A Study Of Quadratic Number Fields

Simran Tinani, Prof. Kapil Paranjape

Indian Institute of Science Education and Research Mohali

Introduction

An algebraic number field, or simply a number field, is a finite extension of the rational numbers $\mathbf{Q}$. When this degree is equal to two, the field is called a quadratic number field (QNF). Every quadratic number field is of the form $\mathbf{Q}(\sqrt{d})$ where d is a nonzero square-free integer. Over any number field K, one may define the ring of integers $\mathcal{O}_K = \{r \in K : r^n + a_1 r^{n-1} + \dots a_{n-1} r + a_0 = 0 \text{ for some } a_i \in \mathbf{Z}\}$. The ring $\mathcal{O}_K$ is a Dedekind domain, and thus, the set $H(K)$ of all its fractional ideals forms an Abelian group. The quotient of this group with the subgroup $P(K)$ of all principal ideals is referred to as the *ideal class group*.

$$I(K) := \frac{H(K)}{P(K)}$$

The order h_K of the ideal class group is finite, and is called the *class number* of K.
The goal of this project is to study the ring of integers $\mathcal{O}_K$, the ideal class group $I(K)$, and the class number h_K of a quadratic number field $K = \mathbf{Q}(\sqrt{d})$, for different values of d. These objects may be understood better through the study of the theory of binary quadratic forms and the theory of factorization of prime ideals of a Dedekind domain in finite extensions of the fraction field.

Binary Quadratic Forms

Binary Quadratic Form (BQF):

$$f = aX^2 + bXY + cY^2, \; a, b, c \in \mathbf{Z}$$

- Discriminant, $D := b^2 - 4ac$.
- Primitive:- a, b, c have no common factor.
- $SL_2(\mathbf{Z})$ acts on the set of all BQF's f by

$$A \star f := f(px + qy, rx + sy), \text{ where}$$

$$A = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in SL_2(\mathbf{Z})$$

- BQFs lying in the same orbit are called equivalent. These have the same discriminant and take on the same values.
- Every BQF is equivalent to a "reduced" form obtainable by a fixed algorithm. For a fixed discriminant D, the total number of these reduced forms, and thus, the number of equivalence classes of BQF's, is finite.

BQFs & QNFs: the relation

- Let $C_p^+(d)$ denote the set of equivalence classes of binary quadratic forms with discriminant d, and containing only forms with positive leading coefficient a if $d < 0$.
- Let $d_K \equiv 0, 1 \pmod 4$, be the discriminant of a quadratic field K.

Theorem. *There exists a bijection between the ideal class group $I(K)$ and $C_p^+(d)$.*

- As a consequence, one obtains that the class number $h_K = |I(K)|$ is finite.
- Using this bijection, $C_p^+(d)$ can be given a natural group structure, and will henceforth be called the **form class group**.

Computing in $C_p^+(d)$

Some results on class numbers

- $C_p^+(-47) \cong \frac{\mathbf{Z}}{5\mathbf{Z}}$
- $C_p^+(12) \cong < 1 >$
- If $-D = 8k + 3$ $(k > 0)$, the class number is divisible by 3 [5].
- For a class number $h = 6n \pm 1$, $n > 0$, we must have $-D = 8k - 1$. [5]
- The determinants corresponding to class number 5 are $-D = 127, 103, 70, 47$. [5]
- The determinants corresponding to class number 13 are

  $-D = 191, 263, 607, 631, 727, 2143$. [5]

Splitting of Prime Ideals

Setup: A is a Dedekind domain, K is the field of fractions of A, L is a finite extension of K with degree n, B is the integral closure of A in L. $P \neq 0$ is a prime ideal of A, $\beta \neq 0$ is a nonzero prime ideal of B. PB denotes the ideal generated by the set P in the ring B.

- If $\beta \supseteq PB$, write $\beta \mid P$, i.e. β divides P.
- PB decomposes as

$$PB = \prod_{\beta \mid P} \beta^{e_{\beta/P}}$$

- $e_{\beta/P}$ is the *Ramification Index* of P in β.
- *Inertial Degree* of β over P:

$$f_{\beta/P} := [B/\beta : A/P]$$

- $\sum_i e_i f_i = n = [B/PB : A/P]$
- P is *ramified* if $e_{\beta/P} > 1$ for some $\beta \mid P$.
- If L/K is Galois, $e_{\beta/P}$ and $f_{\beta/P}$ depend only on P and we have $[L : K] = n = efg$

Prime Ideals in Number Fields

Let K be a number field.

- In general, there is no straightforward method to compute the factorization of $p\mathcal{O}_K$ for $p \in \mathbf{Z}$ prime.
- Consider the case where $\mathcal{O}_K = \mathbf{Z}[\theta]$ for some $\theta \in K$. In particular, this occurs for quadratic number fields K. In this case, a theorem by Kummer gives a method to compute the factorization of $p\mathcal{O}_K$ in terms of the factors of the reduction of the minimal polynomial f of θ in the field $\frac{\mathbf{Z}}{p\mathbf{Z}}$.
- For $K = \mathbf{Q}(\sqrt{d})$ and $p \in \mathbf{Z}$ prime, the factorization of $p\mathcal{O}_K$ is determined by the value of the Legendre symbol $(\frac{d}{p})$ and the residue class of d modulo 4.

Theorem. *A prime $p \in \mathbf{Z} \subset K$ is ramified in K if and only if it divides the discriminant d_K.*

The Chebotarev Density Theorem

- In general, a prime integer will factor into several prime ideals in $\mathcal{O}_K$. For a given prime, only finitely may splitting patterns may occur. The full description of splitting of every p in a general Galois extension is an unsolved problem.
- The theorem states that the frequency of occurrence of a given pattern for all primes less than or equal to N (for some large integer N) tends to a given limit as N goes to infinity.

Applying Ramification theory

Theorem. *A positive integer n can be written as a sum of two squares if and only if n has a prime factorization $n = p_1^{e_1} \dots p_n^{e_n}$ (p_i distinct) where e_i is even whenever $p_i \equiv 2$ or $3 \pmod 4$.*

Unramified Extensions

- L/K is called an *unramified extension* if every prime ideal P of $\mathcal{O}_K$ is unramified (every ramification index equals 1) in $\mathcal{O}_L$.
- Let K be any algebraic number field. Let $a, b \in \mathcal{O}_K$. Let L denote the minimal splitting field of a polynomial $f(X) = X^n - aX + b$, i.e. $L = K(\alpha_1, \dots \alpha_n)$, where $\alpha_1, \dots, \alpha_n$ are the roots of $f(X) = 0$. Let $D = \prod_{i<j}(\alpha_i - \alpha_j)^2$ be the discriminant of $f(X)$.

Theorem. *If $(n-1)a$ and nb are relatively prime, L is unramified over $K(\sqrt{D})$.*

Theorem. *If $(n-1)a$ and nb are relatively prime, any prime ideal of L has the ramification index 1 or 2 over K.*

Theorem. *Let G be a finite group. Then, there exists an algebraic number field k which has an unramified extension with Galois group G.*

Theorem. *Infinitely many real quadratic fields have a class number divisible by 3.*

Class Numbers: More Results

Theorem. *Let $K = \mathbf{Q}(\sqrt{d})$ be a QNF whose discriminant d_K is divided by at least two distinct primes. Then, h_K is even.*

Let $g > 1$ be an integer and p, q be odd primes.

Theorem.

$$\#\{(p,q) \mid p \neq q \pmod 4, \; 2g \mid h(-pq)\} = \infty$$

Theorem.

$$\#\{(p,q) \mid p \equiv q \pmod 4, \; 2g \mid h(-pq)\} = \infty$$

References

[1] Corentin Perret-Gentil (2012), The correspondence between binary quadratic forms and quadratic fields.

[2] Kôji Uchida (1970), Unramified extensions of quadratic number fields, I & II.

[3] Byeon & Lee (2008), Divisibility of class numbers of imaginary quadratic fields whose discriminant has only two prime factors.

[4] Akiko Ito (2012), On the divisibility of class numbers of imaginary quadratic fields whose discriminant has only two odd prime factors.

[5] Daniel Shanks (2010), On Gauss's Class Number Problems.