i$ belong to $\mathbb{N}$ for $1 \leq i \leq k$. We further suppose that $(a_i, b_i) = 1$ for all $i$ and that $a_i b_j - a_j b_i \neq 0$ for $1 \leq i < j \leq k$. Let

$$\Omega^{(*)}(x,z) := \{n \leq x : (L_1(n)\cdots L_{k-1}(n),\ Pr_\Sigma(z)) = 1,\ L_k(n) \text{ prime}\}.$$

Here $(t_1, t_2)$ denotes the greatest common divisor of the numbers $t_1$ and $t_2$. Further we assume that all the prime divisors of

$$(2k)! \prod_{i=1}^{k} a_i \prod_{1\leq i<j\leq k} (a_i b_j - a_j b_i) \tag{2.2.1}$$

belong to $\Sigma$. We now give the statement of the sieve.

**Theorem 2.2.1** (Bilu, Deshouillers, Gun and Luca [1]). *Under the above notation and assumption* (2.2.1) , *we have for* $2 \leq z \leq x$

$$|\Omega^{(*)}(x,z)| = \frac{Li(|a_k|x)}{\varphi(|a_k|)} W_{k-1}^{(*)}(z)(1 + O(E^{(*)}(x,z)))$$

*where* $\varphi$ *denotes the Euler totient function,*

$$E^{(*)}(x,z) \quad = \quad exp(-(u/3)(\log u - \log\log u - \log(k-1) - 3)) + \frac{1}{\log z},$$

$$u = \frac{\log x}{\log z} \qquad \textit{and} \qquad W_\ell^{(*)}(z) = \prod_{p|Pr_\Sigma(z)} \left(1 - \frac{\ell}{p-1}\right).$$

*As a convention, we assume that the empty product is* 1.

This sieve will be applied in Chapter 3 to prove Theorem 1.5.1. The next section will deal with the more complicated linear lower bound sieve.

### 2.2.2 Linear lower bound sieve

We will now provide the details of the linear lower bound sieve which will be used in the proofs of the theorems in Chapter 4. To give the precise statement of this sieve we again start with some notations and definitions. Let $\mathcal{P}$ be a subset of the set of positive rational primes, $z$ a real number and

$$\mathcal{P}(z) \ := \ \prod_{\substack{p\in\mathcal{P},\\ p\leq z}} p. \tag{2.2.2}$$

Given a finite subset of non-negative integers $\mathcal{A}$, let $\mathcal{A}_d := \{a \in \mathcal{A} \ : \ d|a\}$, where $d$ is a square free natural number with all it prime divisors in $\mathcal{P}$. Suppose that $\omega$ is a multiplicative function such that

$$|\mathcal{A}_d| \ = \ \frac{\omega(d)}{d}|\mathcal{A}| \ + \ r_d, \tag{2.2.3}$$

for some $r_d$. Further, set

$$V(z) := \prod_{\substack{p<z,\\ p\in\mathcal{P}}} \left(1 - \frac{\omega(p)}{p}\right) \tag{2.2.4}$$

and

$$S(\mathcal{A}, \mathcal{P}, z) := \{a \in \mathcal{A} \ : \ (a, \mathcal{P}(z)) = 1\}, \tag{2.2.5}$$

where $(a, \mathcal{P}(z))$ denotes the gcd of $a$ and $\mathcal{P}(z)$. We now introduce the notion of a well factorable function as defined by Iwaniec [24] (see also page 255 of [10]).

**Definition 2.2.2.** *Let $D \geq 1$ be a real number and $\lambda(q)$ be an arithmetic function with support $[1, D]$. We say that $\lambda$ is a well factorable function of level $D$ if for any real numbers $M, N \geq 1$ with $MN = D$, one can write*

$$\lambda(q) := \sum_{\substack{mn=q,\\ m\leq M,\\ n\leq N}} \alpha(m)\beta(n), \qquad \text{where} \quad 1 \leq q \leq MN$$

*for some arithmetic functions $\alpha$ and $\beta$ which depend on $M, N$ and $|\alpha(m)|, |\beta(n)| \leq 1$.*

In this set-up, one has the following lower bound sieve.

**Theorem 2.2.3** (Friedlander and Iwaniec (see page 256 of [10], see also Iwaniec [24]))**.** *Let $D \geq 1$, $s \geq 2$ be real numbers and $z = D^{1/s}$. Also let $\mathcal{A}$ be a subset of non-negative integers satisfying*

$$\prod_{\substack{u\leq p<z,\\ p\in\mathcal{P}}} \left(1 - \frac{\omega(p)}{p}\right)^{-1} \leq T \left(\frac{\log z}{\log u}\right),$$

*where $u \geq 2$ is an integer and $T > 0$ is an absolute constant. Then for sufficiently large $D$ and for any real number $\varepsilon > 0$, we have*

$$S(\mathcal{A}, \mathcal{P}, z) \;\geq\; XV(z)\{g(s) - \varepsilon\} + \sum_{d|\mathcal{P}(z)} \lambda(d)\, r_d.$$

*Here $|\mathcal{A}| \sim X$, $\mathcal{P}(z)$ and $V(z)$ are as in (2.2.2) and (2.2.4), respectively. Finally, $\lambda$ is some well factorable function of level $D$ and $g$ is a continuous function on $[2, \infty)$ satisfying*

$$g(s) \;=\; 2e^{\gamma} \log(s-1)/s,$$

*for $s \in [2, 4]$. Also $\gamma$ is the Euler and Mascheroni constant.*

One will notice that to use the above sieve, we need a way to estimate the sum of $r_d$ and show that it is dominated by the main term. In order to do this, one may use the following theorem, as we shall see in Chapter 4.

**Theorem 2.2.4** (Bombieri, Friedlander and Iwaniec (see [2], see also [9, 20]))**.** *Let $a, k$ be positive natural numbers with $(a, k) = 1$. For any positive natural number $q$ with $(q, k) = 1$, let*

$$u_q \equiv a \bmod k \qquad \text{and} \qquad u_q \equiv 1 \bmod q.$$

*Fix a positive integer $A > 0$ and a real number $\theta < 4/7$. Then, for every well factorable function $\lambda$ of level $x^\theta$, one has*

$$\sum_{\substack{q \leq x^\theta \\ (q,k)=1}} \lambda(q) \left( \pi(x, qk, u_q) - \frac{Li(x)}{\varphi(qk)} \right) \ll \frac{x}{\log^A x}.$$

*The constant in $\ll$ depends on $a, A, k$ and $\theta$.*

As the reader will observe during the course of the proof, the exponent 4/7, also known as the level of distribution, will play a major role in determining the lower bound on the unit rank. So it is natural to expect that better exponents will yield better results. This line of thought led us to examine the consequences of the Elliott and Halberstam conjecture on this problem. In order to do this, we use an older version of the linear sieve, developed before the emergence of the theory of well factorable weights.

**Theorem 2.2.5** (Halberstam and Richert (see page 236 of [17]))**.** *Let $\mathcal{P}$ be a subset of the set of positive rational primes, $z$ be a real number and $\mathcal{P}(z), \omega, r_d, V(z)$ and $S(\mathcal{A}, \mathcal{P}, z)$ be as in (2.2.2), (2.2.3), (2.2.4) and (2.2.5). Suppose that*

1. *there exists a constant $A_1 \geq 1$ such that*

$$0 \;\leq\; \frac{\omega(p)}{p} \;\leq\; 1 - \frac{1}{A_1} \tag{2.2.6}$$

   *for all $p \in \mathcal{P}$;*

2. *there exist constants $L$ and $A_2$, independent of $z$ and integer $g_1$ with $2 \leq g_1 \leq z$ such that*

$$-L \leq \sum_{\substack{g_1 \leq p \leq z \\ p \in \mathcal{P}}} \frac{\omega(p)\log p}{p} - \log\left(\frac{z}{g_1}\right) \leq A_2 \ ; \tag{2.2.7}$$

3. *there exists a real number $\alpha$ with $0 < \alpha \leq 1$ such that*

$$\sum_{\substack{p|d \implies p \in \mathcal{P}, \\ d < \frac{X^{\alpha}}{\log^{F} X}}} \mu^2(q)\ 3^{\nu(d)} |\ r_d| \;\leq\; \frac{G_1 X}{\log^2 X} \tag{2.2.8}$$

   *for some positive constants $F$ and $G_1$. Here $\mu$ is the Möbius function and $\nu(d)$ denotes the number of distinct prime divisors of $d$.*

*Then for $X \geq z$,*

$$S(\mathcal{A}, \mathcal{P}, z) \geq XV(z)\left\{g\left(\alpha\frac{\log X}{\log z}\right) - \frac{B}{\log^{1/14} X}\right\},$$

*where $B$ is an absolute constant, $g$ and $X$ are as in Theorem 2.2.3.*

This time, since the terms $r_d$ appear with an absolute value, we can estimate the sum in Equation (2.2.8) if we assume the following conjecture.

**Conjecture 2.2.6** (Elliott and Halberstam conjecture [8])**.** *Let $a, q$ be natural numbers, $\pi(y, q, a) := \{p \leq y \ : \ p$ prime in $\mathbb{N}$, $p \equiv a \bmod q\}$. For every real number*

*$\theta < 1$ and for every positive integer $e > 0$, one has*

$$\sum_{q \leq x^\theta} \max_{y \leq x} \max_{(a,q)=1} \left| \pi(y,q,a) - \frac{Li(y)}{\varphi(q)} \right| \ll \frac{x}{\log^e x}$$

*for all real numbers $x > 2$.*

With these we conclude the subsection on the linear lower bound sieve which will be applied to deduce the results in Chapter 4. We now move on to the next section where we quote an application of a combination of the linear lower and upper bound sieve.

### 2.2.3 Application of lower and upper bound sieve

In this section, instead of speaking about the lower bound linear sieve and its counter part, the upper bound linear sieve, in detail, we will directly look at a useful lemma which was derived by Heath-Brown using these sieves. This lemma will be a major tool used in the proofs of Chapter 5. The lemma is as follows.

**Lemma 2.2.7** (Heath-Brown [20], [29]). *Suppose that $u$ and $v$ are natural numbers with the following properties*

$$(u,v) = 1, \quad v \equiv 0 \bmod 16 \quad \textit{and} \quad \left(\frac{u-1}{2},\ v\right) \ = \ 1.$$

*Then there exist $a, b \in (\frac{1}{4}, \frac{1}{2})$ with $a < b$ such that for any $\epsilon > 0$, the cardinality of the set*

$$P(x) \ := \ \{p \equiv u \bmod v \ : \ p \in (x^{1-\epsilon}, x) \textit{ such that } \frac{p-1}{2} \textit{ is either prime or}$$
$$\textit{is a product of primes } q_1 q_2 \textit{ with } x^a \leq q_1 \leq x^b\}$$

*is $\gg \frac{x}{\log^2 x}$.*

With this theorem we conclude this subsection and the section on the sieve-theoretic preliminaries of this chapter.

## 2.3 Arithmetic preliminaries

Finally we come to the last section of this chapter on preliminaries. Here we state certain arithmetic prerequisites which we will be required for all the chapters that follow. Throughout this section, we fix a number field $\mathbf{K}$. In Chapter 1 we saw Motzkin's criterion and later partially generalised the notion of Euclidean domains. We did not however speak about generalisations of Motzkin's criterion to this new setup. This was done in a paper by Graves in [13]. We begin this section with this generalisation.

**Definition 2.3.1.** *For a non-zero integral ideal $\mathfrak{a}$ of $\mathbf{K}$, let us define*

$$\begin{aligned} B_{0,\mathfrak{a}} &:= \{\mathcal{O}_{\mathbf{K}}\} \quad \textit{and for } i \geq 1, \\ B_{i,\mathfrak{a}} &:= \{\mathfrak{p} \ : \ \mathfrak{p} \textit{ prime }, \forall x \in \mathfrak{p}^{-1}\mathfrak{a} \setminus \mathfrak{a}, \ \exists \ y \in \mathfrak{a} \textit{ such that } \mathfrak{a}^{-1}\mathfrak{p}(x-y) \in B_{i-1,\mathfrak{a}}\} \\ &\quad \cup B_{i-1,\mathfrak{a}} \end{aligned}$$

Note that $B_{i,\mathfrak{a}} \setminus B_{i-1,\mathfrak{a}} \subset [\mathfrak{a}^i]$, the class of $\mathfrak{a}^i$.

In this set-up, Graves [13] proved the following theorem.

**Theorem 2.3.2.** *(Graves [13]) If $\mathfrak{a}$ is a non-zero integral ideal of $\mathbf{K}$, then*

$$B_{1,\mathfrak{a}} = \{\mathfrak{p} \ : \ \mathfrak{p} \textit{ is prime}, \ [\mathfrak{p}] = [\mathfrak{a}], \ \mathcal{O}_{\mathbf{K}}^{\times} \to (\mathcal{O}_{\mathbf{K}}/\mathfrak{p})^{\times} \textit{ is surjective } \} \cup \{\mathcal{O}_{\mathbf{K}}\}.$$

*Further let $B_{\mathfrak{a}} = \bigcup_i B_{i,\mathfrak{a}}$. If $B_{\mathfrak{a}}$ contains all prime ideals of $\mathcal{O}_{\mathbf{K}}$, then $\mathfrak{a}$ is a Euclidean ideal.*

The first part of the above theorem will prove to be a very useful observation and the second part of the above theorem can be thought of as a generalization of a result of Clark and Murty [4] or as a variant of Weinberger's version of Motzkin's theorem. Now let

$$B_{1,\mathfrak{a}}(x) := \ \{\mathfrak{p} \in B_{1,\mathfrak{a}} \ : \ \mathfrak{N}(\mathfrak{p}) \leq x\} \cup \{\mathcal{O}_{\mathbf{K}}\}.$$

Graves [13] showed that to prove Theorem 2.3.2, it is sufficient to prove that that the cardinality of $B_{1,\mathfrak{a}}(x)$, denoted by $|B_{1,\mathfrak{a}}(x)|$, is large. More precisely,

**Theorem 2.3.3.** *(Graves [13]) Suppose* $\mathbf{K}$ *is a number field with unit rank at least one. Further suppose that* $\mathcal{O}_{\mathbf{K}}$ *has cyclic class group and that* $\mathfrak{a}$ *is an integral ideal of* $\mathcal{O}_{\mathbf{K}}$ *such that* $[\mathfrak{a}]$ *generates the class group. If*

$$|B_{1,\mathfrak{a}}(x)| \gg x/\log^2 x,$$

*then* $\mathfrak{a}$ *is a Euclidean ideal.*

The above theorem is a generalisation of a result of Harper [18], which appeared in Section 1.4. In most of the major proofs in this thesis, we will try to show that the set $B_{1,\mathfrak{a}}$ is large in the sense indicated by Theorem 2.3.3. In order to do this we will consider the complement set and show that it is negligible by using the following result of Gupta and Murty (as given in the paper of Harper and Murty [19]).

**Lemma 2.3.4** (Gupta and Murty [16]). *Let* $K$ *be a number field and* $r$ *be the unit rank of* $\mathcal{O}_K$. *For* $\mathfrak{p}$, *a prime ideal of* $\mathcal{O}_{\mathbf{K}}$, *if* $l_{\mathfrak{p}}$ *denotes the cardinality of the set*

$$\{\alpha \bmod \mathfrak{p} : \alpha \in \mathcal{O}_K^{\times}\},$$

*then*

$$|\{\mathfrak{p} \ : \ \mathfrak{p} \textit{ prime ideal of } \mathcal{O}_{\mathbf{K}}, \ l_{\mathfrak{p}} \leq y\}| \ll y^{1+\frac{1}{r}}.$$

*Here* $|S|$ *is used to denote the cardinality of a set* $S$.

In Chapter 5, we will observe that the techniques of Graves and Murty ([14]) will no longer be able to help us. In that chapter we will resort to the techniques of Heath-Brown [20] and Narkiewicz [31]. In this case one of the essential ingredients is the following lemma by Narkiewicz [31] which revolves around primitive roots.

**Lemma 2.3.5** (Narkiewicz [31]). *Let $a_1, a_2$ and $a_3$ be multiplicatively independent elements of $\mathbf{K}^\times$, $T$ be a set of prime ideals of degree 1 in $\mathcal{O}_\mathbf{K}$ and $\mathfrak{N}(\mathfrak{p})$ be as in Definition 2.1.7 . Suppose that $T$ has the following properties;*

1. *there exists a constant $c > 0$ and an unbounded increasing sequence $\{x_n\}_{n\in\mathbb{N}}$ such that*

$$|T(x_n) := \{\mathfrak{p} \in T \ : \ \mathfrak{N}(\mathfrak{p}) \leq x_n\}| \ > \ cx_n/\log^2 x_n \textit{ for all } n.$$

2. *there exist $\alpha, \beta \in (1/4, 1/2)$ with $\alpha < \beta$ such that if $\mathfrak{p} \in T$ and $p := \mathfrak{N}(\mathfrak{p})$, then either $p - 1 = 2q$ or $p - 1 = 2q_1q_2$ where $q$, $q_1$ and $q_2$ are primes and $p^\alpha < q_1 < p^\beta$.*

3. *the numbers $a_1, a_2$ and $a_3$ are quadratic non-residues with respect to every prime in $T$.*

*Then for any $0 < \epsilon < c$, there exists a subsequence $\{y_m\}_{m\in\mathbb{N}}$ of $\{x_n\}_{n\in\mathbb{N}}$ such that one of the $a_i$'s is a primitive root for at least $(c - \epsilon)y_m/\log^2 y_m$ elements of $T(y_m)$.*

In order to use Lemma 2.3.5 along with the ideas of Theorem 2.3.3 we will need to deduce a sequential variant of Lemma 2.3.3 in the later chapters. To do that we need to introduce a few more definitions and results from [13].

**Definition 2.3.6.** *Suppose that $\mathfrak{a}$ is a non-zero integral ideal of $\mathbf{K}$ such that $[\mathfrak{a}]$ generates the class group of $\mathbf{K}$. Let $A \subset E$ be a finite set of ideals in the same equivalence class of the class group. If $\mathfrak{p}$ is a prime ideal such that $[\mathfrak{p}] = [I\mathfrak{a}]$ for any*

*$I \in A$ and if $x \in \mathfrak{p}^{-1}\mathfrak{a}$, we define*

(2.3.1)

$$Z_A(x, \mathfrak{p}, \mathfrak{a}) := \begin{cases} |\{H \in A : \textit{ there exists some } y \ \in \mathfrak{a} \textit{ such that } (x-y)\mathfrak{p}\mathfrak{a}^{-1} = H\}| \\ \qquad \textit{if } x \notin \mathfrak{a}; \\ l_{\mathfrak{p}} \times |\{H \in A : \textit{ there exists some } y \ \in \mathfrak{a} \textit{ such that } (x-y)\mathfrak{p}\mathfrak{a}^{-1} = H\}| \\ \qquad \textit{if } x \in \mathfrak{a}. \end{cases}$$

*where $l_{\mathfrak{p}}$ is as defined in Lemma 2.3.4*

Another theorem which will be handy in proving the sequential variant of Lemma 2.3.3 is the following variant of Dirichlet's theorem on primes in arithmetic progressions.

**Theorem 2.3.7** (Graves [13])**.** *Suppose that $\mathfrak{a}$ is a fractional ideal of $\mathbf{K}$ and $\mathfrak{b}$ is a non-zero integral ideal of $\mathbf{K}$ with $\mathfrak{b} \neq \mathcal{O}_{\mathbf{K}}$. If $x$ is an element of $\mathfrak{a}\mathfrak{b}^{-1}$ and $x + \mathfrak{a} = \mathfrak{a}\mathfrak{b}^{-1}$, then there is a set of primes $\mathfrak{p}$ with positive density such that*

$$\mathfrak{p} = \mathfrak{b}(x-y)\mathfrak{a}^{-1},$$

*for some $y$ in $\mathfrak{a}$.*

Further, we will require the following isomorphism to help us with some counting arguments in the proof of the variant of Theorem 2.3.3

**Lemma 2.3.8** (Graves [13])**.** *For a number field $\mathbf{K}$, let us assume that $\mathcal{O}_{\mathbf{K}}$ has cyclic class group. Further $\mathfrak{p}, \mathfrak{a}$ are ideals in $\mathbf{K}$ with $\mathfrak{p}$ prime such that $[\mathfrak{p}] = [\mathfrak{a}^2]$ and $[\mathfrak{a}]$ generates the class group of $\mathbf{K}$. Also suppose that $x_{\mathfrak{p}}$ is a generator of $\mathfrak{p}\mathfrak{a}^{(h_{\mathcal{O}_{\mathbf{K}}}-2)}$, where $h_{\mathcal{O}_{\mathbf{K}}}$ is the class number of $\mathcal{O}_{\mathbf{K}}$. Then the map $\phi \ : \ \mathfrak{p}^{-1}\mathfrak{a}/\mathfrak{a} \to \mathfrak{a}^{h_{\mathcal{O}_{\mathbf{K}}}-1}/\mathfrak{p}\mathfrak{a}^{h_{\mathcal{O}_{\mathbf{K}}}-1}$ defined by $\alpha + \mathfrak{a} \mapsto \alpha x_{\mathfrak{p}} + \mathfrak{p}\mathfrak{a}^{h_{\mathcal{O}_{\mathbf{K}}}-1}$ is an isomorphism.*

Finally we list some consequences of the large sieve inequality as proved by

Graves in [13]. Note that all these theorems are essentially tools used by Graves to prove Theorem 2.3.3. We will use the same to prove a stronger form of Theorem 2.3.3.

**Definition 2.3.9.** *Let* $\mathbf{K}$ *be a number field with cyclic class group and* $\mathfrak{a}$ *be a non-zero integral ideal of* $\mathbf{K}$ *such that* $[\mathfrak{a}]$ *generates the class group of* $\mathcal{O}_{\mathbf{K}}$. *For some natural number* $n$ *let*

$$A_{\mathfrak{a}} \subset \{I : I \in E \textit{ and } [I] = [\mathfrak{a}^n]\}$$

*be a finite set. Then we define for* $\mathfrak{p} \in [\mathfrak{a}^{n+1}]$

$$\lambda(\mathfrak{p}, \mathfrak{a}, A_{\mathfrak{a}}) := |\{[\alpha] \in \mathfrak{p}^{-1}\mathfrak{a}/\mathfrak{a} \ : \ Z_{A_{\mathfrak{a}}}(\alpha, \mathfrak{p}, \mathfrak{a}) = 0\}|. \tag{2.3.2}$$

Having defined the above we can now state the consequence of the large sieve inequality.

**Lemma 2.3.10** (Graves [13])**.** *Let* $\mathbf{K}$ *be a number field with cyclic class group and* $\mathfrak{a}$ *an integral ideal of* $\mathbf{K}$ *such that* $[\mathfrak{a}]$ *generates the class group of* $\mathcal{O}_{\mathbf{K}}$. *Also let* $A$ *and* $P$ *be finite sets of integral ideals with* $A \subset E \bigcap \{I \ : \ I \in [\mathfrak{a}^n]\}$ *and*

$$P \subset \{\mathfrak{p} : \mathfrak{p} \textit{ is prime }, [\mathfrak{p}] = [\mathfrak{a}^{n+1}]\},$$

*where* $n$ *is a natural number. If* $X = \max_{I \in A} \mathfrak{N}(I)$ *and* $Q = \max_{\mathfrak{p} \in P} \mathfrak{N}(\mathfrak{p})$, *then*

$$\sum_{\mathfrak{p} \in P} \frac{\lambda(\mathfrak{p}, \mathfrak{a}, A)}{\mathfrak{N}(\mathfrak{p})} \ll \frac{Q^2 + X}{|A|},$$

*where the implied constant depends only on* $\mathbf{K}$,$\mathfrak{a}$ *and* $n$. *Once again* $\mathfrak{N}(\mathfrak{p})$ *is as defined in Definition 2.1.7*

This concludes our chapter on the preliminaries required to show the results that will appear in this thesis. In the next chapter we begin with our results.

# Chapter 3

# Lower bound on unit rank

## 3.1 Introduction

Let us first set the central theme of this chapter. We have a Galois number field $\mathbf{K}$ with ring of integers $\mathcal{O}_{\mathbf{K}}$. Standing assumption throughout the chapter is that the class group of $\mathcal{O}_{\mathbf{K}}$ is cyclic and we are given a generator $[\mathfrak{a}]$ of the class group.

Under the extended Riemann hypothesis we know that there exists a Euclidean ideal class in the class group of $\mathcal{O}_{\mathbf{K}}$. Our goal is to prove the existence of such an ideal class unconditionally at least for some special class of fields.

The results stated in Chapter 1 indicate that the existence of a large unit group is amenable to detect a Euclidean ideal class. In order to quantify the previous statement we begin by recalling the following theorem of Graves.

**Theorem 3.1.1** (Graves [13]). *If $\mathfrak{a}$ is a non-zero integral ideal of $\mathcal{O}_{\mathbf{K}}$, then*

$$B_{1,\mathfrak{a}} = \left\{\mathfrak{p} : \mathfrak{p} \textit{ is a prime ideal of } \mathcal{O}_{\mathbf{K}}, [\mathfrak{p}] = [\mathfrak{a}], \mathcal{O}_{\mathbf{K}}^{\times} \to (\mathcal{O}_{\mathbf{K}}/\mathfrak{p})^{\times} \textit{ is surjective}\right\} \bigcup \{\mathcal{O}_{\mathbf{K}}\}.$$

For a definition of $B_{1,\mathfrak{a}}$ see Definition 2.3.1. Let us consider the following set

$B_{1,\mathfrak{a}}(x) := \{\mathfrak{p} \in B_{1,\mathfrak{a}} : \mathfrak{N}(\mathfrak{p}) \leq x\}$. We have already seen by Theorem 2.3.3 that if

$$|B_{1,\mathfrak{a}}(x)| \gg \frac{x}{\log^2 x},$$

then $[\mathfrak{a}]$ is a Euclidean ideal class. Since the above characterization of $B_{1,\mathfrak{a}}$ involves a surjective map from $\mathcal{O}_{\mathbf{K}}^{\times}$ to $(\mathcal{O}_{\mathbf{K}}/\mathfrak{p})^{\times}$, one suspects that as the unit rank of $\mathcal{O}_{\mathbf{K}}$ grows larger, at least in principle, it will be easier to find Euclidean ideal classes (of course assuming that the class group is cyclic).

We note that for a number field $\mathbf{K}$, in order to show that the number of primes $B_{1,\mathfrak{a}}(x)$ is large, it is sufficient to count the rational primes that lie below the prime ideals in $B_{1,\mathfrak{a}}(x)$.

For a non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}_{\mathbf{K}}$, we note that if the set $\{\alpha \bmod \mathfrak{p} : \alpha \in \mathcal{O}_{\mathbf{K}}^{\times}\}$ does not cover all of $(\mathcal{O}_{\mathbf{K}}/\mathfrak{p})^{\times}$, then it is a proper subgroup of $(\mathcal{O}_{\mathbf{K}}/\mathfrak{p})^{\times}$ and we can compute the index of this subgroup. This index, by Lagrange's theorem, divides the cardinality of $(\mathcal{O}_{\mathbf{K}}/\mathfrak{p})^{\times}$. We would like to find this cardinality. To do so, we observe the following. Given a prime ideal $p\mathbb{Z}$ which does not split or ramify in $\mathcal{O}_{\mathbf{K}}$, the norm of a prime above $p\mathbb{Z}$ in $\mathcal{O}_{\mathbf{K}}$ is at least $p^2$. Therefore the contribution of these primes to the cardinality of $B_{1,\mathfrak{a}}(x)$ is at most $\sqrt{x}/\log x$ which is negligible compared to the lower bound we require on the cardinality of $B_{1,\mathfrak{a}}(x)$. Thus, we have now reduced the problem of counting the number of elements in $B_{1,\mathfrak{a}}(x)$ to counting the number of split primes with norm less than $x$ in the class of $[\mathfrak{a}]$ for which $\mathcal{O}_{\mathbf{K}}^{\times}$ surjects onto $(\mathcal{O}_{\mathbf{K}}/\mathfrak{p})^{\times}$.

It will be shown in due course of the proof that with the help of Lemma 2.3.4 one can reduce the problem of finding Euclidean ideal classes to counting rational primes, $p \in \mathbb{N}$, which split in $\mathbf{K}$ and for which $p-1$ has a few large prime divisors. To be more precise, let us consider an arbitrary number field $\mathbf{K}$. Suppose further that $d = \max\{n \in \mathbb{N} : \mathbb{Q}(\zeta_n) \subseteq \mathbf{K}\}$. Consider a prime $p$ in $\mathbb{N}$ which splits in $\mathbf{K}$, it is immediate that $d$ divides $p-1$. Therefore one can only hope to show that $B_{1,\mathfrak{a}}(x)$ consists of a set of $x/\log^2 x$ primes for which all the prime divisors of $\frac{p-1}{d}$ are greater than some power of $x$. It appears that this is a reasonable target and can be approached in at least two ways, one of which will be elaborated on in this chapter.

We will apply sieve-theoretic techniques to sets containing elements of the form $p-1$ for some set of primes $p$. In order to do this we need more arithmetic information about the distribution of these primes in arithmetic progressions. This puts natural conditions on the kind of number fields to which our arguments can be applied.

The first condition one needs to impose is that the extension $H(\mathbf{K})/\mathbb{Q}$ is abelian. This will allow us to characterise split primes through congruence relationships.

The other restriction pertains to an obstruction we have already come across. If $p \in \mathbb{N}$ is a prime which splits in $\mathbf{K}$ and $d = \max\{n \in \mathbb{N} : \mathbb{Q}(\zeta_n) \subseteq \mathbf{K}\}$, then $d$ divides $(p-1)$. We would like to show that the index of $\left\{\alpha \bmod \mathfrak{p} : \alpha \in \mathcal{O}_{\mathbf{K}}^{\times}\right\}$ (which will turn out to be a divisor of $\frac{\mathfrak{N}(\mathfrak{p})-1}{d}$) is co-prime to $d$. In order to achieve this, we shall need that $\mathbb{Q}(\zeta_f)/\mathbf{K}$ is cyclic, where $f$ is the smallest even number such that $H(\mathbf{K}) \subseteq \mathbb{Q}(\zeta_f)$.

In this chapter we show that one can navigate around these obstructions under the above conditions. As a result one can give an ineffective lower bound on the unit rank such that whenever the unit rank of the number field exceeds this bound, the class group of $\mathcal{O}_{\mathbf{K}}$ will have a Euclidean ideal class for a specific family of fields. More precisely, the main result proved in this chapter is the following.

**Theorem 3.1.2.** *Let $\mathbf{K}$ be a number field and $H(\mathbf{K})$ its Hilbert class field. Suppose that the Hilbert class field is abelian over $\mathbb{Q}$. Let $f$ be the smallest even positive integer such that $H(\mathbf{K}) \subseteq \mathbb{Q}(\zeta_f)$. Further, suppose that the Galois group of $\mathbb{Q}(\zeta_f)$ over $\mathbf{K}$ is cyclic, then there exists a finite natural number $r$ such that if $\mathbf{K}$ has unit rank at least $r$, it has a Euclidean ideal class.*

We can deduce the following corollary from the above theorem for number fields $\mathbf{K}$ with class number one.

**Corollary 3.1.3.** *Let $\mathbf{K}$ be an abelian number field with class number one. Let $f$ be the smallest even positive integer such that $\mathbb{Q}(\zeta_f)$ contains $H(\mathbf{K})$. If $\mathbb{Q}(\zeta_f)$ over $\mathbf{K}$ is cyclic, then there exists a finite natural number $r$ such that if unit rank of $\mathbf{K}$ is greater than or equal to $r$, $\mathcal{O}_{\mathbf{K}}$ is a Euclidean domain.*

The sieve which we will be using to prove the above theorem is a modified version of Brun's sieve as stated in Theorem 2.2.1.

## 3.2 Application of Brun's sieve

We now state and prove the sieve-theoretic result required to show Theorem 3.1.2.

**Proposition 3.2.1.** *Let $\mathbf{K}$ be a number field. Suppose that the Hilbert class field $H(\mathbf{K})$ of $\mathbf{K}$ is abelian over $\mathbb{Q}$ and let $f$ be the smallest even integer such that $H(\mathbf{K})$ is contained in $\mathbb{Q}(\zeta_f)$. Now suppose that $\mathbb{Q}(\zeta_f)$ over $\mathbf{K}$ is cyclic and generated by $\zeta_f \to \zeta_f^b$. Further, let $d = \max(n : \mathbb{Q}(\zeta_n) \subseteq \mathbf{K})$. For $\eta > 0$ define*

$$\mathcal{A}(x)(\eta) := \left\{ \frac{\ell - 1}{d} \; : \; \ell \in \mathbb{N} \textit{ prime} \; , \; \ell \leq x \; , \ell \equiv b \bmod f \textit{ and } \left( \frac{\ell-1}{d}, \prod_{\substack{2 \leq p < x^{\eta} \\ p \textit{ prime}}} p \right) = 1 \right\}$$

*where $(a, b)$ is used to denote the greatest common divisor of two positive integers $a$ and $b$. Then, there exists $\eta > 0$ such that*

$$|\mathcal{A}(x)(\eta)| \gg \frac{x}{\log^2 x}.$$

*The implied constant depends on $\eta$ and $\mathbf{K}$. Here $|S|$ is used to denote the cardinality of a set $S$.*

*Proof.* Let $\Sigma_1 = \{p \in \mathbb{N} \ : \ p \text{ prime and } p \mid 3f\}$. Let $G_1$ be the Galois group of $\mathbb{Q}(\zeta_f)$ over $\mathbf{K}$, $G_2$ be the Galois group of $\mathbb{Q}(\zeta_f)$ over $H(\mathbf{K})$ and $G_3$ be the Galois group of $\mathbb{Q}(\zeta_f)/\mathbb{Q}$. Consider the diagram.

$$\begin{tikzcd}
\mathbb{Q}(\zeta_f) \arrow[d, dash] \arrow[d, dash, bend right, "G_2"] \arrow[dd, dash, bend left=60, "G_1"] \arrow[dddd, dash, bend right=60, "G_3"'] \\
H(\mathbf{K}) \arrow[d, dash] \\
\mathbf{K} \arrow[d, dash] \\
\mathbb{Q}(\zeta_d) \arrow[d, dash] \\
\mathbb{Q}
\end{tikzcd}$$

Then $G_3 = \{\sigma_a \ : \ 1 \leq a \leq n, \ \ (a, f) = 1\}$, where $\sigma_a : \mathbb{Q}(\zeta_f) \to \mathbb{Q}(\zeta_f) \in G_3$ is such that $\sigma_a(\zeta_f) = \zeta_f^a$ and $G_1 \subset \{\sigma_a \in G_3 \ : \ a \equiv 1 \bmod d\}$. By assumption, $G_1$ is cyclic and $\mathbb{Q}(\zeta_d)$ is the maximal cyclotomic field inside $\mathbf{K}$. Since $f$ is assumed to be even, $d|f$. We claim that

$$G_1 \bigcap \left\{\sigma_a \in G_3 \ : \ a \equiv 1 \bmod d, \quad \left(\frac{a-1}{d}, \ \frac{f}{d}\right) = 1\right\} \neq \emptyset.$$

Suppose that our claim is not true i.e., we have $((b-1)/d, f/d) = h \neq 1$, where $G_1$ is generated by $\sigma_b$. Using the binomial theorem, we then have

$$G_1 \subset \{\sigma_a \in G_3 \ : \ a \equiv 1 \bmod dh\}.$$

This implies that $\mathbb{Q}(\zeta_{dh}) \subset K$, a contradiction to the maximality of $d$.

Let $m = (b-1)/d$. Further, let $n_0 \in \mathbb{N}$ be such that $m + n_0 f/d$ is a prime co-prime to $3f$ and $1 + dm + n_0 f$ is co-prime to $3df$. We claim that such an $n_0$ exists. To prove the existence of $n_0$, we break the argument into two cases. Case 1 will deal with the possibility that $3|f$. In this case we just need to choose a prime congruent to $m$ mod $f/d$ co-prime to $3f$ to satisfy both these conditions. In case 2, we have $3 \nmid f$, then we use the Chinese remainder theorem to choose a prime congruent to $m$ mod $f/d$ co-prime to $3f$ and not congruent to $-d^{-1}$ mod 3.

We recall that

$$\Sigma_1 = \{p \in \mathbb{N} : \ p \text{ prime}, p \mid 3f\} \qquad \text{and} \qquad Pr_{\Sigma_1}(z) = \prod_{\substack{p<z \\ p \notin \Sigma_1}} p.$$

We can now define the set

$$\mathcal{A}'(x,z) := \{y \leq x : 1+dm+n_0 f+3ydf \text{ is prime and } (m+n_0(f/d)+3yf, Pr_{\Sigma_1}(z)) = 1\}.$$

Then by Theorem 2.2.1

$$|\mathcal{A}'(x,z)| = \frac{Li(3dfx)}{\varphi(3df)} \prod_{p \mid Pr_{\Sigma_1}(z)} \left(1 - \frac{1}{p-1}\right)(1 + O(E^{(*)}(x,z))), \tag{3.2.1}$$

where

$$E^{(*)}(x,z) = \exp(-(u/3)(\log u - \log\log u - 3)) + \frac{1}{\log z},$$

$u = \frac{\log x}{\log z}$ and $\varphi$ is used to denote the Euler-totient function. Since the $O$ constant in Equation (3.2.1) is absolute, if we put $u = 1/\eta$ for small $\eta$ and large $x$ we get,

$$\begin{aligned}
|\mathcal{A}'(x,x^\eta)| &\gg \frac{x}{\log x} \prod_{\substack{p<x^\eta \\ p \notin \Sigma_1}} \left(1 - \frac{1}{p-1}\right), \\
&\gg \frac{x}{(\log x)\left(\exp\left(\sum_{\substack{p<x^\eta, \\ p \neq 2}} \left(\frac{1}{p-1} + \frac{1}{2(p-1)^2} \cdots\right)\right)\right)}, \\
&\gg \frac{x}{(\log x)\left(\exp\left(\sum_{\substack{p<x^\eta \\ p \neq 2}} \left(\frac{1/(p-1)}{1-1/(p-1)}\right)\right)\right)}, \\
&\gg \frac{x}{(\log x)\left(\exp\left(\sum_{\substack{p<x^\eta, \\ p \neq 2}} \left(\frac{1}{p} + \frac{2}{p(p-2)}\right)\right)\right)}, \\
&\gg \frac{x}{\log^2 x}.
\end{aligned}$$

Note that for any

$$l = 1 + dm + n_0 f + 3ydf, \qquad y \in \mathcal{A}'(x, x^\eta),$$

the term $\frac{l-1}{d}$ is co-prime to $3f$. Therefore, there exists $\eta > 0$ such that

$$|\mathcal{A}(x)(\eta)| \gg \frac{x}{\log^2 x}.$$

□

With this we conclude this section on application of the modified Brun's sieve. We note that the hypothesis of Proposition 3.2.1 allows us to avoid all the obstructions stated out in the introduction. In the last section of this chapter, we will formalize the initial part of the argument mentioned in the introduction.

## 3.3 Proof of Theorem 3.1.2

In this last section of Chapter 3, we use Theorem 3.2.1 and complete the proof of Theorem 3.1.2.

*Proof.* Let $[\mathfrak{a}]$ be a generator of the class group $Cl_{\mathcal{O}_\mathbf{K}}$ of $\mathcal{O}_\mathbf{K}$. Then for any real number $x > 0$, we have

(3.3.1)

$$B_{1,\mathfrak{a}}(x) = \left\{\mathfrak{p} : \mathfrak{p} \text{ prime ideal of } \mathcal{O}_\mathbf{K},\ \mathfrak{N}(\mathfrak{p}) \leq x, [\mathfrak{p}] = [\mathfrak{a}], \mathcal{O}_\mathbf{K}^\times \to (\mathcal{O}_\mathbf{K}/\mathfrak{p})^\times \text{ is surjective}\right\}.$$

In order to complete the proof of Theorem 3.1.2, by Lemma 2.3.3, it suffices to show that

$$|B_{1,\mathfrak{a}}(x)| \gg \frac{x}{\log^2 x}.$$

By our assumption $\mathbb{Q}(\zeta_f)/\mathbf{K}$ is cyclic. Therefore, we can talk about a generator of the Galois group of $\mathbb{Q}(\zeta_f)/\mathbf{K}$. Let $\zeta_f \to \zeta_f^b$ be a generator of $\mathbb{Q}(\zeta_f)$ over $\mathbf{K}$. By Proposition 3.2.1, we have

$$\left|\mathcal{A}(x)(\gamma) = \left\{\frac{\ell-1}{d}\ :\ \ell \in \mathbb{N} \text{ prime },\ \ell \leq x\ , \ell \equiv b \bmod f \text{ and } \left(\frac{\ell-1}{d}, Q\left(x^{\gamma}\right)\right) = 1\right\}\right| \gg \frac{x}{\log^2 x},$$

for all real $\gamma < \eta$. Let

$$\begin{aligned} \mathcal{B}(x)(\gamma) &:= \left\{\ell : \frac{\ell-1}{d} \in \mathcal{A}(x)(\gamma)\right\}, \\ l_{\mathfrak{p}} &:= \left|\left\{\alpha \bmod \mathfrak{p} : \alpha \in \mathcal{O}_{\mathbf{K}}^{\times}\right\}\right|, \quad S_{\mathfrak{p}} := \left(\mathfrak{N}(\mathfrak{p}) - 1\right)/l_{\mathfrak{p}}, \\ J_1(x) &:= \{\mathfrak{p}\ :\ \mathfrak{p} \text{ prime ideal of } \mathcal{O}_{\mathbf{K}},\ \mathfrak{N}(\mathfrak{p}) \in \mathcal{B}(x)(\gamma),\ S_{\mathfrak{p}} = 1\} \quad \text{and} \\ J_2(x) &:= \{\mathfrak{p}\ :\ \mathfrak{p} \text{ prime ideal of } \mathcal{O}_{\mathbf{K}},\ \mathfrak{N}(\mathfrak{p}) \in \mathcal{B}(x)(\gamma),\ S_{\mathfrak{p}} > 1\}. \end{aligned}$$

Consider the following setup : $\mathbb{Q} \subseteq \mathbf{K} \subseteq H(\mathbf{K}) \subseteq \mathbb{Q}(\zeta_f)$. Let $p \in \mathcal{A}(x)(\gamma)$ and let $\mathfrak{P}$ be a prime above it in $\mathbb{Q}(\zeta_f)$. Suppose that $\mathfrak{p} = \mathfrak{P} \cap \mathbf{K}$. From the properties of the Frobenius, we observe that

$$\left(\frac{\mathbb{Q}(\zeta_f)/\mathbb{Q}}{p}\right) = \left(\frac{\mathbb{Q}(\zeta_f)/\mathbf{K}}{\mathfrak{p}}\right)$$

and that

$$\left(\frac{\mathbb{Q}(\zeta_f)/\mathbf{K}}{\mathfrak{p}}\right)\Bigg|_{H(\mathbf{K})} = \left(\frac{H(\mathbf{K})/\mathbf{K}}{\mathfrak{p}}\right)$$

where $\left(\frac{\cdot}{\cdot}\right)$ is used to denote the Artin symbol, as defined in Chapter 2. This allows us to conclude that $J_1(x) \subseteq B_{1,\mathfrak{a}}(x)$. So, it suffices to show that

$$|J_2(x)| = o\left(\frac{x}{\log^2 x}\right).$$

Note that $\mathfrak{N}(\mathfrak{p}) \in \mathcal{B}(\gamma)(x)$ implies that $(\mathfrak{N}(\mathfrak{p}), d) = 1$. Since $d = \prod_{i=1}^{d-1}(1-\zeta_d^i)$, where $\zeta_d$ is a primitive $d$-th root of unity, the elements $\zeta_d^i$ for $1 \leq i \leq d-1$ are distinct modulo $\mathfrak{p}$ and hence they are distinct in $(\mathcal{O}_{\mathbf{K}}/\mathfrak{p})^{\times}$. Thus

$$S_{\mathfrak{p}} \left| \frac{\mathfrak{N}(\mathfrak{p}) - 1}{d} \right. \implies S_{\mathfrak{p}} = 1 \text{ or } S_{\mathfrak{p}} > x^{\gamma}.$$

Now if $\mathfrak{p} \in J_2$, then $S_{\mathfrak{p}} > x^{\gamma}$. Using Lemma 2.3.4, we then have

$$\left|\left\{\mathfrak{p} \ : \ \mathfrak{p} \text{ prime ideal of } \mathcal{O}_{\mathbf{K}}, \ l_{\mathfrak{p}} \leq x^{1-\gamma}\right\}\right| \ \ll \ x^{(1-\gamma)\left(1+\frac{1}{r}\right)},$$

where $r$ is the unit rank of $\mathbf{K}$. Now we choose $\gamma = 1/r$, then

$$(1-\gamma)\left(1+\frac{1}{r}\right) < 1 \implies \left|\left\{\mathfrak{p} \ : \ \mathfrak{p} \text{ prime ideal of } \mathcal{O}_{\mathbf{K}}, \ l_{\mathfrak{p}} \leq x^{1-\gamma}\right\}\right| = o\left(\frac{x}{\log^2 x}\right).$$

This implies that

$$|J_2(x)| \ \leq \ \left|\left\{\mathfrak{p} \ : \ \mathfrak{p} \text{ prime ideal of } \mathcal{O}_{\mathbf{K}}, \ l_{\mathfrak{p}} \leq x^{1-\gamma}\right\}\right| = o\left(\frac{x}{\log^2 x}\right).$$

and hence

$$|B_{1,\mathfrak{a}}(x)| \gg \frac{x}{\log^2 x}$$

whenever $r > 1/\eta$. Since, we only have the existence of an $\eta > 0$ the bound on $r$ is ineffective. Now, an application of Theorem 2.3.3 completes the proof of Theorem 3.1.2. □

With this we conclude the chapter on our results regarding ineffective lower bounds on the unit rank to find Euclidean ideal classes.

# Chapter 4

# Large unit rank

## 4.1 Introduction

Let $\mathbf{K}$ be a Galois number field with ring of integers $\mathcal{O}_{\mathbf{K}}$. We will always assume that the class group of $\mathcal{O}_{\mathbf{K}}$ is cyclic.

Having produced an ineffective bound on the unit rank in Chapter 3, our next aim is to get an effective lower bound such that whenever the unit rank exceeds this bound, we have a Euclidean ideal class for a specific family of fields. As mentioned in the introduction, the first step towards making Lenstra's result (Theorem 1.4.8 [26]) unconditional was taken by Graves and Murty [14]. More precisely, their result is the following.

**Theorem 4.1.1** (Graves and Murty [14])**.** *Suppose that the unit rank of a number field* $\mathbf{K}$ *is at least* 4 *and that the Hilbert class field of* $\mathbf{K}$ *is abelian over* $\mathbb{Q}$*. Further suppose that* $f$ *is the conductor of the Hilbert class field and* $\mathbb{Q}(\zeta_f)/\mathbf{K}$ *is cyclic. Then* $Cl_{\mathcal{O}_{\mathbf{K}}}$ *is cyclic if and only if there is a Euclidean ideal class in* $Cl_{\mathcal{O}_{\mathbf{K}}}$*.*

Graves and Murty proved the above by using the linear lower bound sieve and the Bombieri and Vinogradov theorem. The lower bound required by Graves and

Murty, as mentioned above, is 4. The main aim of this section is to extend this result to the case where the unit rank is 3 and consider the consequences of the Elliott and Halberstam conjecture on this particular result. More precisely, in this chapter, we will prove the following theorems.

**Theorem 4.1.2.** *Suppose that* $\mathbf{K}$ *is a number field with unit rank at least* 3 *and its Hilbert class field* $H(\mathbf{K})$ *is abelian over* $\mathbb{Q}$. *Also suppose that the conductor of* $H(\mathbf{K})$ *is* $f$ *and* $\mathbb{Q}(\zeta_f)$ *over* $\mathbf{K}$ *is cyclic. Then* $Cl_{\mathcal{O}_{\mathbf{K}}}$ *is cyclic if and only if it has a Euclidean ideal class.*

We know that the proof of Graves and Murty depends on the Bombieri and Vinogradov theorem. So it is natural to investigate the implications of the Elliott and Halberstam conjecture on this problem. Under the Elliott and Halberstam conjecture, we have the following result.

**Theorem 4.1.3.** *Let* $\mathbf{K}$ *be a number field such that the Hilbert class field* $H(\mathbf{K})$ *is abelian over* $\mathbb{Q}$ *and the Galois group* $Gal(\mathbb{Q}(\zeta_f)/\mathbf{K})$ *is cyclic where* $f$ *is the conductor of* $H(\mathbf{K})$. *Now if the Elliott and Halberstam conjecture is true and the unit rank of* $\mathbf{K}$ *is at least two, then* $Cl_{\mathcal{O}_{\mathbf{K}}}$ *is cyclic if and only if it has a Euclidean ideal class.*

We recall here that under the extended Riemann hypothesis, Lenstra [26] was able to prove this result for unit rank at least one. However under the Elliott and Halberstam conjecture, our methods only allow us to prove this result for unit rank at least two.

To prove Theorem 4.1.2 we use the linear lower bound sieve with well factorable weights (Theorem 2.2.3 [24]) as opposed to the modified version of Brun's sieve which was used in Chapter 3. We add here that this new ingredient allows us to improve upon the work of Graves and Murty. We replace their application of the lower bound sieve (Theorem 2.2.5) with the more modern lower bound sieve with well factorable weights. Further the process of estimating the error term will be done by using a theorem of Bombieri, Friedlander and Iwaniec on primes in arithmetic progressions (Theorem 2.2.4 [2, 9, 20]), instead of the Bombieri and Vinogradov theorem as used by Graves and Murty.

To prove Theorem 4.1.3, on the other hand, we use Theorem 2.2.5 and the Elliott and Halberstam conjecture (Conjecture 2.2.6).

## 4.2 Applications of the linear lower bound sieve

In this section, using Theorem 2.2.3 and Theorem 2.2.4, we deduce the following sieve theoretic result which plays a key role in the proof of Theorem 4.1.2. Later, we will also prove an analogous sieve theoretic result (Theorem 4.2.3), using Theorem 2.2.5, which will be used in the proof of Theorem 4.1.3

**Theorem 4.2.1.** *Let $\mathbf{K}$ be a number field and its Hilbert class field $H(\mathbf{K})$ be abelian over $\mathbb{Q}$. Also let $f$ be the smallest even integer such that $H(\mathbf{K})$ is contained in $\mathbb{Q}(\zeta_f)$ and $\mathbb{Q}(\zeta_f)$ over $\mathbf{K}$ be cyclic. Set $d := \max\{n \ : \ \mathbb{Q}(\zeta_n) \subseteq \mathbf{K}\}$ and*

$$\mathcal{A}(x) := \left\{ \frac{\ell - 1}{d} \ : \ \ell \in \mathbb{N}, \ \ell \text{ prime}, \ \ell \leq x, \ \text{and } \ell \equiv b \bmod f \right\},$$

*where $\zeta_f \to \zeta_f^b$ is a generator of $\mathbb{Q}(\zeta_f)$ over $\mathbf{K}$. Let $\mathcal{P} := \{p \in \mathbb{N} \ : \ p \text{ prime}\}$. Then for any real number $\eta < 16/63$, one has*

$$S(\mathcal{A}(x), \mathcal{P}, x^\eta) \gg \frac{x}{\log^2 x}.$$

**Remark 4.2.2.** *Here we point out that Theorem 4.2.1 is explicit as opposed to Theorem 3.2.1. More precisely, it gives an explicit bound on the exponent $\eta$ which is not possible with the techniques used in the proof of Theorem 3.2.1.*

*Proof.* Let $G_1$ be the Galois group of $\mathbb{Q}(\zeta_f)$ over $\mathbf{K}$, $G_2$ be the Galois group of $\mathbb{Q}(\zeta_f)$

over $H(\mathbf{K})$ and $G_3$ be the Galois group of $\mathbb{Q}(\zeta_f)/\mathbb{Q}$. Consider the diagram

$$\begin{tikzcd}
\mathbb{Q}(\zeta_f) \arrow[d, dash] \arrow[d, bend right, dash, "G_2"] \arrow[dd, bend left=60, dash, "G_1"] \arrow[dddd, bend right=60, dash, "G_3"] \\
H(K) \arrow[d, dash] \\
K \arrow[d, dash] \\
\mathbb{Q}(\zeta_d) \arrow[d, dash] \\
\mathbb{Q}
\end{tikzcd}$$

Then

$$G_3 = \{\sigma_a \ : \ 1 \leq a \leq n, \ \ (a, f) = 1\},$$

where $\sigma_a : \mathbb{Q}(\zeta_f) \to \mathbb{Q}(\zeta_f) \in G_3$ is such that $\sigma_a(\zeta_f) = \zeta_f^a$ and

$$G_1 \subset \{\sigma_a \in G_3 \ : \ a \equiv 1 \bmod d\}.$$

By assumption, $G_1$ is cyclic and $\mathbb{Q}(\zeta_d)$ is the maximal cyclotomic field inside $\mathbf{K}$. Since $f$ is assumed to be even, $d|f$. We claim that

$$G_1 \cap \left\{\sigma_a \in G_3 \ : \ a \equiv 1 \bmod d, \ \ \left(\frac{a-1}{d}, \ \frac{f}{d}\right) = 1\right\} \neq \emptyset.$$

Suppose not. Now if $G_1$ is generated by $\sigma_b$, where $((b-1)/d, \ f/d) = h \neq 1$, then every element of $G_1$ is of the form

$$\underbrace{\sigma_b \circ \cdots \circ \sigma_b}_{r \text{ times}} \ = \ \sigma_{b^r}.$$

Using the binomial theorem, we then have

$$G_1 \subset \{\sigma_a \in G_3 \ : \ a \equiv 1 \bmod dh\}.$$

This implies that

$$\mathbb{Q}(\zeta_{dh}) \quad \subset \ \mathbf{K},$$

a contradiction to the maximality of $d$. Let $m = (b-1)/d$. Now choose $n_0 > 0$ such that

$$m + n_0 f/d \text{ is prime} \quad \text{ and } \quad (m + n_0 f/d, f) = 1.$$

For any real number $x > 0$, define

$$\mathcal{A}'(x) := \{\ell - 1 \leq x \ : \ \ell \in \mathbb{N} \text{ is prime and } \ell \equiv 1 + dm + n_0 f \bmod df\}.$$

Then we have

$$|\mathcal{A}'(x)| \sim \frac{Li(x)}{\varphi(df)}$$

as $x \to \infty$. Set $\mathcal{P}_1 := \{p : p \nmid f\}$. Then for any $p \in \mathcal{P}_1$, we have

$$|\mathcal{A}'_p(x) := \{u \in \mathcal{A}'(x) : p|u\}| \sim \frac{Li(x)}{\varphi(pdf)}$$

as $x \to \infty$. Therefore for any square-free number $q$ with prime divisors in $\mathcal{P}_1$, we have

$$|\mathcal{A}'_q(x)| \ = \ \frac{\omega(q)}{q}|\mathcal{A}'(x)| \ + \ r_q(x).$$

Here

$$\frac{\omega(q)}{q} = \frac{1}{\varphi(q)} \quad \text{and} \quad r_q(x) = \left(\pi(x, qdf, u_q) - \frac{Li(x)}{\varphi(qdf)}\right),$$

where $u_q$ satisfies

$$u_q \ \equiv \ 1 \bmod q \quad \text{and} \quad u_q \ \equiv \ 1 + dm + n_0 f \bmod df.$$

Since $2|f$, for any integer $w \geq 2$, one has

$$\begin{aligned}\prod_{\substack{w \leq p < z \\ p \in \mathcal{P}_1}} \left(1 - \frac{\omega(p)}{p}\right)^{-1} &= \exp\left(-\sum_{\substack{w \leq p < z \\ p \in \mathcal{P}_1}} \log\left(1 - \frac{1}{p-1}\right)\right), \\ &= \exp\left(\sum_{\substack{w \leq p < z \\ p \in \mathcal{P}_1}} \left(\frac{1}{p-1} + \frac{1}{2(p-1)^2} + \cdots\right)\right), \\ &\leq \exp\left(\sum_{\substack{w \leq p < z \\ p \in \mathcal{P}_1}} \frac{1/(p-1)}{1 - 1/(p-1)}\right), \\ &\leq \exp\left(\sum_{\substack{w \leq p < z \\ p \in \mathcal{P}_1}} \frac{1}{p} + \frac{2}{p(p-2)}\right) \ll \frac{\log z}{\log w}.\end{aligned}$$

Therefore using Merten's theorem and Theorem 2.2.3, there exists an absolute constant $C_1 > 0$ such that

$$S(\mathcal{A}(x), \mathcal{P}_1, D^{1/s}) \geq \frac{C_1 x}{\log^2 x} + \sum_{(q,df)=1} \lambda_n(q)\ r_q(x), \tag{4.2.1}$$

for some well factorable function $\lambda_n$ of level $D \geq 1$ and for any $s \geq 2$. Now let $D = x^{4/7-\varepsilon}$ where $0 < \varepsilon < 4/7$ is a real number. Then applying Theorem 2.2.4 with $k = df$, we have

$$\sum_{\substack{q \leq D, \\ (q,df)=1}} \lambda_n(q)\ r_q(x) \ll \frac{x}{\log^A x} \tag{4.2.2}$$

for any positive integer $A$. Finally by choosing $s = 9/4$ and using equations (4.2.1), (4.2.2), we get that

$$S(\mathcal{A}'(x), \mathcal{P}_1, x^{\frac{4-7\varepsilon}{15.75}}) \gg \frac{x}{\log^2 x}.$$

Set

$$\mathcal{A}''(x) := \left\{\frac{\ell - 1}{d} \ : \ \text{for all } \ell - 1 \in \mathcal{A}'(x)\right\}.$$

Clearly $S(\mathcal{A}''(x), \mathcal{P}_1, x^\eta) \gg x/\log^2 x$ for any real number $\eta < 16/63$ $\left(= \frac{4}{15.75}\right)$. Since every element of $\mathcal{A}''(x)$ is co-prime to $f$ and $\mathcal{A}''(x) \subset \mathcal{A}(x)$, we have

$$S(\mathcal{A}(x), \mathcal{P}, x^\eta) \ \geq \ S(\mathcal{A}''(x), \mathcal{P}, x^\eta) \gg \frac{x}{\log^2 x}.$$

□

Now if we assume the conjecture of Elliott and Halberstam (see Conjecture 2.2.6), we can prove the following statement using Theorem 2.2.5. We use the older linear lower bound sieve as opposed to Theorem 2.2.3 because we only have an estimate for sums of absolute values of the error terms $r_q(x)$ appearing in the sieve.

**Theorem 4.2.3.** *Suppose that the Elliott and Halberstam conjecture is true. Let* $\mathbf{K}$ *be a number field and its Hilbert class field* $H(\mathbf{K})$ *be abelian over* $\mathbb{Q}$*. Also let* $f$ *be the smallest even integer such that* $H(\mathbf{K})$ *is contained in* $\mathbb{Q}(\zeta_f)$ *and* $\mathbb{Q}(\zeta_f)$ *over* $\mathbf{K}$ *be cyclic. Set* $d := \max\{n \ : \ \mathbb{Q}(\zeta_n) \subseteq \mathbf{K}\}$ *and*

$$\mathcal{A}(x) := \left\{ \frac{\ell - 1}{d} \ : \ \ell \in \mathbb{N}, \ \ell \leq x, \ \ell \textit{ prime and } \ell \equiv b \bmod f \right\},$$

*where* $b \bmod f$ *is a generator of* $\mathbb{Q}(\zeta_f)$ *over* $\mathbf{K}$*. Let* $\mathcal{P} := \{p \in \mathbb{N} \ : \ p \textit{ prime } \}$*. Then for any positive real number* $\eta < 1/2$*, one has*

$$S(\mathcal{A}(x), \mathcal{P}, x^\eta) \gg \frac{x}{\log^2 x}$$

*where the constant implied in the symbol* $\gg$ *depends on* $\eta$*.*

**Remark 4.2.4.** *We now highlight the difference between the above theorem and Theorem 4.2.1. The bound for the exponent* $\eta$ *here (*$< 1/2$*), is better than that in Theorem 4.2.1(*$< 16/63$*). But we hasten to add that Theorem 4.2.1 is unconditional.*

*Proof.* As in the proof of Theorem 4.2.1, we can show that there exists a $b \bmod f$ which generates $\mathbb{Q}(\zeta_f)$ over $\mathbf{K}$ such that $b = 1 + dm$ with $(m, f/d) = 1$. As before, choose an $n_0$ such that $m + n_0 f/d$ is a prime co-prime to $f$. Now let

$$\mathcal{A}'(x) := \{\ell - 1 \leq x \ : \ \ell \in \mathbb{N}, \ \ell \text{ prime and } \ell \equiv 1 + dm + n_0 f \bmod df\}$$

and $\mathcal{P}_1 = \{p \ : \ p \nmid f\}$ be as in the proof of Theorem 4.2.1. Using Theorem 2.2.5, we would like to estimate $S(\mathcal{A}'(x), \ \mathcal{P}_1, \ x^{1/2-\delta})$ for any $\delta > 0$. In order to apply Theorem 2.2.5, we need $\mathcal{A}'(x)$ and $\mathcal{P}_1$ to satisfy the conditions of Theorem 2.2.5. Note that for all $p \in \mathcal{P}_1$, one has $\omega(p)/p = 1/\varphi(p)$ and

$$|r_q(x)| \ \leq \ \max_{y \leq x} \max_{(a,qdf)=1} \left| \pi(y, qdf, a) - \frac{Li(y)}{\varphi(qdf)} \right|,$$

where $q$ is any square-free number with prime divisors in $\mathcal{P}_1$. Since $f$ is always even, Condition 1 (Equation (2.2.6)) of Theorem 2.2.5 will be trivially satisfied by choosing $A_1 = 2$. To check Condition 2 (Equation (2.2.7)), we consider

$$\sum_{\substack{g_1 \leq p \leq z \\ p \in \mathcal{P}_1}} \frac{\omega(p) \log p}{p} \ = \ \sum_{g_1 \leq p \leq z} \frac{\frac{p}{p-1} \log p}{p} \ - \ \sum_{\substack{g_1 \leq p \leq z, \\ p | df}} \frac{\frac{p}{p-1} \log p}{p}.$$

Since the second term in the above equality is bounded by a constant, we have

$$\begin{aligned}\sum_{\substack{g_1 \leq p \leq z \\ p \in \mathcal{P}_1}} \frac{\omega(p) \log p}{p} - \log(z/g_1) \ &= \ \sum_{g_1 \leq p \leq z} \frac{\log p}{p} \ + \ \sum_{g_1 \leq p \leq z} \frac{\log p}{p(p-1)} \ - \ \log(z/g_1) \ + \ O(1) \\ &= \ O(1).\end{aligned}$$

In order to check Condition 3 (Equation (2.2.8)), we observe by Cauchy and Schwarz inequality that

$$\sum{}' \mu^2(q) \ 3^{\nu(q)} \ |r_q(x)| \ \leq \ \sqrt{\sum{}' \ 9^{\nu(q)} \ |r_q(x)|} \sqrt{\sum{}' \ |r_q(x)|}$$

where the sum $\sum'$ is over the positive integers $q$ which are less than $X^\alpha / \log^F X$ and are divisible only by primes in $\mathcal{P}_1$. Note that for any $q$ with all its prime divisors in

$\mathcal{P}_1$, we have

$$\begin{aligned} |r_q(x)| \;&\leq\; |\mathcal{A}'_q(x)| \;+\; \left|\frac{Li(x)}{\varphi(qdf)}\right| \;\leq\; \frac{2x}{\varphi(q)} \\ \text{and} \quad {\sum}' \frac{9^{\nu(q)}}{\varphi(q)} \;&\leq\; \sum_{\substack{1 \leq q < \frac{X^\alpha}{(\log X)^F}, \\ q \text{ square free}}} \frac{9^{\nu(q)}}{\varphi(q)} \\ &\leq\; \prod_{p < \frac{X^\alpha}{(\log X)^F}} \left(1 + \frac{1}{p-1}\right)^9 \\ &\leq\; \prod_{p < \frac{X^\alpha}{(\log X)^F}} \left(1 - \frac{1}{p}\right)^{-9} \;\ll\; \log^9 x \;, \end{aligned}$$

where in the last step, we have used Merten's theorem. Hence

$$ {\sum}' \; 9^{\nu(q)} \; |r_q(x)| \;\ll\; x \log^9 x. $$

We now use Elliott and Halberstam conjecture to see that

$$ \sum_{\substack{p|q \implies p \in \mathcal{P}_1, \\ q \leq \frac{x^{1-\varepsilon_1}}{\log^B x}}} |r_q(x)| \;\leq\; \sum_{q \leq \frac{(dfx)^{1-\varepsilon_1}}{\log^B (dfx)}} \max_{y \leq x} \max_{(a,q)=1} \left| \pi(y,q,a) - \frac{Li(y)}{\varphi(q)} \right| \ll \frac{x}{\log^3 x} $$

for any $\varepsilon_1 > 0$. Therefore by applying Theorem 2.2.5 and choosing $z = x^{1/2-\varepsilon}$ with $\varepsilon < 1/2$, we have

$$ S(\mathcal{A}'(x),\ \mathcal{P}_1,\ x^{1/2-\varepsilon}) \;\geq\; \frac{Li(x)}{\varphi(df)} V(x^{1/2-\varepsilon}) \left\{ g\left( \frac{(1-\varepsilon_1)\log X}{(\frac{1}{2}-\varepsilon)\log x} \right) \;-\; \frac{B}{\log^{14} X} \right\}. $$

Choose $\max(0, 4\varepsilon - 1) < \varepsilon_1 < 2\varepsilon$. Then we get

$$ \frac{(1-\varepsilon_1)\log X}{(\frac{1}{2}-\varepsilon)\log x} \;\leq\; \frac{(2-2\varepsilon_1)(\log(Li(x)))}{(1-2\varepsilon)\log x} \;\leq\; \frac{2-2\varepsilon_1}{1-2\varepsilon} \;\leq\; 4. $$

Similarly, for $\varepsilon' > 0$ such that

$$ \varepsilon' < \frac{2\varepsilon - \varepsilon_1}{1-\varepsilon_1}, $$

and sufficiently large $x$, we get

$$\frac{(1-\varepsilon_1)\log X}{(\frac{1}{2}-\varepsilon)\log x} \geq \frac{(2-2\varepsilon_1)(\log x - \log\log x + \log(1/\varphi(df)))}{(1-2\varepsilon)\log x} \geq \frac{(2-2\varepsilon_1)(1-\varepsilon')}{1-2\varepsilon} > 2.$$

Thus there exists a constant $Z > 0$ such that for any real number $\eta < 1/2$ and $x$ sufficiently large, we have

$$S(\mathcal{A}'(x), \mathcal{P}_1, x^\eta) \;\geq\; \frac{Zx}{\log^2 x}. \tag{4.2.3}$$

Using arguments similar to the proof of Theorem 4.2.1, we now have

$$S(\mathcal{A}(x), \mathcal{P}, x^\eta) \;\gg\; \frac{x}{\log^2 x},$$

where

$$\mathcal{A}(x) := \left\{ \frac{\ell-1}{d} \;:\; \ell \in \mathbb{N},\ \ell \text{ prime },\ \ell \leq x \;\text{ and } \ell \equiv b \bmod f \right\},$$

and $\mathcal{P} = \{p \in \mathbb{N} \;:\; p \text{ prime}\}$. □

We now formalise the algebraic arguments required to complete the proof.

## 4.3 Proof of Theorem 4.1.2 and Theorem 4.1.3

In this final section of Chapter 4, we complete the proofs of Theorem 4.1.2 and Theorem 4.1.3.

### 4.3.1 Proof of Theorem 4.1.2

In this subsection we give in detail the proof Theorem 4.1.2.

*Proof.* Let $[\mathfrak{a}]$ be a generator of the class group $Cl_{\mathcal{O}_{\mathbf{K}}}$ of $\mathcal{O}_{\mathbf{K}}$. Then for any real number $x > 0$, set

(4.3.1)

$B_{1,\mathfrak{a}}(x) = \{\mathfrak{p} \ : \ \mathfrak{p}$ prime ideal in $\mathcal{O}_{\mathbf{K}}, \ \mathfrak{N}(\mathfrak{p}) \leq x, \ [\mathfrak{p}] = [\mathfrak{a}], \ \mathcal{O}_{\mathbf{K}}^{\times} \to (\mathcal{O}_{\mathbf{K}}/\mathfrak{p})^{\times}$ is surjective$\}$.

In order to complete the proof of Theorem 4.1.2, by Lemma 2.3.3, it suffices to show that

$$|B_{1,\mathfrak{a}}(x)| \gg \frac{x}{\log^2 x}.$$

Applying Theorem 4.2.1 to

$$\mathcal{A}(x) = \left\{ \frac{p-1}{d} \ : \ p \leq x, \ p \in \mathbb{N}, \ p \text{ prime }, \ p \equiv b \bmod f \right\},$$

where $b \bmod f$ is a generator of the Galois group $G := Gal(\mathbb{Q}(\zeta_f)/\mathbf{K})$, we get

$$S(\mathcal{A}(x), \mathcal{P}, x^{\eta}) = |\{ \ u \in \mathcal{A}(x) \ : \ \ell | u, \ \ell \in \mathbb{N}, \ \ell \text{ prime } \implies \ell > x^{\eta}\}| \ \gg \ \frac{x}{\log^2 x}$$

for any positive real number $\eta < 16/63$, where $\mathcal{P} = \{p \in \mathbb{N} : p \text{ prime}\}$. Set

$$\begin{aligned} \mathcal{B}(x) \ &:= \ \{u \in \mathcal{A}(x) \ : \ \ell | u, \ \ell \in \mathbb{N}, \ \ell \text{ prime } \implies \ell > x^{\eta}\} \\ \text{and} \ \ \mathcal{C}(x) \ &:= \ \{p \in \mathbb{N} \ : \ \ p \text{ prime }, \ \frac{p-1}{d} \in \mathcal{B}(x)\}. \end{aligned}$$

Also let

$$\begin{aligned} l_{\mathfrak{p}} \ &:= \ |\{\alpha \bmod \mathfrak{p} : \alpha \in \mathcal{O}_{\mathbf{K}}^{\times}\}|, \quad S_{\mathfrak{p}} := (\mathfrak{N}(\mathfrak{p}) - 1)/l_{\mathfrak{p}}, \\ J_1(x) \ &:= \ \{\mathfrak{p} \ : \ \text{ prime ideal of } \mathcal{O}_{\mathbf{K}}, \ \mathfrak{N}(\mathfrak{p}) \in \mathcal{C}(x), \ S_{\mathfrak{p}} = 1\} \quad \text{and} \\ J_2(x) \ &:= \ \{\mathfrak{p} \ : \ \text{ prime ideal of } \mathcal{O}_{\mathbf{K}}, \ \mathfrak{N}(\mathfrak{p}) \in \mathcal{C}(x), \ S_{\mathfrak{p}} > 1\}. \end{aligned}$$

Since every prime which is equivalent to $b \bmod f$ splits completely in $\mathbf{K}$, it suffices to show that

$$|J_2(x)| = o\left(\frac{x}{\log^2 x}\right).$$

By the same argument as in proof of Theorem 3.1.2, one can show that if $\mathfrak{N}(\mathfrak{p}) \in \mathcal{C}(x)$,

$$S_{\mathfrak{p}} \left| \frac{\mathfrak{N}(\mathfrak{p})-1}{d} \right. \implies S_{\mathfrak{p}} = 1 \text{ or } S_{\mathfrak{p}} > x^{\eta}.$$

Now if $\mathfrak{p} \in J_2(x)$, then $S_{\mathfrak{p}} > x^{\eta}$. Using Lemma 2.3.4, we then have

$$\left|\{\mathfrak{p} \ : \ \mathfrak{p} \text{ prime ideal in } \mathcal{O}_{\mathbf{K}}, \ l_{\mathfrak{p}} \leq x^{1-\eta}\}\right| \ \ll \ x^{(1-\eta)(1+\frac{1}{r})},$$

where $r$ is the unit rank of $\mathbf{K}$. If the unit rank $r$ of $\mathbf{K}$ is greater than or equal to 3 and $\eta = 251/1000$, then

$$(1-\eta)\left(1+\frac{1}{r}\right) < 1 \implies \left|\{\mathfrak{p} \ : \ \mathfrak{p} \text{ prime ideal in } \mathcal{O}_{\mathbf{K}}, \ l_{\mathfrak{p}} \leq x^{1-\eta}\}\right| = o\left(\frac{x}{\log^2 x}\right).$$

This implies that

$$|J_2(x)| \ \leq \ \left|\{\mathfrak{p} \ : \ \mathfrak{p} \text{ prime ideal in } \mathcal{O}_{\mathbf{K}}, \ l_{\mathfrak{p}} \leq x^{1-\eta}\}\right| = o\left(\frac{x}{\log^2 x}\right).$$

and hence

$$|B_{1,\mathfrak{a}}(x)| \gg \frac{x}{\log^2 x}.$$

This completes the proof of Theorem 4.1.2. □

Therefore one can see that with the use of well factorable weights, we can improve the result of Graves and Murty [14], to the case of unit rank 3. In the next section, we outline the proof of Theorem 4.1.3 by highlighting the modifications required in the proof of Theorem 4.1.2.

### 4.3.2 Proof of Theorem 4.1.3

Suppose that the Elliott and Halberstam conjecture is true. Then by Theorem 4.2.3, we have $S(\mathcal{A}(x), \mathcal{P}, x^{\eta}) \gg \frac{x}{\log^2 x}$, for any real $\eta < 1/2$. Let

$$\begin{aligned}
\mathcal{B}(x) &:= \{\ u \in \mathcal{A}(x)\ :\ \ell | u,\ \ell \in \mathbb{N},\ \ell \text{ prime } \implies \ell > x^{\eta}\},\\
\mathcal{C}(x) &:= \left\{ p \in \mathbb{N}\ :\ p \text{ prime },\ \frac{p-1}{d} \in \mathcal{B}(x) \right\},\\
l_{\mathfrak{p}} &:= |\{\alpha \bmod \mathfrak{p} : \alpha \in \mathcal{O}_{\mathbf{K}}^{\times}\}|, \quad S_{\mathfrak{p}} := (\mathfrak{N}(\mathfrak{p}) - 1)/l_{\mathfrak{p}},\\
J_1(x) &:= \{\mathfrak{p}\ :\ \mathfrak{p} \text{ prime ideal in } \mathcal{O}_{\mathbf{K}},\ \mathfrak{N}(\mathfrak{p}) \in \mathcal{C}(x),\ S_{\mathfrak{p}} = 1\} \quad \text{and}\\
J_2(x) &:= \{\mathfrak{p}\ :\ \mathfrak{p} \text{ prime ideal in } \mathcal{O}_{\mathbf{K}},\ \mathfrak{N}(\mathfrak{p}) \in \mathcal{C}(x),\ S_{\mathfrak{p}} > 1\}.
\end{aligned}$$

Then proceeding as in the proof of Theorem 4.1.2, we have

$$\left|\{\mathfrak{p}\ :\ \mathfrak{p} \text{ prime ideal in } \mathcal{O}_{\mathbf{K}},\ l_{\mathfrak{p}} \le x^{1-\eta}\}\right| \ll x^{(1-\eta)(1+\frac{1}{r})},$$

where $r$ is the unit rank of $\mathbf{K}$ and $\eta := 1/2 - \varepsilon$. If the unit rank $r$ of $\mathbf{K}$ is greater than or equal to 2 and $\eta = 5/14$, then

$$(1-\eta)\left(1 + \frac{1}{r}\right) < 1 \implies |J_2(x)| = o\left(\frac{x}{\log^2 x}\right) \implies |B_{1,\mathfrak{a}}(x)| \gg \frac{x}{\log^2 x},$$

where $B_{1,\mathfrak{a}}(x)$ is as defined in Equation (4.3.1). This completes the proof of Theorem 4.1.3 when the unit rank of $\mathbf{K}$ is strictly greater than 1.

## 4.4 Concluding remarks

In the final section of this chapter, we note that the proof of Theorem 4.1.2 actually yields a result that is stronger. We state the stronger result below.

As in the previous sections, let $\mathbf{K}$ be a number field with unit rank greater than or equal to 3 and let its Hilbert class field $H(\mathbf{K})$ be abelian over $\mathbb{Q}$. Consider the diagram

$$\begin{tikzcd}
\mathbb{Q}(\zeta_f) \arrow[d, dash] \arrow[dd, dash, bend left, "G_1"] \arrow[dddd, dash, bend right, "G_3"'] \\
H(\mathbf{K}) \arrow[d, dash] \arrow[d, dash, bend right, "G_2"'] \\
\mathbf{K} \arrow[d, dash] \\
\mathbb{Q}(\zeta_d) \arrow[d, dash] \\
\mathbb{Q}
\end{tikzcd}$$

Let $G_3$ be the Galois group of $\mathbb{Q}(\zeta_f)$ over $\mathbb{Q}$. Then $G_3 = \{\sigma_a \ : \ 1 \leq a \leq n, \ \ (a, f) = 1\}$, where $\sigma_a : \mathbb{Q}(\zeta_f) \to \mathbb{Q}(\zeta_f) \in G_3$ is such that $\sigma_a(\zeta_f) = \zeta_f^a$. If $G_1$ is the Galois group of $\mathbb{Q}(\zeta_f)$ over $K$, $Cl_{\mathcal{O}_\mathbf{K}}$ is cyclic and

$$\big\{\sigma_a \in G_1 \ : \quad G_2 = \langle \sigma_a|_{H(K)} \rangle\big\} \bigcap \left\{\sigma_a \in G_3 \ : \quad a \equiv 1 \bmod d, \quad \left(\frac{a-1}{d}, \ \frac{f}{d}\right) = 1\right\} \neq \phi,$$

then it has a Euclidean ideal class. Here the notation $G_2 = \langle \sigma_a|_{H(K)} \rangle$ denotes that $\sigma_a|_{H(K)}$ generates $G_2$. Now if we assume the Elliott and Halberstam conjecture, then one can improve the unit rank up to 2. These results are stronger than Theorem 4.1.2 and Theorem 4.1.3 as they also include number fields

$$\mathbf{K} \subset \ \mathbb{Q}(\zeta_{2^k}), \ \text{for all } k \geq 1$$

whose ring of integers $\mathcal{O}_\mathbf{K}$ is a principal ideal domain. Here $\zeta_{2^k}$ is a $2^k$-th primitive root of unity. One can also adapt Theorem 4.2.3, to the set up where one has the above co-primality condition. This will be useful in the Chapter 5. More precisely, one can show the following.

**Theorem 4.4.1.** *Suppose that the Elliott and Halberstam conjecture is true. Let* $\mathbf{K}$ *be a number field such that its Hilbert class field* $\mathbf{H}(\mathbf{K})$ *is abelian over* $\mathbb{Q}$*. Also let* $f$

*be the conductor of* $\mathbf{H}(\mathbf{K})$ *and* $d := \max\{n \ : \ \mathbb{Q}(\zeta_n) \subseteq \mathbf{K}\}$. *Set*

$$\mathcal{A}(x) := \left\{ \frac{\ell - 1}{d} \ : \ \ell \in \mathbb{N}, \ \ell \text{ prime }, \ell \leq x \text{ and } \ell \equiv b \bmod f \right\},$$

*where* $\zeta_f \to \zeta_f^b$ *is an element of the Galois group of* $\mathbb{Q}(\zeta_f)$ *over* $\mathbf{K}$ *such that* $((b-1)/d, \ f/d) = 1$ *(provided it exists). Then for any real number* $\eta < 1/2$, *one has*

$$|\{u \in \mathcal{A}(x) : p \text{ prime}, p|u \implies p > x^\eta\}| \gg \frac{x}{\log^2 x},$$

*where the implied constant depends on* $\eta$ *and* $\mathbf{K}$.

**Remark 4.4.2.** *Observe that we assumed that* $f$ *is the conductor of* $\mathbf{K}$. *However the proof holds if* $f$ *is replaced by any multiple of* $f$, *say for* $16f$, *in the above statement. Further Theorem 4.4.1 is stronger than Theorem 4.2.3 since the co-primality condition is weaker than that of cyclicity of* $\mathbb{Q}(\zeta_f)/\mathbf{K}$.

With this we conclude the chapter on number fields with large unit rank and move on to the case of lower unit rank in the next chapter.

# Chapter 5

# Small unit rank

## 5.1 Introduction

In the last chapter of this thesis we will prove results on Galois number fields of small unit rank. As we saw in Chapters 3 and 4, whenever the unit rank of $\mathcal{O}_{\mathbf{K}}$ is large, one can show that the class group of $\mathcal{O}_{\mathbf{K}}$ has a Euclidean ideal class for certain number fields. However in the case of real quadratic and Galois cubic fields, the unit rank will not be large enough. To address this situation we use an idea of Narkiewicz (see [29], [31]). The idea is to look at the compositum of number fields with lower unit rank to generate a new field of larger unit rank.

Let us first briefly recall a theorem of Graves here in order to put the next step in perspective.

**Theorem 5.1.1** (Graves [13]). *If $\mathfrak{a}$ is a non-zero integral ideal of $\mathcal{O}_{\mathbf{K}}$, then*

$$B_{1,\mathfrak{a}} = \left\{\mathfrak{p} : \mathfrak{p} \textit{ is a prime ideal of } \mathcal{O}_{\mathbf{K}}, [\mathfrak{p}] = [\mathfrak{a}], \mathcal{O}_{\mathbf{K}}^{\times} \to (\mathcal{O}_{\mathbf{K}}/\mathfrak{p})^{\times} \textit{ is surjective}\right\} \bigcup \{\mathcal{O}_{\mathbf{K}}\}\,.$$

Further, $B_{1,\mathfrak{a}}(X) = \{\mathfrak{p} \in B_{1,\mathfrak{a}} : \mathfrak{N}(\mathfrak{p}) \leq X\}$.

Coming back to our strategy; we use a lemma of Narkiewicz (Lemma 2.3.5, [29]) and the sieve of Heath-brown (Lemma 2.2.7, [20]) to show that there exists a sequence of positive real numbers $(x_n)_{n\in\mathbb{N}}$ tending to infinity such that

$$|B_{1,\mathfrak{p}}(x_n)| \gg \frac{x_n}{\log^2 x_n} \tag{5.1.1}$$

for some prime ideal $\mathfrak{p}$ in the compositum. The set $B_{1,\mathfrak{p}}$ considered in Equation (5.1.1) is a subset of the set of prime ideals in the compositum of either the quadratic or cubic fields as the case may be.

We then use the pigeonhole principle to show that at least one class from the ideal class group of at least one of the cubic or quadratic fields will have $y_n/\log^2 y_n$ prime ideals for which $\mathcal{O}_{\mathbf{K}}^{\times}$ surjects onto $(\mathcal{O}_{\mathbf{K}}/\mathfrak{p})^{\times}$ (where $(y_n)_{n\in\mathbb{N}}$ is a subsequence of $(x_n)_{n\in\mathbb{N}}$ again going to infinity). We pause now to recall another theorem of Graves that we have used time and again in this thesis.

**Theorem 5.1.2.** *(Graves [13]) Suppose* $\mathbf{K}$ *is a number field with unit rank at least one. Further suppose that* $\mathcal{O}_{\mathbf{K}}$ *has cyclic class group and that* $\mathfrak{a}$ *is an integral ideal of* $\mathcal{O}_{\mathbf{K}}$ *such that* $[\mathfrak{a}]$ *generates the class group. If*

$$|B_{1,\mathfrak{a}}(x)| \gg x/\log^2 x,$$

*then* $\mathfrak{a}$ *is a Euclidean ideal.*

We would like to use Theorem 5.1.2 to detect a Euclidean ideal class. But since the bound we get holds only for a sequence of $y_n \in \mathbb{R}$ and not all $y \in \mathbb{R}$, we develop a sequential analog of Theorem 5.1.2 or Theorem 2.3.3 (See Theorem 5.2.1). But Theorem 5.2.1, like Theorem 5.1.2 or Theorem 2.3.3, will require that the class with $x/\log^2 x$ ideals must generate the class group. This will be ensured by using two conditions. These conditions are as follows:

1. None of the prime ideals thus obtained split in the Hilbert class field of the cubic or quadratic field. Therefore by Theorem 2.1.36, the class cannot be principal.

2. Assume that the class numbers of the cubic or quadratic fields are prime. This will ensure that any non-principal class is a generator.

Before we state the results, we introduce some notation. Let $\mathbf{K}_1, \mathbf{K}_2$ and $\mathbf{K}_3$ be number fields with Hilbert class fields $\mathbf{H}(\mathbf{K}_1), \mathbf{H}(\mathbf{K}_2)$ and $\mathbf{H}(\mathbf{K}_3)$ respectively, all of which are abelian over $\mathbb{Q}$. Also let $f_1, f_2$ and $f_3$ be their conductors, i.e. $\mathbb{Q}(\zeta_{f_1}), \mathbb{Q}(\zeta_{f_2})$ and $\mathbb{Q}(\zeta_{f_3})$ be the smallest cyclotomic fields containing $\mathbf{H}(\mathbf{K}_1), \mathbf{H}(\mathbf{K}_2)$ and $\mathbf{H}(\mathbf{K}_3)$ respectively. Here $\zeta_{f_1}, \zeta_{f_2}$ and $\zeta_{f_3}$ are primitive $f_1, f_2$ and $f_3$th roots of unity respectively. Set $f$ to be the least common multiple of $16, f_1, f_2$ and $f_3$ if $\mathbf{K}_1, \mathbf{K}_2, \mathbf{K}_3$ are three real quadratic fields, the least common multiple of $16, f_1$ and $f_2$ if $\mathbf{K}_1, \mathbf{K}_2$ are two real quadratic fields or the least common multiple of $16, f_1$ and $f_2$ if $\mathbf{K}_1, \mathbf{K}_2$ are real cubic fields. Further put $\mathbf{F} := \mathbb{Q}(\zeta_f)$, where $\zeta_f$ is a primitive $f$th root of unity. We will now state the main results which have been proved in this chapter.

**Theorem 5.1.3.** *Let $\mathbf{K}_1, \mathbf{K}_2$ be distinct real cubic fields with prime class numbers and $\mathbf{H}(\mathbf{K}_1), \mathbf{H}(\mathbf{K}_2), \mathbf{F}$, $f$ be as above. Also let $G$ be the Galois group of $\mathbf{F}$ over $\mathbf{K}_1\mathbf{K}_2$, $G_\ell$ be the Galois group of $\mathbf{F}$ over $\mathbb{Q}(\zeta_\ell)$, where either $\ell$ is an odd prime dividing $f$ or $\ell = 4$ and $Gal(\mathbf{F}/\mathbf{H}(\mathbf{K}_i))$ be the Galois group of $\mathbf{F}/\mathbf{H}(\mathbf{K}_i)$ for $i = 1, 2$. If*

$$G \not\subset \bigcup_{\ell} G_\ell \bigcup \ Gal(\mathbf{F}/\mathbf{H}(\mathbf{K}_1)) \bigcup \ Gal(\mathbf{F}/\mathbf{H}(\mathbf{K}_2)),$$

*then at least one of the $\mathbf{K}_i$ $(i = 1, 2)$ has a Euclidean ideal class.*

We also have an analogous result in the quadratic case.

**Theorem 5.1.4.** *Let $\mathbf{K}_1, \mathbf{K}_2$ and $\mathbf{K}_3$ be distinct real quadratic fields with prime class numbers and $\mathbf{H}(\mathbf{K}_1)$, $\mathbf{H}(\mathbf{K}_2)$, $\mathbf{H}(\mathbf{K}_3), \mathbf{F}$, $f$ be as above. Also let $G$ be the*

*Galois group of* $\mathbf{F}$ *over* $\mathbf{K}_1\mathbf{K}_2\mathbf{K}_3$*,* $G_\ell$ *be the Galois group of* $\mathbf{F}$ *over* $\mathbb{Q}(\zeta_\ell)$*, where either* $\ell$ *is an odd prime dividing* $f$ *or* $\ell = 4$ *and* $Gal(\mathbf{F}/\mathbf{H}(\mathbf{K}_i))$ *be the Galois group of* $\mathbf{F}/\mathbf{H}(\mathbf{K}_i)$ *for* $i = 1, 2, 3$*. If*

$$G \not\subset \bigcup_{\ell} G_\ell \bigcup \ Gal(\mathbf{F}/\mathbf{H}(\mathbf{K}_1)) \bigcup \ Gal(\mathbf{F}/\mathbf{H}(\mathbf{K}_2)) \bigcup \ Gal(\mathbf{F}/\mathbf{H}(\mathbf{K}_3)),$$

*then at least one of the* $\mathbf{K}_i$ $(i = 1, 2, 3)$ *has a Euclidean ideal class.*

Now if we assume the Elliott and Halberstam conjecture, we can strengthen Theorem 5.1.4 in the following manner.

**Theorem 5.1.5.** *Let* $\mathbf{K}_1$ *and* $\mathbf{K}_2$ *be distinct real quadratic fields with prime class numbers and* $\mathbf{H}(\mathbf{K}_1)$*,* $\mathbf{H}(\mathbf{K}_2), \mathbf{F}$ *and* $f$ *be as above. Also let* $G$ *be the Galois group of* $\mathbf{F}$ *over* $\mathbf{K}_1\mathbf{K}_2$*,* $G_\ell$ *be the Galois group of* $\mathbf{F}$ *over* $\mathbb{Q}(\zeta_\ell)$*, where either* $\ell$ *is an odd prime dividing* $f$ *or* $\ell = 4$ *and* $Gal(\mathbf{F}/\mathbf{H}(\mathbf{K}_i))$ *be the Galois group of* $\mathbf{F}/\mathbf{H}(\mathbf{K}_i)$ *for* $i = 1, 2$*. If*

$$G \not\subset \bigcup_{\ell} G_\ell \bigcup \ Gal(\mathbf{F}/\mathbf{H}(\mathbf{K}_1)) \bigcup \ Gal(\mathbf{F}/\mathbf{H}(\mathbf{K}_2)),$$

*then at least one of the* $\mathbf{K}_i$ $(i = 1, 2)$ *has a Euclidean ideal class provided the Elliott and Halberstam conjecture holds.*

In the next section we begin with a generalisation of Theorem 5.1.2 required for our proof.

## 5.2 Generalisation of Theorem 5.1.2

In this section we prove a sequential variant of the criterion given by Graves in [13]. This criterion can be thought of as a generalization of Narkiewicz's result (see page 338, Lemma 2 of [31]).

**Theorem 5.2.1.** *Suppose that $\mathbf{K}$ is a number field with unit rank at least one and its class group $Cl_{\mathbf{K}} = \langle [\mathfrak{a}] \rangle$. If there exists an unbounded increasing sequence $\{x_n\}_{n\in\mathbb{N}}$ such that*

$$\left|\{\mathfrak{p} : \mathfrak{p} \textit{ prime ideal}, \ [\mathfrak{p}] = [\mathfrak{a}], \ \mathfrak{N}(\mathfrak{p}) \le x_n, \ \mathcal{O}_{\mathbf{K}}^{\times} \to (\mathcal{O}_{\mathbf{K}}/\mathfrak{p})^{\times} \textit{ is surjective}\}\right| \gg \frac{x_n}{\log^2 x_n} ,$$

*then $[\mathfrak{a}]$ is a Euclidean ideal class.*

*Proof.* We will apply Theorem 2.3.2 to prove Theorem 5.2.1. Since every ideal class $[\mathfrak{a}]$ contains infinitely many prime ideals, to show that $[\mathfrak{a}]$ is a Euclidean ideal class, it is sufficient to show that any prime ideal in $[\mathfrak{a}]$ is a Euclidean ideal. From now onwards, we shall assume that $\mathfrak{a}$ is a prime ideal.

For $i \in \mathbb{N}$, let $B_{i,\mathfrak{a}}$ and $B_{\mathfrak{a}}$ be as in Chapter 2 (Theorem 2.3.2). In order to complete the proof of Theorem 5.2.1, we need to show that all prime ideals of $\mathcal{O}_{\mathbf{K}}$ are in $B_{\mathfrak{a}}$. We start with the following definition. For $i \in \mathbb{N}$, let $B_{i,\mathfrak{a}}(X) := \{\mathfrak{p} \in B_{i,\mathfrak{a}} : \mathfrak{N}(\mathfrak{p}) \le X\}$. We claim that for any $i \ge 1$ and for any prime ideal $\mathfrak{p}$ of $\mathcal{O}_{\mathbf{K}}$,

$$\text{if} \quad \mathfrak{p} \in [\mathfrak{a}^{i+2}], \quad \text{then} \quad \mathfrak{p} \in B_{i+2,\mathfrak{a}}. \tag{5.2.1}$$

We will prove this claim by induction on $i$. Set

$$\begin{aligned} A := B_{1,\mathfrak{a}}(x_n^2) \setminus B_{0,\mathfrak{a}}, \qquad W &:= \{\mathfrak{p} : \mathfrak{p} \in [\mathfrak{a}^2]\} \setminus B_{2,\mathfrak{a}} \\ \text{and} \quad W(x_n) &:= \{\mathfrak{p} : \mathfrak{p} \in [\mathfrak{a}^2] \ , \ \mathfrak{N}(\mathfrak{p}) \le x_n\} \setminus B_{2,\mathfrak{a}}(x_n). \end{aligned}$$

By given hypothesis, we have $|B_{1,\mathfrak{a}}(x_n^2)| \gg \frac{x_n^2}{\log^2(x_n^2)}$. Let $\lambda(\mathfrak{p}, \mathfrak{a}, A)$ be as in Equation (2.3.2). Then applying Lemma 2.3.10, we get

$$\sum_{p\in W(x_n)} \frac{\lambda(\mathfrak{p}, \mathfrak{a}, A)}{\mathfrak{N}(\mathfrak{p})} \ll \frac{x_n^2}{|A|} \ll \frac{x_n^2}{\frac{x_n^2}{\log^2(x_n^2)}} \ll \log^2 x_n.$$

If $\mathfrak{p} \in W$, then there exists an $x \in \mathfrak{p}^{-1}\mathfrak{a} \backslash \mathfrak{a}$ such that $\mathfrak{a}^{-1}\mathfrak{b}(x-q) \notin B_{1,\mathfrak{a}}$, for all $q \in \mathfrak{a}$. This implies that $Z_A(x, \mathfrak{p}, \mathfrak{a}) = 0$ for $Z_A(x, \mathfrak{p}, \mathfrak{a})$ be as defined in Equation (2.3.1). Therefore for any unit $u$ of $\mathcal{O}_{\mathbf{K}}$, we have

$$\mathfrak{a}^{-1}\mathfrak{b}(ux - q') \notin B_{1,\mathfrak{a}},$$

for all $q' \in \mathfrak{a}$. This implies that for any unit $u \in \mathcal{O}_{\mathbf{K}}^{\times}$, one has $Z_A(ux, \mathfrak{p}, \mathfrak{a}) = 0$. Now suppose that $u_1, u_2 \in \mathcal{O}_{\mathbf{K}}^{\times}$. We now show that if $u_1$ and $u_2$ are distinct modulo $\mathfrak{p}$, then $xu_1$ and $xu_2$ are distinct elements in $\mathfrak{p}^{-1}\mathfrak{a}/\mathfrak{a}$. Let $h_{\mathcal{O}_{\mathbf{K}}}$ be the order of $Cl_{\mathcal{O}_{\mathbf{K}}}$. Then $\mathfrak{p}\mathfrak{a}^{\left(h_{\mathcal{O}_{\mathbf{K}}}-2\right)}$ is a principal ideal as $\mathfrak{p} \in W \subset [\mathfrak{a}^2]$. Let $x_{\mathfrak{p}}$ be a generator of $\mathfrak{p}\mathfrak{a}^{\left(h_{\mathcal{O}_{\mathbf{K}}}-2\right)}$. For the rest of this proof, we will denote $h_{\mathcal{O}_{\mathbf{K}}}$ by $h$ for ease of notation. Consider the map

$$\begin{aligned} \psi_1 : \mathfrak{p}^{-1}\mathfrak{a}/\mathfrak{a} &\rightarrow \mathfrak{a}^{h-1}/\mathfrak{a}^{h-1}\mathfrak{p} \\ \alpha \bmod \mathfrak{a} &\mapsto \alpha x_{\mathfrak{p}} \bmod \mathfrak{a}^{h-1}\mathfrak{p}, \end{aligned}$$

which is well defined since $x_{\mathfrak{p}}\mathfrak{a} = \mathfrak{p}\mathfrak{a}^{h-2} \cdot \mathfrak{a} = \mathfrak{a}^{h-1}\mathfrak{p}$. Also consider the map

$$\begin{aligned} \psi_2 : \mathfrak{a}^{h-1}/\mathfrak{a}^{h-1}\mathfrak{p} &\rightarrow \mathcal{O}_{\mathbf{K}}/\mathfrak{p} \\ \beta \bmod \mathfrak{a}^{h-1}\mathfrak{p} &\mapsto \beta \bmod \mathfrak{p}, \end{aligned}$$

which is well defined since $\mathfrak{a}$ is an integral ideal, and hence $\mathfrak{a}^{h-1}\mathfrak{p} \subset \mathfrak{p}$. We know by Lemma 2.3.8 that $\psi_1$ is an isomorphism. Also it is easy to check that $\psi_2$ is an injective group homomorphism as $\mathfrak{a}$ is a prime ideal which is co-prime to $\mathfrak{p}$. Since $x \in \mathfrak{p}^{-1}\mathfrak{a} \setminus \mathfrak{a}$, we see that $x_{\mathfrak{p}}x \bmod \mathfrak{p}$ is a non-zero element in $\mathcal{O}_{\mathbf{K}}/\mathfrak{p}$, i.e. $x_{\mathfrak{p}}x \notin \mathfrak{p}$. This implies that $x_{\mathfrak{p}}x(u_1 - u_2) \in \mathfrak{p}$ if and only if $u_1 - u_2 \in \mathfrak{p}$, as required. Let

$$l_{\mathfrak{p}} := |\{\alpha \bmod \mathfrak{p} : \alpha \in \mathcal{O}_{\mathbf{K}}^{\times}\}|.$$

Thus if $\mathfrak{p} \in W$, then $\lambda(\mathfrak{p}, \mathfrak{a}, A) \geq l_{\mathfrak{p}}$. Therefore

$$\begin{aligned}\log^2 x_n \gg \sum_{\mathfrak{p} \in W(x_n)} \frac{\lambda(\mathfrak{p}, \mathfrak{a}, A)}{\mathfrak{N}(\mathfrak{p})} &\geq \sum_{\mathfrak{p} \in W(x_n)} \frac{l_{\mathfrak{p}}}{\mathfrak{N}(\mathfrak{p})} \geq \sum_{\substack{\mathfrak{p} \in W(x_n) \\ l_{\mathfrak{p}} \geq \mathfrak{N}(\mathfrak{p})^{\frac{1}{2}-\epsilon}}} \frac{1}{\mathfrak{N}(\mathfrak{p})^{\frac{1}{2}+\epsilon}} \\ &> \frac{|\{\mathfrak{p} \in W(x_n) \ : \ l_{\mathfrak{p}} > \mathfrak{N}(\mathfrak{p})^{\frac{1}{2}-\epsilon}\}|}{x_n^{\frac{1}{2}+\epsilon}}.\end{aligned}$$

Multiplying both sides by $x_n^{\frac{1}{2}+\epsilon}$, we get that

$$|\{\mathfrak{p} \in W(x_n) : l_{\mathfrak{p}} > \mathfrak{N}(\mathfrak{p})^{\frac{1}{2}-\epsilon}\}| \ = \ o\left(\frac{x_n}{\log x_n}\right).$$

On the other hand, by the Lemma 2.3.4, we have

$$|\{\mathfrak{p} \in W(x_n) : l_{\mathfrak{p}} \leq \mathfrak{N}(\mathfrak{p})^{\frac{1}{2}-\epsilon}\}| \ll x_n^{1-2\epsilon}.$$

Hence

$$|W(x_n)| \ = \ o\left(\frac{x_n}{\log x_n}\right). \tag{5.2.2}$$

Now for any $\mathfrak{p} \in [\mathfrak{a}^3]$ and any $x \in \mathfrak{p}^{-1}\mathfrak{a} \backslash \mathfrak{a}$, we have $(x) = \mathfrak{p}^{-1}\mathfrak{a}\mathfrak{a}_1$ for some integral ideal $\mathfrak{a}_1$. Note that $\mathfrak{a}_1 \not\subset \mathfrak{p}$ as $x \notin \mathfrak{a}$ and hence

$$(x) + \mathfrak{a} = \mathfrak{p}^{-1}\mathfrak{a}(\mathfrak{p} + \mathfrak{a}_1) = \mathfrak{p}^{-1}\mathfrak{a}.$$

Then by Theorem 2.3.7, the set $\overline{W}$ of prime ideals $\mathfrak{q}$ in $\mathcal{O}_{\mathbf{K}}$ such that

$$\mathfrak{q} = (x - y)\mathfrak{p}\mathfrak{a}^{-1}$$

for some $y \in \mathfrak{a}$ has positive density. Note that $\overline{W} \subset [\mathfrak{a}^2]$ and it has positive density. Since by Equation (5.2.2), $W$ has zero density, it follows that $\overline{W}$ cannot be contained in $W$. Therefore there exists $y_0 \in \mathfrak{a}$ such that

$$\mathfrak{q}_0 = (x - y_0)\mathfrak{p}\mathfrak{a}^{-1} \in B_{2,\mathfrak{a}}.$$

This implies that $\mathfrak{p} \in B_{3,\mathfrak{a}}$ and hence by definition all prime ideals $\mathfrak{p}$ for which $[\mathfrak{p}] = [\mathfrak{a}^3]$ are in $B_{3,\mathfrak{a}}$. This proves the claim (5.2.1) for $i = 1$. For the induction hypothesis, suppose that the claim is true for $i = m$. This implies that if $\mathfrak{p} \in [\mathfrak{a}^{m+2}]$ then $\mathfrak{p} \in B_{m+2,\mathfrak{a}}$. Now let $\mathfrak{p} \in [\mathfrak{a}^{m+3}]$. Then arguing exactly as before we see that for any $x \in \mathfrak{p}^{-1}\mathfrak{a} \setminus \mathfrak{a}$, we have $(x) + \mathfrak{a} = \mathfrak{p}^{-1}\mathfrak{a}$. Now by Theorem 2.3.7, there exists a prime ideal $\mathfrak{q}$ such that

$$\mathfrak{q} = (x - y)\mathfrak{p}\mathfrak{a}^{-1}$$

for some $y \in \mathfrak{a}$. Since $\mathfrak{p} \in [\mathfrak{a}^{m+3}]$, we have $\mathfrak{q} \in [\mathfrak{a}^{m+2}]$. Then by induction hypothesis, we have $\mathfrak{q} \in B_{m+2,\mathfrak{a}}$ and hence by definition $\mathfrak{p} \in B_{m+3,\mathfrak{a}}$, as required. This implies that every prime ideal of $\mathcal{O}_{\mathbf{K}}$ is in $B_{h+2,\mathfrak{a}}$ and hence in $B_{\mathfrak{a}}$. Thus $\mathfrak{a}$ is a Euclidean ideal. □

With the above generalisation in hand, we can now use Lemma 2.3.5 to prove Theorem 5.1.3 and Theorem 5.1.4.

## 5.3 Proof of Theorem 5.1.3 and Theorem 5.1.4

In this section, we give a proof for Theorem 5.1.3 and then outline a proof for Theorem 5.1.4 as the arguments are similar.

### 5.3.1 Proof of Theorem 5.1.3

We start by proving some lemmas which are required to prove Theorem 5.1.3. Throughout this subsection, let $\mathbf{K}_1$ and $\mathbf{K}_2$ be abelian cubic fields with Hilbert class fields $\mathbf{H}(\mathbf{K}_1)$ and $\mathbf{H}(\mathbf{K}_2)$, both of which are abelian over $\mathbb{Q}$. Also let $f_1$ and $f_2$ be their conductors. Set $f$ to be the least common multiple of $16, f_1, f_2$ and $\mathbf{F} := \mathbb{Q}(\zeta_f)$, where $\zeta_f$ is a primitive $f$-th root of unity.

**Lemma 5.3.1.** *Suppose that the Galois group $G$ of $\mathbf{F}$ over $\mathbf{K}_1\mathbf{K}_2$ satisfies the hypothesis of Theorem 5.1.3. Then there exists a co-prime residue class modulo $f$, say $t \bmod f$, such that any rational prime that belongs to this residue class splits completely in $\mathbf{K}_1\mathbf{K}_2$ but does not split completely in $\mathbf{H}(\mathbf{K}_1)$ and $\mathbf{H}(\mathbf{K}_2)$. Further, there exist $a, b \in (\frac{1}{4}, \frac{1}{2})$ such that for any $X, \epsilon > 0$, we have $|J_\epsilon(X)| \gg \frac{X}{\log^2(X)}$, where*

$$\begin{aligned} J_\epsilon(X) \ := \ \Big\{ & p \equiv t \bmod f \ : \ p \textit{ rational prime, } p \in (X^{1-\epsilon}, X) \textit{ such that} \\ & \frac{p-1}{2} \textit{ is either a rational prime or a product of rational} \\ & \textit{primes } q_1 q_2 \textit{ with } X^a < q_1 < X^b \Big\}. \end{aligned}$$

*Proof.* By the given hypothesis, we have

$$G \not\subset \bigcup_\ell G_\ell \bigcup \mathrm{Gal}(\mathbf{F}/\mathbf{H}(\mathbf{K}_1)) \bigcup \mathrm{Gal}(\mathbf{F}/\mathbf{H}(\mathbf{K}_2)).$$

This implies that there exists a co-prime residue class modulo $f$, say $t \bmod f$, such that $((t-1)/2, f) = 1$ and every rational prime in this class splits completely in $\mathbf{K}_1\mathbf{K}_2$ but not in $\mathbf{H}(K_1)$ and $\mathbf{H}(\mathbf{K}_2)$.

We can now apply Lemma 2.2.7 for $u = t$ and $v = f$, which gives us that for some $a, b \in (\frac{1}{4}, \frac{1}{2})$ and any $\epsilon > 0$,

$$|J_\epsilon(X)| \gg \frac{X}{\log^2 X}.$$

This completes the proof of the lemma. □

Next let $\mathbf{K} = \mathbf{K}_1\mathbf{K}_2$ and $t \bmod f$ be as in Lemma 5.3.1. Since we know that

$(t, f) = 1$ and $((t-1)/2, f) = 1$, it follows that $t \equiv 3 \bmod 4$. For $a$ and $b$ as in the previous lemma, choose $\epsilon$ such that $a < \frac{b}{1-\epsilon} < \frac{1}{2}$. Consider the set

$$\begin{aligned} M_\epsilon \ := \ \{\mathfrak{p} \ : \ & \mathfrak{p} \text{ is a prime ideal, } \mathfrak{N}(\mathfrak{p}) = p \text{ rational prime }, \ p \equiv t \bmod f, \\ & \frac{p-1}{2} \text{ is either a rational prime or a product of rational primes} \\ & q_1 q_2 \text{ with } p^a < q_1 < p^{\frac{b}{1-\epsilon}}\} \end{aligned}$$

and also the set $M_\epsilon(X) \ := \ \{\mathfrak{p} \in M_\epsilon : \mathfrak{N}(\mathfrak{p}) \leq X\}$ for any real number $X > 0$. With this notation, we have the following lemma.

**Lemma 5.3.2.** *Let* $\mathbf{K}$ *be as above and* $e_1, e_2$, $e_3$ *be multiplicatively independent elements in* $\mathcal{O}_{\mathbf{K}}^{\times}$. *Then for some* $i \in \{1, 2, 3\}$, *either* $e_i$ *or* $-e_i$ *is a primitive root mod* $\mathfrak{p}$ *for infinitely many ideals in the set* $M_\epsilon$. *Let this set of prime ideals be called* $V$ *and let* $V(X)$ *denote the set of elements in* $V$ *of norm less than or equal to* $X$. *Then there exists an increasing unbounded sequence* $\{x_n\}_{n \in \mathbb{N}}$ *such that*

$$|V(x_n)| \gg \frac{x_n}{\log^2 x_n}.$$

*Proof.* For any real number $X > 0$, let $J_\epsilon(X)$ be as in Lemma 5.3.1. Since for every rational prime $p \in J_\epsilon$, there exists a prime ideal $\mathfrak{p} \in M_\epsilon$ such that $\mathfrak{N}(\mathfrak{p}) = p$ and by Lemma 5.3.1, we know that

$$|J_\epsilon(X)| \gg X/\log^2 X.$$

It follows that

$$|M_\epsilon(X)| \gg \frac{X}{\log^2 X}. \tag{5.3.1}$$

For any multiplicatively independent elements $e_1, e_2$ and $e_3$ in $\mathcal{O}_{\mathbf{K}}^{\times}$, we can partition the set $M_\epsilon = \cup_{j=1}^{8} M_j$, where each $M_j$ correspond to a tuple $(c_1, c_2, c_3)$ with entries in $\{\pm 1\}$ such that

$$\left(\frac{e_i}{\mathfrak{p}}\right) = -c_i$$

for all $\mathfrak{p} \in M_j$. See page 394 of [30] for the definition of second power residue symbol $\left(\frac{e_i}{\mathfrak{p}}\right)$. We now claim that there exists an increasing unbounded sequence $\{x_n\}_{n\in\mathbb{N}}$ and $1 \leq j_0 \leq 8$ such that

$$|M_{j_0}(x_n)| \gg x_n/\log^2 x_n.$$

Suppose our claim is not true, i.e. none of the $M_j$ have such a sequence. Then

$$\limsup_{X\to\infty} |M_j(X)|/(X/\log^2 X) = 0.$$

However since

$$\liminf_{X\to\infty} |M_j(X)|/(X/\log^2 X) = 0,$$

we have

$$|M_j(X)| = o\left(\frac{X}{\log^2 X}\right),$$

for all $1 \leq j \leq 8$. This implies that

$$|M_\epsilon(X)| = o\left(\frac{X}{\log^2 X}\right),$$

a contradiction to Equation (5.3.1). Since $t \equiv 3 \bmod 4$, any $\mathfrak{p} \in M_\epsilon$ has the property that $\left(\frac{-1}{\mathfrak{p}}\right) = -1$. Now by applying Lemma 2.3.5 with $T = M_{j_0}$ and noting that for any $i \in \{1, 2, 3\}$, the elements $c_i e_i$ are quadratic non-residues modulo any prime ideal $\mathfrak{p} \in M_{j_0}$, we get our lemma. □

**Remark 5.3.3.** *Note that $\pm 1$ cannot be a subset of a multiplicatively independent set. Also both $e_i \bmod \mathfrak{p}$ and $-e_i \bmod \mathfrak{p}$ for any $\mathfrak{p} \in M_\epsilon$ cannot simultaneously be quadratic residues as $\left(\frac{-1}{\mathfrak{p}}\right) = -1$. Therefore the usual exclusion of $\pm 1$ and perfect squares for Artin's primitive root conjecture does not appear in Lemma 5.3.2.*

We now complete the proof of Theorem 5.1.3. Since $\mathbf{K}_1$ and $\mathbf{K}_2$ are real cubic, their compositum $\mathbf{K}$ contains three multiplicatively independent units, say $\epsilon_1, \epsilon_2$ and $\epsilon_3$. Let $V$ be as in Lemma 5.3.2 and $\eta$ be one of the elements $\pm\epsilon_1, \pm\epsilon_2, \pm\epsilon_3$ which generates $(\mathcal{O}_{\mathbf{K}}/\mathfrak{p})^\times$ for all $\mathfrak{p} \in V$. Then $\eta \in \mathbf{K}_s$, where $s \in \{1, 2\}$ and by Lemma 5.3.2, we have a sequence $\{x_n\}_{n\in\mathbb{N}}$ such that

$$|V(x_n)| \geq cx_n/\log^2 x_n.$$

Since every $\mathfrak{p} \in V$ has degree 1, $\eta$ generates $(\mathcal{O}_{\mathbf{K}_s}/\mathfrak{r})^\times$ where $\mathfrak{r} = \mathfrak{p} \cap K_s$. Since there are only finitely many ideal classes, arguing as in Lemma 5.3.2, there exists some ideal class $[\mathfrak{f}]$ in the class group of $\mathbf{K}_s$ so that

$$|\{\mathfrak{q} \cap \mathbf{K}_s \in [\mathfrak{f}] \ : \ \mathfrak{q} \in V, \ \mathfrak{N}(\mathfrak{q} \cap \mathbf{K}_s) \leq y_n\}| \gg \frac{y_n}{h_{\mathcal{O}_{\mathbf{K}_s}} \log^2 y_n},$$

for a subsequence $\{y_n\}_{n\in\mathbb{N}}$ of $\{x_n\}_{n\in\mathbb{N}}$. Here $h_{\mathcal{O}_{\mathbf{K}_s}}$ denotes the class number of $\mathcal{O}_{\mathbf{K}_s}$. Since $V \subset M_\epsilon$, our choice of $t$ (see Lemma 5.3.1) ensures that none of the elements of $V$ lie above any ideal in the trivial class of $\mathbf{K}_s$. Since $h_{\mathcal{O}_{\mathbf{K}_s}}$ is prime, the ideal class $[\mathfrak{f}]$ must generate the ideal class group. Therefore by Theorem 5.2.1, we see that $[\mathfrak{f}]$ is a Euclidean ideal class. This completes the proof of Theorem 5.1.3.

### 5.3.2 Proof of Theorem 5.1.4

In this subsection, we outline the proof of Theorem 5.1.4. Throughout this subsection, let $\mathbf{K}_1, \mathbf{K}_2$ and $\mathbf{K}_3$ be real quadratic fields with abelian Hilbert class fields $\mathbf{H}(\mathbf{K}_1), \mathbf{H}(\mathbf{K}_2)$ and $\mathbf{H}(\mathbf{K}_3)$ respectively. Also let $f_1, f_2$ and $f_3$ be their conductors. Set $f$ to be the least common multiple of $16, f_1, f_2, f_3$ and $\mathbf{F} := \mathbb{Q}(\zeta_f)$, where $\zeta_f$ is a primitive $f$-th root of unity. Also set $\mathbf{K} = \mathbf{K}_1\mathbf{K}_2\mathbf{K}_3$. For the sake of completeness, we now state two lemmas required to prove Theorem 5.1.4. Their proofs follow by arguing exactly as in Lemma 5.3.1 and Lemma 5.3.2.

**Lemma 5.3.4.** *Suppose that the Galois group $G$ of $\mathbf{F}$ over $\mathbf{K}$ satisfies the hypothesis of Theorem 5.1.4. Then there exists a co-prime residue class modulo $f$, say $t \bmod f$, such that any rational prime that belongs to this residue class splits completely in $\mathbf{K}$ but does not split completely in $\mathbf{H}(\mathbf{K}_1), \mathbf{H}(\mathbf{K}_2)$ and $\mathbf{H}(\mathbf{K}_3)$. Further, there exist $a, b \in (\frac{1}{4}, \frac{1}{2})$ such that for any $X, \epsilon > 0$, we have $|J_\epsilon(X)| \ll \frac{X}{\log^2 X}$, where*

$$\begin{aligned} J_\epsilon(X) \;&:=\; \Big\{p \equiv t \bmod f \;:\; p \in \mathbb{N},\ p \textit{ prime, } p \in (X^{1-\epsilon}, X) \textit{ such that} \\ &\quad\ \frac{p-1}{2} \textit{ is either a rational prime or a product of rational} \\ &\quad\ \textit{primes } q_1 q_2 \textit{ with } X^a < q_1 < X^b\Big\}. \end{aligned}$$

We modify the definition of $M_\epsilon$ as follows. For $a$ and $b$ as in Lemma 5.3.4, choose $\epsilon > 0$ such that $a < \frac{b}{1-\epsilon} < \frac{1}{2}$. Consider the sets

$$\begin{aligned} M_\epsilon \;&:=\; \{\mathfrak{p} \;:\; \mathfrak{p} \text{ is a prime ideal, } \mathfrak{N}(\mathfrak{p}) = p \in \mathbb{N},\ p \text{ prime },\ p \equiv t \bmod f, \\ &\quad\ \frac{p-1}{2} \text{ is either a rational prime or a product of rational primes} \\ &\quad\ q_1 q_2 \text{ with } p^a < q_1 < p^{\frac{b}{1-\epsilon}}\} \end{aligned}$$

and $M_\epsilon(X) \;:=\; \{\mathfrak{p} \in M_\epsilon : \mathfrak{N}(\mathfrak{p}) \leq X\}$ for any real number $X > 0$. We have the following lemma.

**Lemma 5.3.5.** *Let $e_1$, $e_2$ and $e_3$ be multiplicatively independent elements in $\mathcal{O}_{\mathbf{K}}^\times$. Then for some $i \in \{1, 2, 3\}$, either $e_i$ or $-e_i$ is a primitive root mod $\mathfrak{p}$ for infinitely many ideals in the set $M_\epsilon$. Let this set of prime ideals be called $V$ and let $V(X)$ denote the set of elements in $V$ of norm less than or equal to $X$. Then there exists an increasing unbounded sequence $\{x_n\}_{n \in \mathbb{N}}$ such that*

$$|V(x_n)| \gg \frac{x_n}{\log^2 x_n}.$$

This completes the proof of Theorem 5.1.4. In the next section of this chapter, we investigate the implications of the Elliott and Halberstam conjecture on the problem of finding Euclidean ideal classes in real quadratic fields with cyclic class groups.

## 5.4 Consequences of Elliott and Halberstam conjecture

As seen in chapter 4, we would like to examine the improvements that can be obtained on Theorem 5.1.3 and Theorem 5.1.4, under the Elliott and Halberstam conjecture (Conjecture 2.2.6).

We first note the following improvement of Lemma 2.3.5.

**Lemma 5.4.1.** *Let $a_1$ and $a_2$ be multiplicatively independent elements of $\mathbf{K}^\times$, $T$ be a set of prime ideals of degree $1$ in $\mathbf{K}$ and $\mathfrak{N}(\mathfrak{p})$ denotes the absolute norm of a prime ideal $\mathfrak{p}$ of $\mathcal{O}_{\mathbf{K}}$. Suppose that $T$ has the following properties,*

1. *there exists a constant $c > 0$ and an unbounded increasing sequence $\{x_n\}_{n\in\mathbb{N}}$ such that*
$$|T(x_n) := \{\mathfrak{p} \in T \ : \ \mathfrak{N}(\mathfrak{p}) \leq x_n\}| \gg x_n/\log^2 x_n,$$

2. *there exist $\alpha < \beta$ in the open interval $(1/3, 1/2)$ such that if $\mathfrak{p}$ is an element of $T$ and $p = \mathfrak{N}(\mathfrak{p})$, then $(p-1)/2$ is either a prime $q$ or a product of primes $q_1q_2$, with $p^\alpha < q_1 < p^\beta$,*

3. *the numbers $a_1$ and $a_2$ are both quadratic non-residues with respect to every prime in $T$.*

*Then for any $c > \epsilon > 0$, there exists a subsequence $\{y_m\}_{m\in\mathbb{N}}$ of $\{x_n\}_{n\in\mathbb{N}}$ such that one of the $a_i$s is a primitive root for at least $(c-\epsilon)y_m/\log^2 y_m$ elements of $T(y_m)$.*

*Proof.* If the order of $a_1$ or $a_2$ is two in $(\mathcal{O}_{\mathbf{K}}/\mathfrak{p})^\times$ (the multiplicative group of units of $\mathcal{O}_{\mathbf{K}}/\mathfrak{p}$), then $a_i^2 - 1 \in \mathfrak{p}$ and hence there are only finitely many such prime ideals $\mathfrak{p}$ in $\mathcal{O}_{\mathbf{K}}$. Without loss of generality, we can assume that neither $a_1$ nor $a_2$ has order 2 in $(\mathcal{O}_{\mathbf{K}}/\mathfrak{p})^\times$ with $\mathfrak{N}(\mathfrak{p})$ sufficiently large.

From now onwards assume that $\mathfrak{p} \in T$ with $\mathfrak{N}(\mathfrak{p}) = p$ such that neither $a_1$ nor $a_2$ has order 2 in $(\mathcal{O}_{\mathbf{K}}/\mathfrak{p})^\times$. Also we shall denote the order of any element $a$ in $(\mathcal{O}_{\mathbf{K}}/\mathfrak{p})^\times$ by $o_{\mathfrak{p}}(a)$. By the given hypothesis, $p = 1+2q$ for a prime $q$ or $p = 1+2q_1q_2$, with $q_1, q_2$ primes such that $p^\alpha < q_1 < p^\beta$. If both $a_1$ and $a_2$ are not primitive roots modulo $\mathfrak{p}$, then they have order $q$ when $p-1 = 2q$ or they have order $q_1, q_2, 2q_1, 2q_2$, or $q_1q_2$ when $p-1 = 2q_1q_2$. Again by the hypothesis, $a_1, a_2$ are quadratic non-residues modulo $\mathfrak{p}$ and hence $o_{\mathfrak{p}}(a_1), o_{\mathfrak{p}}(a_2)$ must be divisible by 2. This implies that there are no primes $p$ with $p-1 = 2q$ for which both $a_1$ and $a_2$ are not primitive roots modulo $\mathfrak{p}$. When $p-1 = 2q_1q_2$ and both $a_1$ and $a_2$ are not primitive roots modulo $\mathfrak{p}$, then $o_{\mathfrak{p}}(a_1)$ is equal to $2q_1$ or $2q_2$ and same is true for $o_{\mathfrak{p}}(a_2)$. Now suppose that at least one of $o_{\mathfrak{p}}(a_i)$ $(i = 1,2)$ is equal to $2q_1$. Then for any $i = 1,2$, we have

$$|\{\mathfrak{p} \in T : \mathfrak{N}(\mathfrak{p}) \leq X,\ o_{\mathfrak{p}}(a_i) := e \leq 2X^\beta\}| \quad \leq \quad \sum_{e \leq 2X^\beta} |\{\mathfrak{p} \in T : \mathfrak{N}(\mathfrak{p}) \leq X,\ \mathfrak{p} | (a_i^e - 1)\}|,$$

where $\beta$ is as in the hypothesis. Taking norms, we get

$$\begin{aligned}
\sum_{e \leq 2X^\beta} |\{p \leq X \ : \ p | \mathfrak{N}(a_i^e - 1)\}| \quad &\ll \quad \sum_{e \leq 2X^\beta} \log |\mathfrak{N}(a_i^e - 1)|, \\
&= \quad \sum_{e \leq 2X^\beta} \log \left( \prod_\sigma |\sigma(a_i^e) - 1| \right), \\
&\ll \quad \sum_{e \leq 2X^\beta} \log \left( \prod_\sigma (|\sigma(a_i)| + 1)^e \right), \\
&\ll \quad \sum_{e \leq 2X^\beta} e \ll X^{2\beta} \ = \ o\left( \frac{X}{\log^2 X} \right).
\end{aligned}$$

Here, $\sigma$ varies over all the embeddings of $\mathbf{K}$ into $\mathbb{C}$. If both $o_{\mathfrak{p}}(a_1)$ and $o_{\mathfrak{p}}(a_2)$ are equal to $2q_2$, we claim that

$$|\{\mathfrak{p} \in T \ : \ \mathfrak{N}(\mathfrak{p}) \leq X, \ o_{\mathfrak{p}}(a_1) = 2q_2 = o_{\mathfrak{p}}(a_2)\}| \ = \ o\left(\frac{X}{\log^2 X}\right).$$

To prove this, we will show that there exists a set $S$ of tuples $(r, s) \in \mathbb{N} \times \mathbb{N}$ such that

$$\begin{aligned} & \{\mathfrak{p} \in T \ : \ \mathfrak{N}(\mathfrak{p}) \leq X, \ o_{\mathfrak{p}}(a_1) = 2q_2 = o_{\mathfrak{p}}(a_2)\} \\ (5.4.1) \qquad \subset \ & \{\mathfrak{p} \in T \ : \ \mathfrak{N}(\mathfrak{p}) := p \leq X, \ p|\mathfrak{N}(a_1^r a_2^s - 1) \text{ for some } (r, s) \in S\}. \end{aligned}$$

Consider the set

$$\tilde{S} := \ \{(r, s) \in \mathbb{N} \times \mathbb{N} \ : \ 0 \leq r, s \leq 2X^{(1-\alpha)/2}\}.$$

Note that when $o_{\mathfrak{p}}(a_1) = 2q_2 = o_{\mathfrak{p}}(a_2)$ for some $\mathfrak{p} \in T$, then $(a_1^r a_2^s)^{2q_2} \equiv 1 \bmod \mathfrak{p}$ for any $(r, s) \in \tilde{S}$. Since $|\tilde{S}|$ is $4X^{1-\alpha} \geq 4p^{1-\alpha} \geq 4q_2$ and the fact that the polynomial $Y^{2q_2} - 1$ over $\mathcal{O}_{\mathbf{K}}/\mathfrak{p}$ can have at most $2q_2$ roots, we have by the pigeonhole principle that there exists $(r, s) \in S$, where $S := \{(r, s) \in \mathbb{Z} \times \mathbb{Z} \ : \ (|r|, |s|) \in \tilde{S}\}$ such that $a_1^r a_2^s - 1 \in \mathfrak{p}$. Let the numerator of $a_1^r a_2^s - 1$ be $M_{r,s}$. Clearly $M_{r,s} \neq 0$ as $a_1$ and $a_2$ are multiplicatively independent. Then the number of prime divisors of the numerator $\mathfrak{N}(M_{r,s})$ is $\log|\mathfrak{N}(M_{r,s})| \ \ll \ X^{(1-\alpha)/2}$. Hence,

$$|\{p \leq X \ : \ p|\mathfrak{N}(M_{r,s}) \text{ for some } (r, s) \in S\}| \ \ll \ X^{1-\alpha} \times X^{(1-\alpha)/2} \ = \ o\left(\frac{X}{\log^2 X}\right),$$

as $\alpha > 1/3$. Thus

$$|\{\mathfrak{p} \in T \ : \ \mathfrak{N}(\mathfrak{p}) := p \leq X, \ p|\mathfrak{N}(a_1^r a_2^s - 1) \text{ for some } (r, s) \in S\}| \ = \ o\left(\frac{X}{\log^2 X}\right).$$

Therefore there exists a subsequence $\{y_m\}_{m \in \mathbb{N}}$ such that one of the $a_i$s is a primitive root for at least $(c - \epsilon)y_m/\log^2 y_m$ primes for any $\epsilon > 0$. □

We now complete the proof of Theorem 5.1.5.

*Proof.* Let $\mathbf{K} := \mathbf{K}_1\mathbf{K}_2$ be the compositum of the real quadratic fields $\mathbf{K}_1$ and $\mathbf{K}_2$ and let $f$ be the least common multiple of $16, f_1$ and $f_2$, where $f_1$ and $f_2$ denote the conductors of $\mathbf{K}_1$ and $\mathbf{K}_2$ respectively. By the hypothesis, there exists an element $b \bmod f$ in the Galois group of $\mathbb{Q}(\zeta_f)$ over $\mathbf{K}$ such that $((b-1)/2, f/2) = 1$. Since $16|f$, we have $b \equiv 3 \bmod 4$. Using the Theorem 4.4.1, it is easy to see that the set

$$\begin{aligned}\tilde{T}(X) \;&:=\; \{\ell \leq X : \ell \in \mathbb{N},\ \ell \text{ prime},\ \ell \equiv b \bmod f,\ \frac{\ell-1}{2} \text{ is either a rational prime} \\ &\qquad\qquad \text{or a product of rational primes } q_1q_2 \text{ with } X^{1/2-\delta} < q_1 < X^{1/2}\}\end{aligned}$$

has cardinality $\gg \frac{X}{\log^2 X}$ for any $\delta < 1/6$. If we set

$$T(X) \;:=\; \{\mathfrak{p} \subset \mathcal{O}_{\mathbf{K}} \;:\; \mathfrak{p} \text{ is a prime ideal of degree one }, \mathfrak{N}(\mathfrak{p}) \in \tilde{T}(X)\},$$

then we have $|T(X)| \gg \frac{X}{\log^2 X}$. Let $a_1 \in \mathbf{K}_1$ and $a_2 \in \mathbf{K}_2$ be two fundamental units. By arguing as in Theorem 5.3.2, it follows that there exists an increasing unbounded sequence $\{x_n\}_{n\in\mathbb{N}}$, and a choice of tuple $(c_1, c_2)$ with entries in $\{\pm 1\}$ such that

$$\left(\frac{a_i}{\mathfrak{p}}\right) = -c_i,$$

for at least $\gg x_n/\log^2 x_n$ primes in $T(x_n)$. Let the set of these primes be called $A_1(x_n)$. Since $b \equiv 3 \bmod 4$, each $c_ia_i$ is a quadratic non-residue modulo all primes in $A_1(x_n)$, $n \geq 1$. Now by applying Lemma 5.4.1, there exists $a \in \{\pm a_1, \pm a_2\}$ in $K_s$ for $s \in \{1, 2\}$ which is a primitive root for every element of a subset $V_1(x_n)$ of $A_1(x_n)$. Further there exists an unbounded increasing sequence $\{y_m\}_{m\in\mathbb{N}}$ such that

$$|V_1(y_m)| \;\gg\; \frac{y_m}{\log^2 y_m}.$$

Since $\mathfrak{p} \in V_1(y_m)$ is of degree one, $a$ generates $(\mathcal{O}_{\mathbf{K}_s}/\mathfrak{q})^\times$, where $\mathfrak{q} = \mathfrak{p} \cap \mathbf{K}_s$. Since there are only finitely many ideal classes in $\mathbf{K}_s$, by arguing as in Theorem 5.3.2, there exists an ideal class $[\mathfrak{f}]$ and a subsequence $\{z_r\}_{r\in\mathbb{N}}$ of $\{y_m\}_{m\in\mathbb{N}}$ such that

$$|\{\mathfrak{q}\cap\mathbf{K}_s\in[\mathfrak{f}]\ :\ \mathfrak{q}\in V_1(z_r)\}|\ \gg\ \frac{z_r}{\log^2 z_r}.$$

By the given hypothesis, none of the primes in $V_1(z_r)$ split completely in $\mathbf{H}(\mathbf{K}_s)$. Thus $[\mathfrak{f}]$ must generate the ideal class group $\mathbf{K}_s$. Therefore by Theorem 5.2.1, we see that $[\mathfrak{f}]$ is a Euclidean ideal class. □

With this we have covered the proofs of all the statements claimed in the introduction of this chapter. In the last and final section we would like to provide some concrete examples of fields for which our theorems are applicable.

## 5.5 Concluding remarks

In this section, we construct some explicit examples for which the hypotheses of our main theorems hold. We start with real quadratic fields.

**Corollary 5.5.1.** *Let $p_1, q_1, p_2, q_2, p_3, q_3$ be six distinct primes which are congruent to* $1 \bmod 4$. *For $j\in\{1,2,3\}$, if each $\mathbf{K}_j := \mathbb{Q}(\sqrt{p_jq_j})$ has class number* 2, *then at least one of them has a Euclidean ideal class.*

*Proof.* Since $p_j$ and $q_j$ are all congruent to $1 \bmod 4$, we note that the conductor of $\mathbf{K}_j$ is $p_jq_j$ for all $j\in\{1,2,3\}$. To see this, we first observe that if $\mathbb{Q}(\zeta_r)$ is the conductor, then $r$ must be a multiple of $p_j$ and $q_j$ since both of these numbers ramify in $\mathbf{K}_j$. However $\mathbb{Q}(\zeta_{p_jq_j})$ contains $\mathbb{Q}(\zeta_{p_j})$ and $\mathbb{Q}(\zeta_{q_j})$. Since both $p_j$ and $q_j$ are congruent to 1 mod 4, we have $\mathbb{Q}(\sqrt{p_j})$ and $\mathbb{Q}(\sqrt{q_j})$ are contained in $\mathbb{Q}(\zeta_{p_j})$ and $\mathbb{Q}(\zeta_{q_j})$ respectively. Therefore $\mathbb{Q}(\zeta_{p_jq_j})$ is the smallest cyclotomic field containing $\mathbf{K}_j$.

The next observation we would like to make is that $\mathbf{H}(\mathbf{K}_j) = \mathbb{Q}(\sqrt{p_j}, \sqrt{q_j})$.

Since the class number of the quadratic field $\mathbf{K}_j$ is two, degree of the extension $\mathbb{Q}(\sqrt{p_j}, \sqrt{q_j})$ over $\mathbb{Q}$ is four and both these fields are totally real, it suffices to show that $\mathbb{Q}(\sqrt{p_j}, \sqrt{q_j})$ is an unramified extension of $\mathbf{K}_j$. Consider the following diagram.

$$\begin{tikzcd}
 & \mathbb{Q}(\sqrt{p_j}, \sqrt{q_j}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{p_j}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{q_j}) \arrow[d, dash] & \mathbf{K}_j \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

The prime $p_j$ does not ramify in $\mathbb{Q}(\sqrt{q_j})$ and hence its ramification index in $\mathbb{Q}(\sqrt{p_j}, \sqrt{q_j})$ is 2. Similarly the ramification index of $q_j$ in $\mathbb{Q}(\sqrt{p_j}, \sqrt{q_j})$ is also 2. Note that the discriminant of $\mathbf{K}_j$ is equal to $p_j q_j$ (as $p_j, q_j$ are 1 mod 4) and hence both $p_j$ and $q_j$ ramify in $\mathbf{K}_j$. Since both $p_j$ and $q_j$ have ramification index 2 in $\mathbb{Q}(\sqrt{p_j}, \sqrt{q_j})$, the primes in $\mathbf{K}_j$ lying above $p_j$ and those above $q_j$ do not ramify in $\mathbb{Q}(\sqrt{p_j}, \sqrt{q_j})$. Thus $\mathbb{Q}(\sqrt{p_j}, \sqrt{q_j})$ is unramified over $\mathbf{K}_j$ as the discriminant of $\mathbb{Q}(\sqrt{p_j}, \sqrt{q_j})$ is $p_j^2 q_j^2$.

Note that $f = 16p_1p_2p_3q_1q_2q_3$ and $\mathbf{K} := \mathbb{Q}(\sqrt{p_1q_1}, \sqrt{p_2q_2}, \sqrt{p_3q_3})$ is the compositum of $\mathbf{K}_j$ for $j \in \{1, 2, 3\}$. We claim that there exists an element $\sigma$ in the Galois group of $\mathbb{Q}(\zeta_f)$ over $\mathbf{K}$ such that

$$\sigma(\iota) = -\iota, \quad \sigma(\sqrt{p_j}) = -\sqrt{p_j} \quad \text{and} \quad \sigma(\sqrt{q_j}) = -\sqrt{q_j}$$

for $j = 1, 2, 3$. Here $\iota \in \mathbb{C}$ is such that $\iota^2 = -1$. To see this, we first observe that since the discriminant of $\mathbb{Q}(\iota, \sqrt{p_2}, \cdots, \sqrt{q_3})$ is co-prime to $p_1$, $\sqrt{p_1}$ is not contained in $\mathbb{Q}(\iota, \sqrt{p_2}, \cdots, \sqrt{q_3})$. So there exists a Galois element in $\mathbb{Q}(\zeta_f)/\mathbb{Q}$ which takes $\sqrt{p_1}$ to $-\sqrt{p_1}$ while fixing the other six elements. The same argument can be applied to the other six elements. The composition of all these Galois isomorphisms will give us the required isomorphism $\sigma$. This isomorphism in fact belongs to the Galois group of $\mathbb{Q}(\zeta_f)$ over $\mathbf{K}$. Since $\sigma$ does not fix the unique quadratic subfield of $\mathbb{Q}(\zeta_\ell)$

for any odd prime $\ell | f$ or $\ell = 4$, it follows that $\sigma$ does not belong to the Galois group of $\mathbb{Q}(\zeta_f)$ over $\mathbb{Q}(\zeta_\ell)$ for all odd primes $\ell | f$ or $\ell = 4$. Also $\sigma$ does not belong to the Galois group of $\mathbb{Q}(\zeta_f)$ over $\mathbf{H}(K_j)$ for $j \in \{1, 2, 3\}$. This is because it does not fix the quadratic subfields $\mathbb{Q}(\sqrt{p_j})$ or $\mathbb{Q}(\sqrt{q_j})$ of $\mathbf{H}(K_j)$ for all $j \in \{1, 2, 3\}$. Therefore we can now apply Theorem 5.1.4 to this set of three real quadratic fields to conclude that at least one of them must have a Euclidean ideal class. □

Let $p_1 = 5$,$q_1 = 41$, $p_2 = 17$, $q_2 = 13$, $p_3 = 29$ and $q_3 = 37$ . Using SAGE we can show that the class numbers of $\mathbb{Q}(\sqrt{p_i q_i})$ are all 2. Then one of the fields $\mathbb{Q}(\sqrt{p_i q_i})$ has a Euclidean ideal class by Corollary 5.5.1. Arguing exactly as in Corollary 5.5.1 and using Theorem 5.1.5, we get the following corollary.

**Corollary 5.5.2.** *Let $p_1, q_1, p_2, q_2$ be distinct primes which are congruent to* 1 mod 4*. If $\mathbb{Q}(\sqrt{p_j q_j})$ for $j \in \{1, 2\}$ have class number* 2*, then at least one of them must contain a Euclidean ideal class provided the Elliott and Halberstam conjecture is true.*

To provide an example for the real Galois cubic fields, we consider the following construction. Let $p_1, q_1, p_2, q_2$ be four distinct primes which are congruent to 1 mod 12. Let $\mathbf{K}_1, \mathbf{K}_2, \mathbf{K}_3$, $\mathbf{K}_4$ denote the unique degree three subfields of $\mathbb{Q}(\zeta_{p_1}), \mathbb{Q}(\zeta_{q_1}), \mathbb{Q}(\zeta_{p_2})$ and $\mathbb{Q}(\zeta_{q_2})$, respectively. Consider a degree three subfield of $\mathbf{K}_1\mathbf{K}_2$ which is distinct from $\mathbf{K}_1$ and $\mathbf{K}_2$. This is possible since the Galois group of $\mathbf{K}_1\mathbf{K}_2$ over $\mathbb{Q}$ is $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ and this group contains more than two subgroups of order 3. Let us denote this field by $\mathbf{K}$. Similarly, we consider a degree three subfield of $\mathbf{K}_3\mathbf{K}_4$, distinct from $\mathbf{K}_3$ and $\mathbf{K}_4$. We denote it by $\tilde{\mathbf{K}}$.

**Corollary 5.5.3.** *If $\mathbf{K}$ and $\tilde{\mathbf{K}}$ have class number* 3*, then one of $\mathbf{K}$ or $\tilde{\mathbf{K}}$ must have a Euclidean ideal class.*

*Proof.* We note that $\mathbf{K}$ is not contained in $\mathbb{Q}(\zeta_{p_1})$ or $\mathbb{Q}(\zeta_{q_1})$, but it is contained in $\mathbb{Q}(\zeta_{p_1 q_1})$. Therefore, the conductor of $\mathbf{K}$ must be $p_1 q_1$. Similarly the conductor of

$\tilde{\mathbf{K}}$ is $p_2q_2$. If $\mathbf{K}$ and $\tilde{\mathbf{K}}$ have class number 3, then the Hilbert class field of $\mathbf{H}(\mathbf{K})$ of $\mathbf{K}$ and the Hilbert class field of $\mathbf{H}(\tilde{\mathbf{K}})$ of $\tilde{\mathbf{K}}$ are $\mathbf{K}_1\mathbf{K}_2$ and $\mathbf{K}_3\mathbf{K}_4$ respectively. This follows from an argument similar to that of Corollary 5.5.1 and the fact that the conductors of $\mathbf{K}$ and $\tilde{\mathbf{K}}$ are $p_1q_1$ and $p_2q_2$, respectively. Now let $\mathbf{K}_1 = \mathbb{Q}(\alpha_1)$ and $\mathbf{K}_3 = \mathbb{Q}(\tilde{\alpha_1})$. We first claim that $\alpha_1 \notin \mathbf{K}\tilde{\mathbf{K}}(\tilde{\alpha_1}, \iota, \sqrt{p_1}, \sqrt{q_1}, \sqrt{p_2}, \sqrt{q_2})$. Suppose not, then

$$\mathbf{K}\tilde{\mathbf{K}}(\alpha_1) \subset \mathbf{K}\tilde{\mathbf{K}}(\tilde{\alpha_1}, \iota, \sqrt{p_1}, \sqrt{q_1}, \sqrt{p_2}, \sqrt{q_2}).$$

This implies that

$$\mathbf{K}\tilde{\mathbf{K}}\mathbf{K}_1 \subset \mathbf{K}\tilde{\mathbf{K}}\mathbf{K}_3(\iota, \sqrt{p_1}, \sqrt{q_1}, \sqrt{p_2}, \sqrt{q_2}).$$

Note that $\mathbf{K}\mathbf{K}_1 = \mathbf{K}_1\mathbf{K}_2$ and $\tilde{\mathbf{K}}\mathbf{K}_3 = \mathbf{K}_3\mathbf{K}_4$. So we have

$$\tilde{\mathbf{K}}\mathbf{K}_1\mathbf{K}_2 \subset \mathbf{K}\mathbf{K}_3\mathbf{K}_4(\iota, \sqrt{p_1}, \sqrt{q_1}, \sqrt{p_2}, \sqrt{q_2}).$$

We first note that $\mathbf{K}, \mathbf{K}_3$ and $\mathbf{K}_4$ have co-prime conductors. Therefore the degree of the field $\mathbf{K}\mathbf{K}_3\mathbf{K}_4(\iota, \sqrt{p_1}, \sqrt{q_1}, \sqrt{p_2}, \sqrt{q_2})$ is $27 \times 2^n$ for some positive natural number $n$. But since the Galois group of this field is abelian, it has a unique Sylow-2 subgroup. Therefore it has a unique subfield of degree 27. This implies that

$$\mathbf{K}_1\mathbf{K}_2\tilde{\mathbf{K}} = \mathbf{K}\mathbf{K}_3\mathbf{K}_4.$$

But composing with $\mathbf{K}_3$ on both sides, we get

$$\mathbf{K}_1\mathbf{K}_2\mathbf{K}_3\mathbf{K}_4 = \mathbf{K}\mathbf{K}_3\mathbf{K}_4$$

which is not possible as seen by a degree argument and the fact that all the $\mathbf{K}_i$s have distinct prime conductors. Further $\iota \notin \mathbf{K}\tilde{\mathbf{K}}(\tilde{\alpha_1}, \alpha_1, \sqrt{p_1}, \sqrt{q_1}, \sqrt{p_2}, \sqrt{q_2})$ since the field under consideration is totally real. And finally $\sqrt{p_1} \notin \mathbf{K}\tilde{\mathbf{K}}(\tilde{\alpha_1}, \alpha_1, \iota, \sqrt{q_1}, \sqrt{p_2}, \sqrt{q_2})$.

To see this consider the following diagram.

$$\begin{tikzcd}
 & \mathbf{K}\tilde{\mathbf{K}}(\tilde{\alpha_1}, \alpha_1, \iota, \sqrt{q_1}, \sqrt{p_2}, \sqrt{q_3}) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbf{K}\tilde{\mathbf{K}}(\alpha_1, \tilde{\alpha_1}) \arrow[dr, dash] & & \mathbb{Q}(\iota, \sqrt{q_1}, \sqrt{p_2}, \sqrt{q_2}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

The degree of $\mathbf{K}\tilde{\mathbf{K}}(\alpha_1, \tilde{\alpha_1}) = \mathbf{K}_1\mathbf{K}_2\mathbf{K}_3\mathbf{K}_4$ is a power of three. Note that $p$ does not ramify in $\mathbb{Q}(\iota, \sqrt{q_1}, \sqrt{p_2}, \sqrt{q_2})$. Since the degree of

$$\mathbf{K}\tilde{\mathbf{K}}(\tilde{\alpha_1}, \alpha_1, \iota, \sqrt{q_1}, \sqrt{p_2}, \sqrt{q_3})$$

over

$$\mathbb{Q}(\iota, \sqrt{q_1}, \sqrt{p_2}, \sqrt{q_2})$$

is a power of three, the ramification index of $p_1$ in $\mathbf{K}\tilde{\mathbf{K}}(\tilde{\alpha_1}, \alpha_1, \iota, \sqrt{q_1}, \sqrt{p_2}, \sqrt{q_2})$ is a power of three but the ramification index of $p_1$ in $\mathbb{Q}(\sqrt{p_1})$ is divisible by two. Therefore $\sqrt{p_1} \notin \mathbf{K}\tilde{\mathbf{K}}(\tilde{\alpha_1}, \alpha_1, \iota, \sqrt{q_1}, \sqrt{p_2}, \sqrt{q_2})$. Similar arguments work for $\sqrt{q_1}$, $\sqrt{p_2}$ and $\sqrt{q_2}$. Arguing as in Corollary 5.5.1, we can choose a Galois isomorphism of $\mathbb{Q}(\zeta_f)$ over $\mathbb{Q}$, where $f = 16p_1q_1p_2q_2$, which fixes $\mathbf{K}\tilde{\mathbf{K}}$ but not any of $\alpha_1, \tilde{\alpha_1}, \iota, \sqrt{p_1}, \sqrt{q_1}, \sqrt{p_2}$ and $\sqrt{q_2}$. This shows that

$$\mathrm{Gal}(\mathbb{Q}(\zeta_f)/\mathbf{K}\tilde{\mathbf{K}}) \not\subset \bigcup_{\ell} G_\ell \bigcup \mathrm{Gal}(\mathbb{Q}(\zeta_f)/\mathbf{K}_1\mathbf{K}_2) \bigcup \mathrm{Gal}(\mathbb{Q}(\zeta_f)/\mathbf{K}_3\mathbf{K}_4),$$

where $\ell$ is either an odd prime dividing $f$ or 4 and $G_\ell$ is the Galois group of $\mathbb{Q}(\zeta_f)/\mathbb{Q}(\zeta_\ell)$. Now applying Theorem 5.1.3 we have that one of $\mathbf{K}$ or $\tilde{\mathbf{K}}$ has a Euclidean ideal class. □

Let $p_1 = 13$, $q_1 = 37$, $p_2 = 61$ and $q_2 = 73$. For each of these primes we can associate the cyclotomic field $\mathbb{Q}(\zeta_{p_i})$ or $\mathbb{Q}(\zeta_{q_i})$. Further each such cyclotomic field contains a unique cubic subfield. Using SAGE, it can be shown that the compositum of the cubic fields corresponding to $p_1$ and $q_1$ contains a cubic subfield (distinct from the ones contained in the cyclotomic field) of class number three. Similarly, there exists a class number three subfield corresponding to $p_2$ and$q_2$. By Corollary 5.5.3, one of these two subfields must contain a Euclidean ideal class.

**Remark 5.5.4.** *Let $p_1, q_1, p_2, q_2$ be distinct primes. Corollary 5.5.3 is also true if we assume that some of the primes $p_1, q_1, p_2, q_2$ are congruent to* $1 \bmod 12$ *and some of them are congruent to* $7 \bmod 12$. *It can be seen by replacing $\mathbb{Q}(\sqrt{p_i})$ or $\mathbb{Q}(\sqrt{q_i})$ for $i = 1, 2$ by $\mathbb{Q}(\sqrt{-p_i})$ or $\mathbb{Q}(\sqrt{-q_i})$ when $p_i$ or $q_i$ are congruent to* $7 \bmod 12$ *in the proof of Corollary 5.5.3.*

With this we would like to conclude the last chapter on the results included in this thesis.

# Chapter 6

# Conclusion

In conclusion, we would like to touch upon two specific aspects of the problem of finding Euclidean ideal classes.

We begin by noting that the case of fields with lower unit rank is far from being solved. As we have seen for a family of real quadratic fields having cyclic class groups, with the exception of at most two fields, the class group will always have a Euclidean ideal class. One would like to extend this result to all real quadratic fields. Similarly, one would like to extend our results on a family of Galois cubic fields to all Galois cubic fields. However, it appears to us that such an extension might not be possible with the techniques mentioned in this thesis. It seems to us that proving such results will require some non-trivial developments in the sieve theoretic techniques involving well factorable weights.

Moreover all our results speak only of number fields whose Hilbert class field is abelian. Therefore, one would like to extend these results to the case of arbitrary Galois extensions. Such an extension would require both the aforementioned improvements in the sieve theoretic techniques and perhaps some new results analogous to those of class field theory for non-abelian extensions. Both of which, apriori, seem to be very difficult situations to handle.

The second aspect we would like to touch upon is the relationship with Artin's primitive root conjecture. In 1972, Weinberger ([36]) proved, under the extended Riemann hypothesis, that a fundamental unit (provided it exists) is a primitive root for infinitely many primes $\mathfrak{p}$. He then used this to show that the ring of integers with unit rank at least one is a principal ideal domain if and only if it is a Euclidean domain. Even the result of Harper and Murty ([19]), that one can go upto a lower bound of 3 on the unit rank for abelian extensions, is closely related to the works of Gupta and Murty ([14]) and Heath-Brown ([20]) on Artin's conjecture (as observed in [18]). For example Gupta and Murty's work on Artin's primitive root conjecture considers the possibility of a surjection from a monoid generated by finitely many primes (distinct from $p$) to $(\mathbb{Z}/p\mathbb{Z})^{\times}$ which is analogous to considering the surjection from $\mathcal{O}_{\mathbf{K}}^{\times}$ to $(\mathcal{O}_{\mathbf{K}}/\mathfrak{p})^{\times}$. Further the number of primes generating the monoid, in the case of Artin's primitive root conjecture, can be seen as analogous to the unit rank in the problem of finding Euclidean ideal classes.

One is therefore hopeful that any further progress with respect to Artin's primitive root conjecture will provide new insights into the problem of finding Euclidean ideal classes.

# Bibliography

[1] Y. F. Bilu, J.-M. Deshouillers, S. Gun, and F. Luca. Random ordering in modulus of consecutive Hecke eigenvalues of primitive forms. *Compos. Math.*, 154(11):2441–2461, 2018.

[2] E. Bombieri, J. B. Friedlander, and H. Iwaniec. Primes in arithmetic progressions to large moduli. *Acta Math.*, 156(3-4):203–251, 1986.

[3] D. Clark. A quadratic field which is Euclidean but not norm-Euclidean. *Manuscripta Mathematica*, 83(1):327–330, 1994.

[4] D. Clark and M. R. Murty. The Euclidean algorithm for Galois extensions of $\mathbb{Q}$. *J. Reine Angew. Math.*, 459:151162, 1995.

[5] G. Cooke and P. J. Weinberger. On the construction of division chains in algebraic number rings,with applications to $sl_2$. *Communications in Algebra*, 3(6):481–524, 1975.

[6] J.-M. Deshouillers, S. Gun, and J. Sivaraman. On Euclidean ideal classes in certain abelian extensions. *Math. Z.* To appear.

[7] P. G. L. Dirichlet. *Lectures on number theory*, volume 16 of *History of Mathematics.* American Mathematical Society, Providence, RI; London Mathematical Society, London, 1999. Supplements by R. Dedekind.

[8] P. D. T. A. Elliott and H. Halberstam. A conjecture in prime number theory. In *Symposia Mathematica, Vol. IV (INDAM, Rome, 1968/69)*, pages 59–72. Academic Press, London, 1970.

[9] É. Fouvry. Théorème de Brun-Titchmarsh: application au théorème de Fermat. *Invent. Math.*, 79(2):383–407, 1985.

[10] J. Friedlander and H. Iwaniec. *Opera de cribro*, volume 57 of *American Mathematical Society Colloquium Publications.* American Mathematical Society, Providence, RI, 2010.

[11] C. F. Gauss. *Disquisitiones arithmeticae.* Springer-Verlag, New York, 1986. Translated and with a preface by A. A. Clarke, Revised by W. C. Waterhouse, C. Greither and A. W. Grootendorst and with a preface by Waterhouse.

[12] H. Graves. $\mathbb{Q}(\sqrt{2}, \sqrt{35})$ has a non-principal Euclidean ideal. *Int. J. Number Theory*, 7(8):2269–2271, 2011.

[13] H. Graves. Growth results and Euclidean ideals. *Journal of Number Theory*, 133(8):2756 – 2769, 2013.

[14] H. Graves and M. R. Murty. A family of number fields with unit rank at least 4 that has Euclidean ideals. *Proc. Amer. Math. Soc.*, 141:2979–2990, 2013.

[15] S. Gun and J. Sivaraman. On existence of Euclidean ideal classes in real cubic and quadratic fields with cyclic class groups. *Michigan Math. J.* To appear.

[16] R. Gupta and M. R. Murty. A remark on Artin's conjecture. *Invent. Math.*, 78(1):127–130, 1984.

[17] H. Halberstam and H.-E. Richert. *Sieve methods.* Academic Press [A subsidiary of Harcourt Brace Jovanovich, Publishers], London-New York, 1974. London Mathematical Society Monographs, No. 4.

[18] M. Harper. $\mathbb{Z}[\sqrt{14}]$ is Euclidean. *Canad. J. Math.*, 56(1):5570, 2004.

[19] M. Harper and M. R. Murty. Euclidean rings of algebraic integers. *Canad. J. Math.*, 56(1):7176, 2004.

[20] D. R. Heath-Brown. Artin's conjecture for primitive roots. *Quart. J. Math. Oxford Ser. (2)*, 37(145):27–38, 1986.

[21] H. Heilbronn. On Euclid's algorithm in real quadratic fields. *Mathematical Proceedings of the Cambridge Philosophical Society*, 34(4):521–526, 1938.

[22] C. Hooley. On Artin's conjecture. *Journal fr die reine und angewandte Mathematik*, 225:209–220, 1967.

[23] C. Hsu. Two classes of number fields with a non-principal Euclidean ideal. *Int. J. Number Theory*, 12(4):1123–1136, 2016.

[24] H. Iwaniec. A new form of the error term in the linear sieve. *Acta Arith.*, 37:307–320, 1980.

[25] M. A. Jodeit Jr. Uniqueness in the division algorithm. *Amer. Math. Monthly*, 74:835–836, 1967.

[26] H. W. Lenstra Jr. Euclidean ideal classes. *Journées Arithmétiques de Luminy (Colloq. Internat. CNRS, Centre Univ. Luminy, Luminy, 1978), Astérisque, Soc. Math. France, Paris*, 61:121131, 1979.

[27] H. W. Lenstra Jr. On Artin's conjecture and Euclid's algorithm in global fields. *Invent. Math.*, 42:201–224, 1977.

[28] T. Motzkin. The Euclidean algorithm. *Bulletin of the American Mathematical Society*, 55(12):11421146, 1949.

[29] W. Narkiewicz. Units in residue classes. *Arch. Math. (Basel)*, 51(3):238–241, 1988.

[30] W. Narkiewicz. *Elementary and analytic theory of algebraic numbers.* Springer-Verlag, Berlin; PWN—Polish Scientific Publishers, Warsaw, second edition, 1990.

[31] W. Narkiewicz. Euclidean algorithm in small abelian fields. *Funct. Approx. Comment. Math.*, 37( part 2):337340, 2007.

[32] C. Queen. Arithmetic Euclidean rings. *Acta Arithmetica*, 26(1):105–113, 1974.

[33] P. Samuel. About Euclidean rings. *Journal of Algebra*, 19(2):282 – 301, 1971.

[34] J. Sivaraman. Existence of Euclidean ideal classes beyond certain rank. *J. Ramanujan Math. Soc.* To appear.

[35] A. Weil. *Sur Les Courbes Algébriques Et Les Variétés Qui S'en Déduisent.* Paris, Hermann, 1948.

[36] P. J. Weinberger. On Euclidean rings of algebraic integers. *Proc. Sympos. Pure Math., Vol. XXIV, Amer. Math. Soc., Providence, R. I.*, page 321332, 1973.