Introduction to Class Field Theory and Primes of the Form $x^2 + ny^2$

Che Li

October 3, 2018

Abstract

This paper introduces the basic theorems of class field theory, based on an exposition of some fundamental ideas in algebraic number theory (prime decomposition of ideals, ramification theory, Hilbert class field, and generalized ideal class group), to answer the question of which primes can be expressed in the form $x^2 + ny^2$ for integers x and y, for a given n.

Contents

1 Number Fields

1.1 Prime Decomposition of Ideals

We will review some basic facts from algebraic number theory, including Dedekind Domain, unique factorization of ideals, and ramification theory. To begin, we define *an algebraic number field* (or, simply, a number field) to be a finite field extension K of $\mathbb{Q}$. The set of algebraic integers in K form a ring $\mathcal{O}_K$, which we call the ring of integers, i.e., $\mathcal{O}_K$ is the set of all $\alpha \in$ K which are roots of a monic integer polynomial. In general, $\mathcal{O}_K$ is not a UFD but a Dedekind domain. This means the following:

Theorem 1.1.1 *Let $\mathcal{O}_K$ be the ring of integers in a number field K. Then $\mathcal{O}_K$ is a Dedekind domain, which means that*

(i) *$\mathcal{O}_K$ is integrally closed in K, i.e., if $\alpha \in K$ satisfies a monic polynomial in $\mathcal{O}_K$[x], then $\alpha \in \mathcal{O}_K$.*

(ii) *$\mathcal{O}_K$ is Noetherian, i.e., for any given ascending ideals $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \ldots$ in $\mathcal{O}_K$, there is an integer n such that $\mathfrak{a}_n = \mathfrak{a}_{n+1} = \ldots$*

(iii) *Every nonzero prime ideal of $\mathcal{O}_K$ is maximal.*

Proof. The proof of (i) follows easily from the properties of algebraic integers (see Marcus [5, Exercise 4 to Chapter 2]). To prove (ii) and (iii), we need a proposition on the basic structure of $\mathcal{O}_K/\mathfrak{a}$ (note that when $\mathfrak{p}$ is a prime ideal, then $\mathcal{O}_K/\mathfrak{p}$ is a finite field which is called the *residue field* of $\mathfrak{p}$):

Proposition 1.1.2 For any nonzero ideal $\mathfrak{a} \subset \mathcal{O}_K$, $\mathcal{O}_K/\mathfrak{a}$ is finite.

Proof. Let $\alpha \in \mathfrak{a}$, $\alpha \neq 0$. Then there exist $a_i \in \mathbb{Z}$ such that $\alpha^m + a_1\ \alpha^{m-1} + ... + a_m = 0$. We may assume that a_m is nonzero. Then, $0 \neq a_m \in \mathfrak{a} \cap \mathbb{Z}$.

Denote a_m by a. Let (a) be the principal ideal generated by a in $\mathcal{O}_K$. Since $\mathcal{O}_K/(a)$ maps onto $\mathcal{O}_K/\mathfrak{a}$ it suffices to show that $\mathcal{O}_K/(a)$ is finite. We will show that it has precisely a^n elements.

Recall as a basic fact in algebraic number theory that $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $n = [\mathrm{K} : \mathbb{Q}]$. That is, we can find an integral basis $\{\omega_1, \omega_2, ..., \omega_n\}$ such that $\mathcal{O}_K = \sum \mathbb{Z}\omega_j$. Let $S = \{\ \sum \gamma_i\omega_i \colon\ 0 \leq \gamma_i < a\}$.We claim that S is a set of coset representatives for $\mathcal{O}_K/\mathfrak{a}$. If this is the case, the result clearly follows. But it is clear that $\mathcal{O}_K/(a) = \sum(\mathbb{Z}/a\mathbb{Z})(\omega_j)$, and the result follows. □

To finish the proof of Theorem 1.1.1, observe for (ii) that since $\mathcal{O}_K/\mathfrak{a}$ is finite there are only finitely many ideals containing $\mathfrak{a}$. For (iii), if $\mathfrak{p}$ is prime then $\mathcal{O}_K/\mathfrak{p}$ is a finite integral domain, and thus a field. Thus by definition $\mathfrak{p}$ is maximal. □

The most important property of a Dedekind domain is that any ideal factors uniquely into products of prime ideals:

Corollary 1.1.3 If K is a number field, then any nonzero ideal $\mathfrak{a}$ in $\mathcal{O}_K$ can be written as a product of prime ideals

$$\mathfrak{a} = \mathfrak{p}_1 ... \mathfrak{p}_r$$

and the factorization is unique up to order. Furthermore, the $\mathfrak{p}_i$'s are exactly the prime ideals of $\mathcal{O}_K$ that contain $\mathfrak{a}$.

Proof. See Marcus [5, Chapter 3, Theorem 16]. □

Prime ideals thus play an essential role in algebraic number theory. Before further describing their behavior, namely the idea of ramification, we need some extra information on fractional fields, which will help us construct the notion of ideal class group $C(\mathcal{O}_K)$ which will be used extensively in this paper.

We define a *fractional ideal* of the number field K as a $\mathcal{O}_K$-module contained inside K, written in the form αI, where $0 \neq \alpha \in$ K and I $\subset \mathcal{O}_K$ an ideal. In this paper, the notion of a fractional ideal will not be fully explored. I thus provide references for the proof of the following important result on fractional ideals:

Proposition 1.1.4 Let $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}_K$, then

(1) for any $\mathfrak{a}$, there exists another fractional ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b} = \mathcal{O}_K$.

(2) $\mathfrak{a}$ can be written as a product

$$\mathfrak{a} = \prod_{j=1}^{n} \mathfrak{p}_j^{r_j}$$

where $\mathfrak{p}_j$'s are distinct prime ideals of $\mathcal{O}_K$ and r_j are integers.

Proof. Consult Lang [4, §1.6] □

Now we introduce the idea of class group. Let I_K denote the set of all fractional ideals in K. With Proposition 1.4 it is easy to see that I_K forms a group. Consider the subgroup of I_K which consists of all the principal fractional ideals in $\mathcal{O}_K$. Denote this subgroup by

$$P_K = \{\alpha\mathcal{O}_K \colon\ \alpha \in \mathrm{K} \text{ and } \alpha \neq 0\ \}.$$

The quotient I_K/P_K is the *ideal class group*, denoted by $\mathcal{C}(\mathcal{O}_K)$. Basically, the ideal class group partitions the set of ideals of $\mathcal{O}_K$ by giving it the following equivalence relation:

Definition 1.1.5 Two ideals $\mathfrak{a}$, $\mathfrak{b} \subset \mathcal{O}_K$ are said to be equivalent if there exist nonzero α, $\beta \in \mathcal{O}_K$ such that $(\alpha)\mathfrak{a} = (\beta)\mathfrak{b}$. This is an equivalence relation. The equivalence classes are called ideal classes. The number of ideal classes, denoted h_K, is called the class number of K.

The notion of ideal class group is crucial to factorization of ideals in number field because the order of an ideal class in the ideal class group, and the order of the ideal class group, measure "how far" $\mathcal{O}_K$ is from being a PID (later in the paper, we will see examples of decomposition of ideal which involves the class number). We can see this by observing the following fact:

Corollary 1.1.6 $h_K = 1 \iff \mathcal{O}_K$ is a PID.

Proof. Suppose $h_K = 1$. If $\mathfrak{a}$ is an ideal, then $\mathfrak{a}$ and $\mathcal{O}_K$ are equivalent, meaning that there are nonzero α and β in $\mathcal{O}_K$ such that $(\alpha)\mathfrak{a} = (\beta)\mathcal{O}_K = (\beta)$. Thus $\mathfrak{a} = (\beta/\alpha)$. On the other hand, it is obvious that if $\mathcal{O}_K$ is a PID then $h_K = 1$. □

1.2 Basic Ramification Theory

Now we introduce the basic theories of ramification. Consider a number field K and a finite extension L/K. Given $\mathfrak{p}$ a prime ideal of $\mathcal{O}_K$, then we have the prime factorization

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1}...\mathfrak{P}_g^{e_g}$$

where $\mathfrak{P}_i$'s are distinct prime ideals of $\mathcal{O}_L$ containing $\mathfrak{p}$. The integer $\text{ord}_{\mathfrak{P}_i}(\mathfrak{p}\mathcal{O}_L) = e_i$ is called the *ramification index* of $\mathfrak{P}_i$ (for any P a prime ideal and A an ideal, $\text{ord}_P(A)$ is defined as the unique nonnegative integer t such that $A \subset P^t$ and $A \nsubseteq P^t$). $\mathcal{O}_L/\mathfrak{P}$ is a finite extension of $\mathcal{O}_K/\mathfrak{p}$. We denote $[\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}] = f$, and thus $|\mathcal{O}_L/\mathfrak{P}| = \|\mathcal{O}_K/\mathfrak{p}\|^f$, for some integer $f \geq 1$. We define f to be the *inertia degree* of $\mathfrak{P}$. The first important theorem that we use in this paper establishes the relation between the ramification index e, the inertia degree f, the number of distinct primes appearing in the factorization g, and the degree of the extension L/K n. We restrict ourselves to the case when L/K is Galois:

Theorem 1.2.1 With the notations above, let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$. Let L/K be Galois, and denote $G = Gal(L/K)$ Then:

(i) Suppose $\mathfrak{P}_i$ and $\mathfrak{P}_j$ are prime ideals of $\mathcal{O}_L$ containing $\mathfrak{p}$. Then there is a $\sigma \in G$ such that $\sigma\mathfrak{P}_i = \mathfrak{P}_j$. i.e., Gal(L/K) acts transitively on the set of prime ideals of $\mathcal{O}_L$ containing $\mathfrak{p}$.

(ii) If $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1}...\mathfrak{P}_g^{e_g}$. Then $e_1 = e_2 = ... = e_g$. $f_1 = f_2 = ... = f_g$. If e and f denote these common values, then $efg = n$.

Proof. (i) For the sake of contradiction, let there be a prime ideal $\mathfrak{P}_0$ containing $\mathfrak{p}$ but not in the set $\{\sigma\mathfrak{P}_l\colon\ \sigma \in G\}$. Since $\mathfrak{P}_l$'s are all primes, $\mathfrak{P}_k + \mathfrak{P}_j = \mathcal{O}_L$ for $k \neq j$. Then, expanding the product

$$(\mathfrak{P}_0 + \sigma\mathfrak{P}_1)(\mathfrak{P}_0 + \sigma\mathfrak{P}_2)...(\mathfrak{P}_0 + \sigma\mathfrak{P}_g) = \mathcal{O}_L$$

we see that all summands, except the last, are in $\mathfrak{P}_0$. Thus

$$\mathfrak{P}_0 + \sigma^g\mathfrak{P}_1\mathfrak{P}_2...\mathfrak{P}_g = \mathcal{O}_L.$$

Then there exists $\alpha \in \mathcal{O}_L$ such that $\alpha \equiv 1\ (\mathfrak{P}_0)$ but $\alpha \equiv 0\ (\sigma\mathfrak{P}_i)$ for all $\sigma \in G$. Similarly, for each j there is an α_j such that $\alpha_j \equiv 1\ (\mathfrak{P}_j)$ but $\alpha_j \equiv 0\ (\mathfrak{P}_i)$ for $i \neq j$. In other words, we can find an $\alpha_0 \in \mathcal{O}_L$ such that $\alpha_0 \equiv 0\ (\mathfrak{P}_0)$ but $\alpha_0 \equiv 1\ (\sigma\mathfrak{P}_i)$ for all σ in G.

Let $\text{Nm}(\alpha)$ denotes the norm of α. Then $\text{Nm}(\alpha) = \prod_{\sigma\in G}\sigma\alpha \in \mathfrak{P}_0 \cap \mathcal{O}_K = \mathfrak{p}\mathcal{O}_K$. Then, $\text{Nm}(\alpha) \in \mathfrak{P}_i$ and thus $\sigma\alpha \in \mathfrak{P}_i$ for some σ. But then $\alpha \in \sigma^{-1}\mathbb{P}_i$ which contradicts $\alpha_0 \equiv 1\ (\sigma^{-1}\mathfrak{P}_i)$

(ii) To prove that $f_1 = f_2 = ... = f_g$, observe that for any i,

$$\mathcal{O}_L/\sigma\mathfrak{P}_i = \sigma\mathcal{O}_L/\sigma\mathfrak{P}_i \cong \mathcal{O}_L/\mathfrak{P}_i$$

because $\sigma\mathcal{O}_L = \mathcal{O}_L$. By (i), for any i there exists a σ such that $\sigma\mathfrak{P}_1 = \mathfrak{P}_i$. Since $\mathcal{O}_L/\mathfrak{P}_1 \cong \mathcal{O}_L/\sigma\mathfrak{P}_1 = \mathcal{O}_L/\mathfrak{P}_i$ we have $f_1 = f_i$ for every i. Thus all f_i's are equal to some f.

To prove $e_1 = e_2 = ... = e_g$, apply σ to both sides of $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1}...\mathfrak{P}_g^{e_g}$. Since $\mathfrak{p} \in \mathcal{O}_K$, $\sigma\mathfrak{p}\mathcal{O}_L = \mathfrak{p}\mathcal{O}_L$. Then we have

$$\mathfrak{p}\mathcal{O}_L = (\sigma\mathfrak{P}_1)^{e_1}...(\sigma\mathfrak{P}_g)^{e_g}$$

In this expression, observe that the exponent of $\mathfrak{P}_i = \sigma\mathfrak{P}_1$ is e_1. But in the original expression of factorization the exponent of $\mathfrak{P}_i$ is e_i. By uniqueness of factorization, we must have $e_1 = e_i$ for all i, i.e., they are all equal to some value e.

Thus, by $\sum e_i f_i = n$ we have $efg = n$. □

Given a prime factorization of ideal $\mathfrak{p} \subset \mathcal{O}_K$ in $\mathcal{O}_L$ where L/K is Galois, we say that $\mathfrak{p}$ is unramified if $e = e(\mathfrak{P}_i|\mathfrak{p}) = 1$ for all i. We say that $\mathfrak{p}$ *splits completely* if $e = f = 1$. To explicate the behavior of ramification, we need some facts about decomposition and inertia groups:

Definition 1.2.2 Given the notations above, we define, for each $\mathfrak{P}$ lying over $\mathfrak{p}$, the decomposition group D and the inertia group E as:

$$\mathrm{D} = \mathrm{D}(\mathfrak{P}|\mathfrak{p}) = \left\{\sigma \in G : \sigma\mathfrak{P} = \mathfrak{P}_i\right\}$$
$$\mathrm{E} = \mathrm{E}(\mathfrak{P}|\mathfrak{p}) = \left\{\sigma \in G : \sigma(\alpha) \equiv \alpha(\mathfrak{P}), \forall \alpha \in \mathcal{O}_L\right\}.$$

It is clear that D and E are subgroups of G, and E is a normal subgroup of D. $\sigma \in$ D naturally induces an automorphism of the field $\mathcal{O}_L/\mathfrak{P}$. We denote this induced automorphism as $\bar{\sigma}$: $\mathcal{O}_L/\mathfrak{P} \longrightarrow \mathcal{O}_L/\mathfrak{P}$. Moreover, it is clear that $\bar{\sigma}$ fixes $\mathcal{O}_K/\mathfrak{p}$ pointwise because it fixes the field K. Thus $\bar{\sigma}$ is a member in the Galois group of $\mathcal{O}_L/\mathfrak{P}$ over $\mathcal{O}_K/\mathfrak{p}$, which we denote by $\bar{G}$.

This can be summarized as the follows: there exists a map from D to $\bar{G}$. (Readers can easily check that this map is a surjective group homomorphism.) Further, the kernel of this map is easily seen to be E and thus D/E $\longrightarrow \bar{G}$ is a group isomorphism. Since we know that the order of $\bar{G}$ is the degree of the extension $\mathcal{O}_L/\mathfrak{P}$ over $\mathcal{O}_K/\mathfrak{p}$, which we know by the definition of inertia degree is f. Thus we have:

Proposition 1.2.3 Let D, E and $\bar{G}$ be defined as above, then

(i) The map from D to $\bar{G}$ is a surjective group homormorphism, thus D/E is isomorphic to $\bar{G}$.

(ii) $|\mathrm{E}| = e(\mathfrak{P}|\mathfrak{p})$. $|\mathrm{D}| = e(\mathfrak{P}|\mathfrak{p})f(\mathfrak{P}|\mathfrak{p})$.

Proof. For detailed proof, see Marcus [5, Theorem 28]. A more intuitive way is to consider $\sigma \in$ D as a stabilizer of $\mathfrak{P}$ in the group $G = \mathrm{Gal(L/K)}$. By orbit-stabilizer theorem, the order of $\sigma \in$ D is

$$|\mathrm{stab}(\mathfrak{P})| = \frac{|G|}{|orb(\mathfrak{P})|} = \frac{n}{g} = ef$$

Thus $|\mathrm{D}| = ef$. By the definition of inertia group, every $\sigma \in$ E maps to the identity element in $\bar{G}$. Thus D/E $\cong \bar{G}$. Finally, since $|\bar{G}|$ is equal to the order of $\mathcal{O}_L/\mathfrak{P}$ over $\mathcal{O}_K/\mathfrak{p}$, $|\bar{G}| = f$. Thus $|\mathrm{D/E}| = f$ and $|\mathrm{E}| = e$ □

We will be concerned with Hilbert class fields, which are field extensions where all primes of the base field are unramified. Hence it is important to consider how $\bar{G}$ and D behave in this situation. Assume that $\mathfrak{p}$ is unramified in L, then $\mathrm{E}(\mathfrak{P}/\mathfrak{p})$ is trivial. We have D $\cong \bar{G}$. We want to prove that $\bar{G}$ has a special generator, which sends every $x \in \mathcal{O}_L/\mathfrak{P}$ to $x^{|\mathfrak{p}|}$. The following lemma establishes this and defines the notion of the *Artin symbol*:

Lemma 1.2.4 Let K $\subset$ L be a Galois extension, and let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$ which is unramified in $\mathcal{O}_L$. If $\mathfrak{P}$ is a prime of $\mathcal{O}_L$ containing $\mathfrak{p}$, then there is a unique element $\phi \in$ Gal(L/K) (in fact in D) such that

$$\phi(\alpha) \equiv \alpha^{Nm(\mathfrak{p})} (\mathrm{mod}\ \mathfrak{P})$$

for every $\alpha \in \mathcal{O}_L$.

Proof. Recall the structure of $\bar{G}$: $\bar{G}$ is a cyclic group generated by some induced automorphism $\bar{\sigma}$. Because $\bar{\sigma}$ has to fix $\mathcal{O}_L/\mathfrak{p}$ pointwise, then, if $|\mathcal{O}_K/\mathfrak{p}| = q$, we have for every $x \in \mathcal{O}_L/\mathfrak{P}$

$$\bar{\sigma}\colon\ x \mapsto x^{|\mathfrak{p}|}$$

This induced automorphism is called the *Frobenius automorphism*. Since D $\cong \bar{G}$, there is a unique $\phi \in$ D that maps to the Frobenius automorphism. Since by definition $q = |\mathfrak{p}|$, ϕ satisfies

$$\phi(\alpha) \equiv \alpha^{|\mathfrak{p}|}(\mathfrak{P})$$

for all $\alpha \in \mathcal{O}_L$. To prove uniqueness, note that any σ satisfying this condition is in D, and thus we are done. □

The unique element ϕ in the above lemma is called the Artin symbol and is denoted as $\left(\frac{L/K}{\mathfrak{P}}\right)$. The Artin symbol satisfies the following useful properties:

Corollary 1.2.5 Let K ⊂ L be a Galois extension, and let $\mathfrak{p}$ be an unramified prime of K. Given a prime $\mathfrak{P}$ of L containing $\mathfrak{p}$, we have:

(i) If $\sigma \in$ Gal(L/K), then

$$\left(\frac{L/K}{\sigma\mathfrak{P}}\right) = \sigma\left(\frac{L/K}{\mathfrak{P}}\right)\sigma^{-1}.$$

(ii) The order of $\left(\frac{L/K}{\mathfrak{P}}\right)$ is the inertia degree $f = f(\mathfrak{P}|\mathfrak{p})$.

(iii) $\mathfrak{p}$ splits completely in L iff $\left(\frac{L/K}{\mathfrak{P}}\right) = 1$.

Proof. To prove (i), notice that

$$\left(\frac{L/K}{\sigma\mathfrak{P}}\right)(\alpha) \equiv \alpha^{|\mathfrak{p}|}(\sigma\mathfrak{P}).$$

But

$$\sigma\left(\frac{L/K}{\mathfrak{P}}\right)\sigma^{-1}(\alpha) \equiv \sigma((\sigma^{-1}(\alpha))^{|\mathfrak{p}|}) \equiv \alpha^{|\mathfrak{p}|}(\mathfrak{P}).$$

By uniqueness of the Artin symbol we have

$$\left(\frac{L/K}{\sigma\mathfrak{P}}\right) = \sigma\left(\frac{L/K}{\mathfrak{P}}\right)\sigma^{-1}.$$

To prove (ii), recall that the Artin symbol maps to the Frobenius automorphism which generates $\bar{G}$. Thus the Artin symbol has order f as desired.

To prove (iii), recall from Theorem 1.2.1 that $\mathfrak{p}$ splits completely *iff* $e = f = 1$. Since we assume $e = 1$, the result follows directly from (ii). □

We conclude this section by the following proposition, which determines when a prime is unramified or split completely in a Galois extension:

Proposition 1.2.6 Let K ⊂ L be a Galois extension, where L = K(α) and $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ for some $\alpha \in \mathcal{O}_L$. Let f(x) be the monic minimal polynomial of α over K, f(x) $\in \mathcal{O}_K$[x]. If $\mathfrak{p}$ is a prime in $\mathcal{O}_K$ and f(x) is separable modulo $\mathfrak{p}$, then:

(i) $\mathfrak{p}$ is unramified in L.

(ii) If $f(\mathrm{x}) \equiv f_1(\mathrm{x})...f_g(x) \bmod \mathfrak{p}$, where the f_i(x) are distinct and irreducible modulo $\mathfrak{p}$, then $\mathfrak{P}_i = \mathfrak{p}\mathcal{O}_L + f_i(\alpha)\mathcal{O}_L$ is a prime ideal of $\mathcal{O}_L$, $\mathfrak{P}_i \neq \mathfrak{P}_j$ for $i \neq j$. And

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1...\mathfrak{P}_g.$$

Furthermore, the f_i(x) all have the same degree, which is equal to the inertial degree *f*.

(iii) $\mathfrak{p}$ splits completely in L *iff* f(x) $\equiv 0$ ($\mathfrak{p}$) has a solution in $\mathcal{O}_K$.

Proof. Note that (i) and (iii) are direct consequences of (ii). (ii) is a standard result in algebraic number theory. For proof, see Milne [6, Theorem 3.41]. □

2 Quadratic Fields

Now we consider an application of the general theory of ramification to quadratic fields. Since later section involves examples of solving quadratic forms, it is important to introduce the basics of quadratic fields. First, we recall some basic definitions:

Definition 2.1 An algebraic number field K is called a quadratic number field if [K:$\mathbb{Q}$] = 2. Such a field is written uniquely in the form K = $\mathbb{Q}(\sqrt{N})$, where $N \in \mathbb{Z}$ is square-free.

Corollary 2.2 Given a quadratic field K = $\mathbb{Q}(\sqrt{N})$

(i) Let d_K denote the discriminant of K. Then

$$d_K = \begin{cases} N, & \text{if N} \equiv 1(4). \\ 4N, & \text{if N} \equiv 2,3(4). \end{cases} \tag{1}$$

(ii) Furthermore,

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\frac{-1+\sqrt{N}}{2}], & \text{if N} \equiv 1(4). \\ \mathbb{Z}[\sqrt{N}], & \text{if N} \equiv 2,3(4). \end{cases} \tag{2}$$

Using the discriminant, (2) can be written more elegantly as:

$$\mathcal{O}_K = \mathbb{Z}[\tfrac{d_K+\sqrt{d_K}}{2}].$$

Proof. This is a standard result on quadratic fields. For a proof, see Ireland [3, Proposition 13.1.1 and 13.1.2]. □

Lemma 2.3 Let U_N denote the multiplicative group of units in the ring of integers of the quadratic field K = $\mathbb{Q}(\sqrt{N})$. If $N < 0$ and square free then

(i) $U_{-1} = \{1, i, -1, -i\}$.

(ii) $U_{-3} = \{\pm 1, \pm\omega, \pm\omega^2\}$, where ω = (-1+$\sqrt{-3}$)/2.

(iii) $U_N = \{1, -1\}$ for $N <$ -3, or N = -2.

Proof. By the above corollary, if $N \equiv 2$ or 3(4) then any unit α can be written as $x + \sqrt{N}y$, x, $y \in \mathbb{Z}$. Thus the norm Nm(α) = ± 1 *iff* $x^2 + |N|y^2 = 1$. If N = -1, we have (i). If $|N| >$ 1, we have (iii).

If $N \equiv 1(4)$ we write any unit as $(x+\sqrt{N}y)/2$ where x and y are of the same parity. Then, Nm(α) = ± 1 *iff* $x^2 + |N|y^2 = 4$. If N = -3, then we have (ii). If $|N| > 3$, we have (iii). This completes the proof. □

Remark 2.4 *Note that the above lemma is a specific case of the more general theorem called the Dirichlet's unit theorem that says the following:*

$$U(\mathcal{O}_K) \cong \mu(\mathcal{O}_K) \times \mathbb{Z}^{r_1+r_2-1}$$

where $\mu(\mathcal{O}_K)$ is the finite cyclic group containing all the roots of unity in $\mathcal{O}_K$ and K is a number field with r_1 real embeddings and r_2 pairs of conjugate complex embeddings (the notion of real and complex embedding will be explicated when defining infinite primes in Definition 3.2). Note that in the case of imaginary quadratic extension, $r_1 = 0$, $r_2 = 1$, and thus we have Lemma 2.3.

With the above results of $\mathcal{O}_K$, d_K, and $U(\mathcal{O}_K)$ we now investigate an important statement on how primes $p\mathcal{O}_K$ split in $\mathcal{O}_K$, $p \in \mathbb{Z}$. We make the one restriction on N in order to build on the notion of Hilbert class field: $N > 0$ and thus K is an imaginary quadratic field (for $N < 0$, the group of units also behaves in a more radical way). Notice that, by Theorem 1.6, we have $efg = n = 2$. We say that p ramifies when $e = 2$ ($f = g = 1$), p splits when $g = 2$ ($e = f = 1$), and p is inertial (remains prime) when $f = 2$ ($e = g = 1$).

Proposition 2.5 Let K be a quadratic field of discriminant d_K. Let p be prime in $\mathbb{Z}$.

(i) If $(d_K/p) = 0$ (i.e., p|d_K), then $p\mathcal{O}_K = \mathfrak{p}^2$ for some prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$.

(ii) If $(d_K/p) = 1$, then $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$, where $\mathfrak{p} \neq \mathfrak{p}'$ are primes in $\mathcal{O}_K$.

(iii) If (d_K/p) = -1, then $p\mathcal{O}_K$ remains prime in $\mathcal{O}_K$.

Proof. In (i) we claim $p\mathcal{O}_K = (p, \sqrt{N})^2$. In fact, $(p, \sqrt{N})^2 = (p)(p,\ \sqrt{N},\ N/p)$. The last ideal is $\mathcal{O}_K$ since $(p,\ d/p) = 1$.

In (ii) suppose there exists $a \in \mathbb{Z}$ s.t. $a^2 \equiv \mathrm{Nm}(p)$. We claim: $p\mathcal{O}_K = (p,\ a+\sqrt{N})(p,\ a-\sqrt{N})$. In fact, $(p,\ a+\sqrt{N})(p,\ a-\sqrt{N}) = (p)(p,\ a+\sqrt{N},\ a-\sqrt{N},\ (a^2-d)/p)$. The latter ideal is $\mathcal{O}_K$ because $(p,\ 2a) = 1$.

In (iii) we claim that $p\mathcal{O}_K = \mathfrak{p}$ and $\mathfrak{p}$ has inertia degree 2. If $\mathfrak{p}$ has degree 1, then $\mathcal{O}_K/\mathfrak{p}$ has order p by the definition of inertial degree. Since $\mathbb{Z}/p\mathbb{Z}$ is injective to $\mathcal{O}_K/\mathfrak{p}$, every coset of $\mathcal{O}_K/\mathfrak{p}$ is represented by an integer. Then, let $a \in \mathbb{Z}$ such that $a \equiv \sqrt{N}(\mathfrak{p})$. But this means $a^2 \equiv \sqrt{N}(\mathfrak{p})$ and $a^2 \equiv \sqrt{N}(p)$ which contradicts the assumption that the inertial degree is 1. Thus $p\mathcal{O}_K$ remains a prime. □

Thus, we have the corollary:

Corollary 2.6 Let K be a quadratic field of discriminant d_K, let p be a prime integer. Then:

(i) p ramifies in K *iff* $p|d_K$

(ii) p splits completely in K *iff* $(d_K/\mathrm{p}) = 1$

Proof. The corollary follows directly from Proposition 2.4. □

3 Class Field Theory

3.1 Hilbert Class Field

We define the Hilbert class field L of a number field K as the maximal unramified Abelian extension of K. To explicate this notion, we need to define what Abelian and unramified mean in this context.

Definition 3.1.1 A field extension K $\subset$ L is *Abelian* if it is Galois and Gal(L/K) is an Abelian group.

To define the notion of unramified field extension, we need to define two classes of primes: finite and infinite primes. While a finite prime $\mathfrak{p}$ is simply a prime ideal of $\mathcal{O}_K$, an infinite prime is defined as follows:

Definition 3.1.2 Given any extension K $\subset$ L,

(i) A *real infinite prime* of K is an embedding σ: K $\longrightarrow \mathbb{R}$.

(ii) A *complex prime* of K is a pair of complex conjugate embeddings $\sigma, \bar{\sigma}$: K $\longrightarrow \mathbb{C}$, $\sigma \neq \bar{\sigma}$.

(iii) An infinite prime σ of K ramifies in L if σ is real but its extension in L are a pair of conjugate complex embeddings, i.e., a complex prime.

(iv) L is unramified if it is unramified at all primes, finite or infinite.

The following statement establishes the existence of Hilbert class field. Note that this result is nontrivial and we will need the main theorems of class field theory in section 3.5 to prove it.

Theorem 3.1.3 Given a number field K, there is a finite Galois extension L such that:

(i) L is an unramified Abelian extension of K.

(ii) Any unramified Abelian extension of K is contained in L.

To further explicate the notion of Hilbert class field, we use the *Artin symbol* to connect the Hilbert class field L with $\mathcal{O}_K$. For any given $\mathfrak{p}$ unramified in L, and for any $\mathfrak{P}$ containing $\mathfrak{p}$, recall that the Artin symbol is defined for $\mathfrak{P}$ as $\left(\frac{L/K}{\mathfrak{P}}\right)$. In the case of an Abelian field extension, the Artin symbol depends only on $\mathfrak{p}$ and is therefore denoted as $\left(\frac{L/K}{\mathfrak{p}}\right)$. To see this, let $\mathfrak{P}'$ be another prime containing $\mathfrak{p}$, then there exists a $\sigma \in$ Gal(L/K), such that $\sigma\mathfrak{P} = \mathfrak{P}'$. Thus

$$\left(\frac{L/K}{\mathfrak{P}'}\right) = \left(\frac{L/K}{\sigma\mathfrak{P}}\right) = \sigma\left(\frac{L/K}{\mathfrak{P}}\right)\sigma^{-1} = \left(\frac{L/K}{\mathfrak{P}}\right) \text{ if Gal(L/K) is Abelian}$$

Thus, when K $\subset$ L is an unramified Abelian extension, $\left(\frac{L/K}{\mathfrak{p}}\right)$ is defined for all $\mathfrak{p}$ in $\mathcal{O}_K$. Now, let I_K be the set of all fractional ideals of $\mathcal{O}_K$. By Proposition 1.4, any fractional ideal $\mathfrak{a}$ of $\mathcal{O}_K$ can be factored into unique product of primes:

$$\mathfrak{a} = \prod_{j=1}^{n} \mathfrak{p}_j^{r_j},\ r_i \in \mathbb{Z},$$

and then we define the Artin symbol $\left(\frac{L/K}{\mathfrak{a}}\right)$ as

$$\left(\frac{L/K}{\mathfrak{a}}\right) = \prod_{j=1}^{n} \left(\frac{L/K}{\mathfrak{p}_i}\right)^{r_i}.$$

The Artin symbol thus defines a homomorphism, called the *Artin map*, as

$$\left(\frac{L/K}{\cdot}\right)\colon I_K \longrightarrow \mathrm{Gal(L/K)}.$$

With the above definitions, we state one of the main theorems of Hilbert class field to see the relation between the class group of $\mathcal{O}_K$ and the Galois group of L/K. The proof of the following results can be found in Cox [1, §5]:

Theorem 3.1.4 (*Artin Reciprocity Theorem for the Hilbert Class Field*) If L is the Hilbert class field of a number field K, then the Artin map

$$\left(\frac{L/K}{\cdot}\right)\colon I_K \longrightarrow \mathrm{Gal(L/K)}$$

is surjective, and its kernel is exactly the subgroup P_K of principal fractional ideals. Thus the Artin map induces an isomorphism

$$C(\mathcal{O}_K) \cong \mathrm{Gal(L/K)}.$$

A consequence of the theorem is that it describes the structure of the maximal unramified Abelian field extension in terms of $\mathcal{O}_K$ alone (in terms of $C(\mathcal{O}_K)$, in fact), and thus leads to the following result, using the fundamental theorem of Galois theory:

Corollary 3.1.5 (*Class field theory for unramified Abelian extensions*) Given a number field K, there is a one-to-one correspondence between unramified Abelian extensions M of K and subgroups H of the ideal class group $C(\mathcal{O}_K)$. If the extension K $\subset$ M corresponds to the subgroup H $\subset C(\mathcal{O}_K)$, then the Artin map induces an isomorphism:

$$C(\mathcal{O}_K)/\mathrm{H} \cong \mathrm{Gal(M/K)}.$$

Another consequence of Theorem 3.1.3 is that it describes how a prime $\mathfrak{p}$ in $\mathcal{O}_K$ splits in the Hilbert class field:

Corollary 3.1.6 Let L be the Hilbert class field of a number field K, and let $\mathfrak{p}$ be a prime ideal of K. Then

$$\mathfrak{p} \text{ splits completely in L} \iff \mathfrak{p} \text{ is principal.}$$

Proof. By Corollary 1.2.5, $\mathfrak{p}$ splits completely *iff* $\left(\frac{L/K}{\mathfrak{p}}\right) = 1$. Since the Artin map induces an isomorphism $C(\mathcal{O}_K) \cong \mathrm{Gal(L/K)}$, the pre-image of 1 in the ideal class group is the trivial class. This is the case *iff* $\mathfrak{p}$ is principal. Thus, $\mathfrak{p}$ splits completely in L *iff* $\mathfrak{p}$ is principal. □

3.2 $p = x^2 + ny^2$ for infinitely n's (1)

In this section, we apply theorems from Hilbert class field and elementary algebraic number theory to give solution for $x^2 + ny^2 = p$ for infinitely many n's. We basically want to prove the following theorem:

Theorem 3.2.1 Let $n > 0$ be an integer satisfying the following condition:

$$n \text{ is square-free, } n \not\equiv 3(4).$$

Then, there is a monic irreducible polynomial $f_n(\mathrm{x}) \in \mathbb{Z}[x]$ of degree $h(\text{-}4n)$ (this is the class number of the form class group $C(D)$ which will appear in section 3.4. Readers unfamiliar with this concept should consult Cox[1, Theorem 3.9]. We need the fact that $h(\text{-}4n) = h(\mathcal{O}_K)$.) such that if an odd prime p divides neither n nor the discriminant of $f_n(\mathrm{x})$, then

$$p = x^2 + ny^2 \text{ for some integer } x \text{ and } y \iff \begin{cases} (-n/p) = 1, \\ \exists a \in \mathbb{Z}, f_n(a) \equiv 0(p) \end{cases}$$

Furthermore, $f_n(\mathrm{x})$ may be taken to be the minimal polynomial of a real algebraic integer α for which $\mathrm{L} = \mathrm{K}(\alpha)$ is the Hilbert class field of $\mathrm{K} = \mathbb{Q}(\sqrt{-n})$.

Proof. To prove this theorem, the first step is to relate the prime $p = x^2 + ny^2$ to the behavior of p (how it splits or ramifies) in the Hilbert class field of K. For this, we need the following theorem:

Theorem 3.2.2 Let L be the Hilbert class field of $\mathrm{K} = \mathbb{Q}(\sqrt{-n})$. Assume that $n > 0$ satisfies the condition: n is square-free and $n \not\equiv 3(4)$, so that $\mathcal{O}_K = \mathbb{Z}[\sqrt{-n}]$. If p is an odd prime not dividing n, then

$$p = x^2 + ny^2 \iff p \text{ splits completely in L.}$$

Proof. Since n is square-free and $n \not\equiv 3(4)$, by Corollary 2.2 $\mathcal{O}_K = \mathbb{Z}[\sqrt{-n}]$ and $d_K = \text{-}4\mathrm{n}$. Let p be an odd prime not dividing n, we know that p is unramified in K by Proposition 2.4. We want to prove the following equivalences:

$p = x^2 + ny^2$

$\iff p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$, $\mathfrak{p} \neq \bar{\mathfrak{p}}$, $\mathfrak{p}$ principal in $\mathcal{O}_K$

$\iff p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$, $\mathfrak{p}$ splits completely in L

$\iff p$ splits completely in L.

For the first equivalence, suppose $p = x^2 + ny^2 = (x + y\sqrt{-n})(x - y\sqrt{-n})$. Set $\mathfrak{p} = (\mathrm{x} + y\sqrt{-n})\mathcal{O}_K$, then $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$ must be prime factorization in $\mathcal{O}_K$. $\mathfrak{p} \neq \bar{\mathfrak{p}}$ because p is unramified. Conversely, suppose $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$, where $\mathfrak{p}$ is principal. Since $\mathcal{O}_K = \mathbb{Z}[\sqrt{-n}]$, we can write $\mathfrak{p} = (x + y\sqrt{-n})\mathcal{O}_K$, which implies $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}} = (x^2 + ny^2)\mathcal{O}_K$. Thus $p = x^2 + ny^2$.

The second equivalence follows from Corollary 3.1.6. To prove the last equivalence, we need the following lemmas:

Lemma 3.2.3 Let L be the Hilbert class field of an imaginary quadratic field K, and let τ be the complex conjugation. Then $\tau(\mathrm{L}) = \mathrm{L}$, and hence L is Galois over $\mathbb{Q}$.

Proof. To prove $\tau(\mathrm{L}) = \mathrm{L}$, note that $\tau(\mathrm{L})$ is an unramified Abelian extension of $\tau(\mathrm{K}) = \mathrm{K}$. Since L is the maximal unramified Abelian extension of L, $\tau(\mathrm{L}) \subset \mathrm{L}$. Since $\tau(\mathrm{L})$ and L have the same degree over K, $\tau(\mathrm{L}) = \mathrm{L}$.

To prove that $\tau(\mathrm{L}) = \mathrm{L}$ implies L is Galois over $\mathbb{Q}$, consider F to be a Galois extension of $\mathbb{Q}$ that contains L. Let $\mathrm{G} = \mathrm{Gal}(\mathrm{F}/\mathbb{Q})$, let A, B $\subset$ G be the subgroups that fix L and K respectively. Then we want to show that $\tau\mathrm{A} = \mathrm{A}\tau$ implies A is a normal subgroup of G.

To show this, note that L is Galois over K implies that A is a normal subgroup of B. Since K is an imaginary quadratic field, $\mathrm{G}/\mathrm{B} = \{1, \tau\}$. Then every element of G can be written as β or $\tau\beta$ for some $\beta \in$ B. Because A is normal in B, it follows that A is normal in G. Hence L is Galois over $\mathbb{Q}$. □

Lemma 3.2.4 If K $\subset$ M $\subset$ L, where M and L are Galois over K, then a prime $\mathfrak{p}$ in $\mathcal{O}_K$ splits completely in L *iff* it splits completely in M and some prime of $\mathcal{O}_M$ containing $\mathfrak{p}$ splits completely in L.

Proof. If $\mathfrak{p}$ splits completely in L, then by tower law of the ramification index and inertia degree, $\mathfrak{p}$ splits completely in M and some prime of $\mathcal{O}_M$ containing $\mathfrak{p}$ splits completely in L.

Conversely, if P is a prime in $\mathcal{O}_M$ such that $P = \mathfrak{P}_1 ... \mathfrak{P}_g$ in $\mathcal{O}_L$, then the $\mathfrak{P}_i$'s are in the prime decomposition of $\mathfrak{p}$. Since L/K is Galois, this means for every i, $e(\mathfrak{P}_i|\mathfrak{p}) = e$, $f(\mathfrak{P}_i|\mathfrak{p}) = f$. By tower law, these common values e and f are both 1. The result follows. □

Since p is a prime in $\mathbb{Z}$ that splits in $\mathcal{O}_K$, and since a prime $\mathfrak{p}$ in $\mathcal{O}_K$ containing p splits completely in $\mathcal{O}_L$, the final equivalence follows from Lemma 3.2.4. Thus,

$$p = x^2 + ny^2 \iff p \text{ splits completely in L.}$$

□

The second step in proving Theorem 3.2.1 is to give a more elementary way of saying how p splits in L:

Theorem 3.2.5 Let K be an imaginary quadratic field, and let L be a finite extension of K which is Galois over $\mathbb{Q}$. Then

(i) There is a real algebraic integer α such that L = K(α)

(ii) Given α as in (i), let $f(\mathrm{x}) \in \mathbb{Z}[\mathrm{x}]$ denote its minimal polynomial. If p is a prime not dividing the discriminant of $f(\mathrm{x})$, then

$$\text{p splits completely in L} \iff \begin{cases} (d_K/p) = 1, \\ \exists a \in \mathbb{Z}, f_n(a) \equiv 0(p) \end{cases}$$

Proof. To prove (i), we need the following lemma:

Lemma 3.2.6 Let K be an imaginary quadratic field, K $\subset$ L be Galois. Then if L is Galois over $\mathbb{Q}$,

(i) [L$\cap\mathbb{R}$:$\mathbb{Q}$] = [L:K].

(ii) For $\alpha \in$ L$\cap\mathbb{R}$, L$\cap\mathbb{R}$ = $\mathbb{Q}(\alpha) \iff$ L = K(α)

Proof. To prove (i), note that L$\cap\mathbb{R}$ is the fixed field of complex conjugation. Then, by Lemma 3.2.3, $[\mathrm{L} \cap \mathbb{R} : \mathbb{Q}] = [\mathrm{L} : \mathrm{K}]$.

To prove (ii), let $f(x) \in \mathbb{Z}[x]$ be the minimal polynomial of α over $\mathbb{Q}$. We need to prove that $f(x)$ is irreducible over K. Suppose that

$$f(\mathrm{x}) = p_1(\mathrm{x})p_2(\mathrm{x})...p_n(\mathrm{x}),\ p_i(x)\text{'s irreducible over K.}$$

Then, since $f(\mathrm{x})$ splits in L, there exists some i such that $p_i(\alpha) = 0$. Without loss of generality, let $p_1(\alpha) = 0$. The splitting field M of $p_1(\alpha)$ is therefore M = K(α). Since $\alpha \in \mathbb{R}$, τ(M) = M where τ is the complex conjugation. By Lemma 3.2.3, we know that M is thus Galois over $\mathbb{Q}$. It follows that f splits in M and thus $[\mathrm{M} : \mathbb{Q}] > \deg(f) = [\mathrm{L} \cap \mathbb{R} : \mathbb{Q}]$. But since M $\subset$ L and $[\mathrm{L} : \mathrm{L} \cap \mathbb{R}] = [\mathrm{K} : \mathbb{Q}]$, M = L. This implies

$$[\mathrm{L} : \mathrm{K}] = \deg(p_1) < \deg(f) = [\mathrm{L} \cap \mathbb{R} : \mathbb{Q}] = [\mathrm{L} : \mathrm{K}],$$

which is a contradiction. Thus, f is irreducible over K and the result follows. □

Thus, if $\alpha \in \mathcal{O}_L\cap\mathbb{R}$ satisfies L$\cap\mathbb{R}$ = $\mathbb{Q}(\alpha)$, then L = K(α) and (i) is proved.

To prove (ii), consider the minimal polynomial of $\alpha \in \mathrm{L} \cap \mathbb{R}$ $f(x)$ over $\mathbb{Q}$. Then, since [L : K] = $[\mathrm{L} \cap \mathbb{R} : \mathbb{Q}]$, $f(x)$ is the minimal polynomial of α over K. Then if p is a prime not dividing the discriminant of $f(x)$, this implies

$$f(x) \equiv f_1(x)...f_n(x) \pmod{p} \text{ for some } n > 1.$$

Then by Proposition 1.2.6 and Corollary 2.5, p is unramified and thus $\left(\frac{d_K}{p}\right) = 1$. We've assumed that p splits completely in L, thus

$$\mathbb{Z}/p\mathbb{Z} \cong \mathcal{O}_K/\mathfrak{p}, \text{ for } p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}.$$

Thus, since $f(x)$ is separable over $\mathbb{Z}/p\mathbb{Z}$, it is separable over $\mathcal{O}_K/\mathfrak{p}$. Since $\mathfrak{p}$ splits completely in L, we have

$$f(x) \equiv 0 \pmod{\mathfrak{p}} \text{ is solvable in } \mathcal{O}_K$$

and, because $\mathbb{Z}/p\mathbb{Z} \cong \mathcal{O}_K/\mathfrak{p}$, implies

$$f(x) \equiv 0 \pmod{p} \text{ is solvable in } \mathbb{Z}.$$

Thus, Theorem 3.2.5 is proved. □

Now, we can prove the main equivalence in Theorem 3.2.1. Since the Hilbert class field L of K is Galois over $\mathbb{Q}$, Theorem 3.2.5 implies that there exists $\alpha \in L \cap \mathbb{R}$ such that $L = K(\alpha)$. Let $f_n(x)$ be the minimal polynomial of α over K, and let p be a prime not dividing n and the discriminant of $f_n(x)$, then by Theorem 3.22 $p = x^2 + ny^2$ implies that p splits completely in L, which by Theorem 3.2.5 implies that $(-n/p) = 1$ and $f_n(x) \equiv 0 \pmod{p}$ has an integer solution.

Recall that n satisfies the condition of Theorem 3.2.1, and thus $d_K = -4n$, and $(d_K/p) = (-n/p)$.

It remains to show that the degree of $f_n(x)$ is the class number $h(-4n)$. Note that by Theorem 3.1.4, $f_n(x)$ has degree

$$[L : K] = |\mathrm{Gal}(L/K)| = |C(\mathcal{O}_K)|.$$

In section 3.4 (Proposition 3.4.9) we will mention a key isomorphism between the ideal class group and form class group of $\mathcal{O}_K$. We know how to compute the order of the form class group $|C(d_K)| = h(-4n)$. Thus the degree of the polynomial is $|C(\mathcal{O}_K)| = h(-4n)$. And we are done. □

3.3 Example: $p = x^2 + 5y^2$

Now we do an example of quadratic form for $n = 5$. By Theorem 3.2.5, we have that

Proposition 3.3.1 For $K = \mathbb{Q}(\sqrt{-5})$ and L its Hilbert class field:

(i) There exists some $\alpha \in \mathcal{O}_L \cap \mathbb{R}$ such that $L = K(\alpha)$,

(ii) $(d_K/p) = 1$ and the minimal polynomial of α over K has an integer solution modulo p.

Our first goal is to find α that satisfies $K(\alpha)$ is the maximal unramified Abelian extension.

Theorem 3.3.2 Given $K = \mathbb{Q}(\sqrt{-5})$, the Hilbert class field is $L = K(\sqrt{-1})$.

Proof. To find α such that $L = K(\alpha)$, we need to firstly find [L:K]. We do this by looking at the ideal class group $C(\mathcal{O}_K)$ which by Theorem 3.1.4 is isomorphic to Gal(L/K):

Proposition 3.3.3 For $K = \mathbb{Q}(\sqrt{-5})$, the order of $Cl(\mathcal{O}_K)$ is 2.

Proof. To prove this proposition, recall the statement on *Minkowski bound*: for a number field K, there exists some constant $M_K \in \mathbb{R}$ (this constant is called the Minkowski bound) such that for every ideal class in $\mathcal{O}_K$, there is a representative $\mathfrak{a}$ such that $\mathrm{Nm}(\mathfrak{a}) \leq M_K$. In other words, the class number h_K of K is equal to the number of ideals whose norm is bounded by M_K. Specifically, the Minkowski bound is given by:

$$M_K = \sqrt{|d_K|}(\tfrac{4}{\pi})^{r_2}\tfrac{n!}{n^n}$$

where $n = [K:\mathbb{Q}]$ and $2r_2$ is the number of complex embeddings. Thus, we have for $K = \mathbb{Q}(\sqrt{-5})$:

$$M_K = \sqrt{20}(\tfrac{4}{\pi})^1\tfrac{2!}{2^2} = 2.84... < 3.$$

Since $\mathrm{Nm}(\mathfrak{l}) \in \mathbb{Z}$ for any ideal $\mathfrak{l}$ in $\mathcal{O}_K$, $\mathrm{Nm}(\mathfrak{l}) = 1$ or 2. Thus, we easily have:

$$Nm(\mathfrak{l}) = \begin{cases} 1, & \text{if } \mathfrak{p} = \mathbb{O}_K. \\ 2, & \text{if } \mathfrak{p} \text{ lies over } 2. \end{cases} \tag{3}$$

For the second case, we check how 2 decomposes in terms of $\mathfrak{l}$ by checking how the minimal polynomial $f(x) = x^2 + 5$ of $\sqrt{-5}$ splits modulo 2:

$$f(x) \equiv (x+1)^2 \bmod 2$$

Thus, $\mathfrak{l} = (2, 1 + \sqrt{-5})$ is the unique ideal lying over 2. Note also that $(2, 1 + \sqrt{-5}) \neq \mathcal{O}_K$. Thus $h_K = |C(\mathcal{O}_K)| = 2$. We finally have:

$$|C(\mathcal{O}_K)| = |\mathrm{Gal}(L/K)| = [L:K] = 2$$

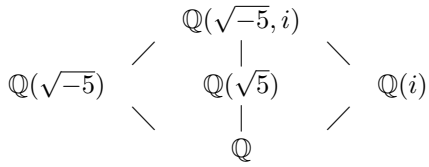
□

The second step is to find α specifically. The process is not a proof *per se*, since we basically do this by trying each possible square-free integer in $\mathbb{C}$ that is not in K. Finding α for the Hilbert class field of $K = \mathbb{Q}(\sqrt{-5})$ is relatively simple, because [L:K] =2 and, as we will show, $\alpha = \sqrt{-1}$.

Set $\alpha = \sqrt{-1}$. We know that if $L = K(\sqrt{-1})$ is an unramified Abelian extension, then it is maximal, because [L:K] = 2. But a quadratic extension is clearly Abelian. Thus, in order to prove that $L = K(\sqrt{-1})$, we want to prove the following statement:

Proposition 3.3.4 For $K = \mathbb{Q}(\sqrt{-5})$, $L = K(\sqrt{-1})$ is an unramified field extension.

Proof. Consider the following lattice diagram:



Note that $L = \mathbb{Q}(\sqrt{-5},\ i)$ contains a third intermediate field $M = \mathbb{Q}(\sqrt{5})$ which is the product of K and $\mathbb{Q}(i)$. In order to check that all primes in $\mathbb{Q}(\sqrt{-5})$ are unramified in L, we only need to verify that all primes in $\mathbb{Q}$ are unramified in $\mathbb{Q}(i)$ (this is true because we are checking those primes in $\mathbb{Q}(\sqrt{-5})$ which lie over primes in $\mathbb{Q}$).

Let $\mathbb{Q}(i)$ be denoted as F. Then, d_F = -4 by Corollary 2.2. The only prime in $\mathbb{Q}$ dividing -4 is 2. Thus all primes in $\mathbb{Q}$ except 2 are unramified in $\mathbb{Q}(i)$. Now, we need to check that the prime $\mathfrak{p}$ in $\mathbb{Q}(\sqrt{-5})$ lying over 2 is unramified in L. Recall that

$$2\mathcal{O}_K = (2, 1 + \sqrt{-5})^2.$$

Before proceeding, we make a modification on notation for the sake of simplicity: Since L/K, L/M, M/$\mathbb{Q}$, and L/$\mathbb{Q}$ are all Galois, the ramification index only depends on the prime in the base field. Thus, we denote the ramification index of $\mathfrak{p} \subset \mathcal{O}_K$ in L, $\mathfrak{q} \subset \mathcal{O}_M$ in L, 2 $\in \mathbb{Q}$ in M, 2 $\in \mathbb{Q}$ in K, and 2 $\in \mathbb{Q}$ in L as, respectively,

$$e_L(\mathfrak{p}),\ e_L(\mathfrak{q}),\ e_M(2),\ e_K(2),\ e_L(2).$$

Thus, we want to show that $e_L(\mathfrak{p}) = 1$ for $\mathfrak{p} = (2,\ 1 + \sqrt{-5})$. Note that because $e_K(2) = 2$, it follows by tower law that $e_L(2) = e_K(2)e_L(\mathfrak{p}) = 2e_L(\mathfrak{p})$. Thus, we want to show that $e_L(2) = 2$ and the desired result will follow.

To show $e_L(2) = 2$, note that

$$e_L(2) = e_M(2)e_L(\mathfrak{q}).$$

Since 2 does not divide $d_M = 5$, 2 is unramified in M and $e_M(2) = 1$. Then

$$e_L(2) = e_M(2)e_L(\mathfrak{q}) = 1 \cdot e_L(\mathfrak{q}) = e_L(\mathfrak{q}) \leq [\mathrm{L} : \mathrm{M}] = 2$$

hence $e_L(2) = 2$, and $e_L(\mathfrak{p}) = 1$. Thus, $L = K(\sqrt{-1})$ is unramified.

□

Having proved this, one also easily finds that $\mathcal{O}_L = \mathcal{O}_K[\frac{1+\sqrt{5}}{2}]$. The minimal polynomial of $\frac{1+\sqrt{5}}{2}$ is $f(x) = x^2$ - x - 1. Set $f(x) \equiv 0$(p), we have the discriminant of $f(x)$ is $\frac{1\pm\sqrt{5}}{2}$. But $f(x)$ has a solution modulo p if and only if its discriminant is a square modulo p. Thus

$$\tfrac{1\pm\sqrt{5}}{2} \text{ is a square modulo } p.$$

Thus, we must have $(\frac{5}{p}) = 1$.

Since we know from Proposition 3.3.1 that $(\frac{d_K}{p}) = (\frac{-20}{p}) = (\frac{-5}{p}) = (\frac{5}{p})(\frac{-1}{p}) = 1$. Thus: $(\frac{-1}{p}) = (\frac{5}{p}) = 1$. This is the case *iff* $p \equiv 1(4)$ and $p \equiv 1$ or $4(5)$. Thus, $p \equiv 1$ or $9(20)$. And we finally have:

$$p = x^2 + 5y^2 \text{ for some integers } x \text{ and } y \iff p \equiv 1 \text{ or } 9(20)$$

□

3.4 Orders in Imaginary Quadratic Fields

In 3.1 and 3.2, we've solved for our question of when p is of the form $x^2 + ny^2$ for infinitely many n's for which $\mathbb{Z}[\sqrt{-n}]$ is the full ring of integers $\mathcal{O}_K$ in K = $\mathbb{Q}(\sqrt{-n})$. The solution, however, leaves out infinitely many other n's, for which $\mathbb{Z}[\sqrt{-n}]$ is not the full ring of integers in K but only a special kind of subring called an *order*. To completely solve the problem, we therefore need to understand orders in imaginary quadratic fields, and the stronger tools of class field theory. We start with some basic definitions:

Definition 3.4.1 An order $\mathcal{O}$ in a quadratic field K is a subset $\mathcal{O} \subset$ K such that

(i) $\mathcal{O}$ is a subring of K containing 1.

(ii) $\mathcal{O}$ is a finitely generated $\mathbb{Z}$-module.

(iii) $\mathcal{O}$ contains a $\mathbb{Q}$-basis of K.

Note that (ii) and (iii) imply that $\mathcal{O}$ is a free $\mathbb{Z}$-module of rank 2, and K is the field of fractions of $\mathcal{O}$. Note also that the ring of integers $\mathcal{O}_K$ is always an order: (i) and (ii) imply that $\mathcal{O} \subset \mathcal{O}_K$ for any order $\mathcal{O}$, so that $\mathcal{O}_K$ is the maximal order.

To fully describe an order in imaginary quadratic field K, recall from Corollary 2.2 that the maximal order can be written as

$$\mathcal{O}_K = [1,\omega_K],\ \omega_K = \frac{d_K+\sqrt{d_K}}{2}$$

where d_K is the discriminant of K. Using this, we have the following lemma:

Lemma 3.4.2 Let $\mathcal{O}$ be an order in a quadratic field K of discriminant d_K. Then $\mathcal{O}$ has finite index in $\mathcal{O}_K$. If we set $f = [\mathcal{O}_K{:}\mathcal{O}]$, then

$$\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K = [1,\ f\omega_K].\ f \text{ is called the } \textit{conductor} \text{ of the order.}$$

Proof. This is an elementary fact in algebraic number theory. For proof, see Cox[1, §7]. □

Besides the conductor, another important invariant of an order is its *discriminant*. Let $\alpha \mapsto \alpha$' to be the nontrivial automorphism of K, and let $\mathcal{O} = [\alpha,\ \beta]$. Then by definition, the discriminant of $\mathcal{O}$ is the number D

$$D = \left(det\begin{pmatrix} \alpha & \beta \\ \alpha' & \beta' \end{pmatrix}\right)^2$$

And by Lemma 3.4.2, we have

$$D = f^2 d_K.$$

Now we study the ideals of an order $\mathcal{O}$. The proof of Proposition 1.1.2 easily adapts to show that $\mathcal{O}/\mathfrak{a}$ is finite for any $\mathfrak{a}$ a non-zero $\mathcal{O}$-ideal. Define the *norm* of $\mathfrak{a}$ to be $\mathrm{Nm}(\mathfrak{a}) = |\mathcal{O}/\mathfrak{a}|$. It is a general fact that $\mathcal{O}$ is not a Dedekind domain when $f > 1$ (because it is not integrally closed). Thus we do not have a unique factorization of ideals in $\mathcal{O}$.

To remedy the situation, we introduce the notion of a proper ideal:

Definition 3.4.3 An $\mathcal{O}$-ideal $\mathfrak{a}$ is called a *proper ideal* of $\mathcal{O}$ if

$$\mathcal{O} = \{\beta \in K : \beta\mathfrak{a} \subset \mathfrak{a}\}.$$

Note that any $\mathcal{O}$-ideal satisfies $\mathcal{O} \subset \{\beta \in K : \beta\mathfrak{a} \subset \mathfrak{a}\}$ by the definition of an ideal. But it is not always the case that equality holds. For example, if $\mathcal{O} = \mathbb{Z}[\sqrt{-3}]$ is the order of conductor 2 in K = $\mathbb{Q}(\sqrt{-3})$, and $\mathfrak{a} = (2,\ 1 + \sqrt{-3})$, then one can easily check that

$$\mathcal{O} \neq \{\beta \in K : \beta\mathfrak{a} \subset \mathfrak{a}\} = \mathcal{O}_K.$$

In order to study the ideal class group for the order $\mathcal{O}$, we also define fractional ideals of $\mathcal{O}$ to be of the form $\alpha\mathfrak{a}$, $\alpha \in U$(K) and $\mathfrak{a}$ is an $\mathcal{O}$-ideal. Furthermore, we need to define an *invertible ideal* $\mathfrak{a}$ in $\mathcal{O}$ to be the $\mathcal{O}$-ideal for which there exists another $\mathcal{O}$-ideal $\mathfrak{b}$ such that $\mathfrak{ab} = \mathcal{O}$. We have the following fact:

Proposition 3.4.4 Let $\mathcal{O}$ be an order in a quadratic field K, and let $\mathfrak{a}$ be a fractional $\mathcal{O}$-ideal. Then $\mathfrak{a}$ is proper *iff* $\mathfrak{a}$ is invertible.

Proof. For proof, see Cox[1, Proposition 7.4]. □

Given an order $\mathcal{O}$, we can now define $I(\mathcal{O})$ to be the set of proper fractional-ideals of $\mathcal{O}$. By Proposition 3.4.4, we know that $I(\mathcal{O})$ is a group under multiplication. The principal ideals of $\mathcal{O}$ give a subgroup $P(\mathcal{O}) \subset I(\mathcal{O})$. Thus we define the ideal class group of $\mathcal{O}$ to be:

$$C(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O}).$$

Having defined the class group for an order $\mathcal{O}$ in imaginary quadratic field K, we wish to relate $C(\mathcal{O})$ to the behavior of $\mathcal{O}_K$ for which we have sufficient knowledge. Specifically, the goal of this section is to prove the following major isomorphism:

$$\mathrm{C}(\mathcal{O}) \cong I(\mathcal{O},f)/P(\mathcal{O},f) \cong I_K(f)/P_{K,\mathbb{Z}}(f).$$

Once we achieve this, it becomes clear that there exists a relation between $C(\mathcal{O})$ and the Galois group of some field extension L of K, under the Artin map that we encounter in section 3.1 (note that although we defined the Artin map in the context of Hilbert class field extension of K, there is a natural version of it that makes sense for any abelian extension L/K). We will do this in the next section. But before this, in order to establish the relation between $C(\mathcal{O})$ and $\mathcal{O}_K$, we need the notion of an $\mathcal{O}$-ideal which is prime to the conductor f:

Definition 3.4.7 Given an order $\mathcal{O}$ of conductor f, we say that a nonzero $\mathcal{O}$-ideal $\mathfrak{a}$ is prime to f if $\mathfrak{a} + f\mathcal{O} = \mathcal{O}$.

This type of ideal has the following basic properties:

Lemma 3.4.8 Let $\mathcal{O}$ be an order of conductor f, then

(i) An $\mathcal{O}$-ideal is prime to f *iff* its norm is relatively prime to f.

(ii) Every $\mathcal{O}$-ideal prime to f is proper.

Proof. Given any $\mathcal{O}$-ideal $\mathfrak{a}$ prime to the conductor:

To prove (i), consider the map m_f: $\mathcal{O}/\mathfrak{a} \longrightarrow \mathcal{O}/\mathfrak{a}$ be given by multiplication by f. Then by definition of the quotient map

$$\mathfrak{a} + f\mathcal{O} = \mathcal{O} \iff m_f \text{ is surjective} \iff m_f \text{ is an isomorphism.}$$

By the structure theorem for finite Abelian groups, m_f is isomorphism *iff* f is relatively prime to the order of $\mathcal{O}/\mathfrak{a}$ (which is $\mathrm{Nm}(\mathfrak{a})$). Thus we are done with (i).

To prove (ii), let $\beta \in$ K satisfy $\beta\mathfrak{a} \subset \mathfrak{a}$. Then $\beta \in \mathcal{O}_K$ since it is in $\mathcal{O}$. Note that

$$\beta\mathcal{O} = \beta(\mathfrak{a} + f\mathcal{O}) = \beta\mathfrak{a} + \beta f\mathcal{O} \subset \mathfrak{a} + f\mathcal{O}_K.$$

And thus $\beta\mathcal{O} \subset$ since $f\mathcal{O}_K \subset \mathcal{O}$. Thus $\beta \in \mathcal{O}$, and we are done. □

It follows that the $\mathcal{O}$-ideals prime to the conductor lie naturally in $I(\mathcal{O})$ and are closed under multiplication (since $\mathrm{Nm}(\mathfrak{ab}) = \mathrm{Nm}(\mathfrak{a})\mathrm{Nm}(\mathfrak{b})$ is prime to f). Denote the subgroup generated by these ideals as $I(\mathcal{O},f) \subset I(\mathcal{O})$. And we have $P(\mathcal{O},f) \subset I(\mathcal{O},f)$ be the set of principal ideals $\alpha\mathcal{O}$ where $\alpha \in \mathcal{O}$ has norm prime to f. We can describe $C(\mathcal{O})$ using $I(\mathcal{O},f)$ and $P(\mathcal{O},f)$:

Proposition 3.4.9 The inclusion $I(\mathcal{O},f) \subset I(\mathcal{O})$ induces an isomorphism:

$$I(\mathcal{O},f)/P(\mathcal{O},f) \cong I(\mathcal{O})/P(\mathcal{O}) = C(\mathcal{O}).$$

Proof. To prove this, we need the following lemma:

Lemma 3.4.10 Any ideal class in $C(\mathcal{O})$ contains an $\mathcal{O}$-ideal prime to its conductor.

Proof. The proof of this lemma is based on knowledge of the form class group $C(D)$. Specifically, it is based on the fact that $C(D) \cong C(\mathcal{O})$. For information on form class group and the proof of this lemma, see Cox[1, Theorem 7.7]. □

By Lemma 3.4.10, we know that the map $I(\mathcal{O},f) \to C(\mathcal{O})$ is surjective. Its kernel is obviously $I(\mathcal{O},f) \cap P(\mathcal{O})$ since any principal $\mathcal{O}$-ideal is in the trivial class of $C(\mathcal{O})$. We want to show $I(\mathcal{O},f) \cap P(\mathcal{O}) = P(\mathcal{O},f)$.

It is obvious that $P(\mathcal{O},f) \subset I(\mathcal{O},f) \cap P(\mathcal{O})$, but we need to show the other direction. Any fractional ideal in $I(\mathcal{O},f) \cap P(\mathcal{O})$ can be written as $\alpha\mathcal{O} = \mathfrak{ab}^{-1}$ where $\alpha \in$ K and $\mathfrak{a}$ and $\mathfrak{b}$ are $\mathcal{O}$-ideals prime to the conductor. Note that $\mathrm{Nm}(\mathfrak{b})\mathcal{O} = \mathfrak{b}\bar{\mathfrak{b}}$ is in $P(\mathcal{O},f)$. Also, we have $\mathrm{Nm}(\mathfrak{b})\mathfrak{b}^{-1} = \bar{\mathfrak{b}}$. Thus

$$\mathrm{Nm}(\mathfrak{b})\alpha\mathcal{O} = \mathfrak{a}(\mathrm{Nm}(\mathfrak{b})\mathfrak{b}^{-1}) = \mathfrak{a}\bar{\mathfrak{b}} \subset \mathcal{O}.$$

Thus, Nm($\mathfrak{b}$)$\alpha\mathcal{O} \in P(\mathcal{O},f)$. And $\alpha\mathcal{O} = (\text{Nm}(\mathfrak{b})\alpha\mathcal{O})(Nm(\mathfrak{b})\mathcal{O})^{-1}$ is also in $P(\mathcal{O},f)$. □

This lemma helps us relate $C(\mathcal{O})$ to the ideals of the maximal order $\mathcal{O}_K$. To see this, we define, for any given positive integer m, an $\mathcal{O}_K$-ideal prime to m to be an $\mathcal{O}_K$-ideal $\mathfrak{a}$ such that $\mathfrak{a} + m\mathcal{O}_K = \mathcal{O}_K$. One easily checks that this is equivalent to the condition $gcd(\text{Nm}(\mathfrak{a}),m)=1$. Thus, we also have a subgroup $I_K(m) \subset I_K$ the set of all fractional ideals of $\mathcal{O}_K$ that are prime to m.

We can now prove our desired isomorphism which will be used extensively in the theories of ring class field in section 3.6:

Proposition 3.4.11 Let $\mathcal{O}$ be an order of conductor f in an imaginary quadratic field K. Then

$$\text{C}(\mathcal{O}) \cong I(\mathcal{O},f)/P(\mathcal{O},f) \cong I_K(f)/P_{K,\mathbb{Z}}(f)$$

where $P_{K,\mathbb{Z}}(f)$ is the subset of $I_K(f)$ generated by principal ideals of the form $\alpha\mathcal{O}_K$ where $\alpha \equiv a(f\mathcal{O}_K)$ for some $a \in \mathbb{Z}$ such that $gcd(a,f) = 1$.

Proof. To prove this, we need the following basic lemma whose proof is not constructive and is not provided in this paper:

Lemma 3.4.12 Let $\mathcal{O}$ be an order of conductor f in an imaginary quadratic field K. Then

(i) If $\mathfrak{a}$ is an $\mathcal{O}_K$-ideal prime to f, then $\mathfrak{a} \cap \mathcal{O}$ is an $\mathcal{O}$-ideal prime to f of the same norm;

(ii) If $\mathfrak{a}$ is an $\mathcal{O}$-ideal prime to f, then $\mathfrak{a}\mathcal{O}_K$ is an $\mathcal{O}_K$ ideal prime to f of the same norm;

(iii) The map $\mathfrak{a} \mapsto \mathfrak{a} \cap \mathcal{O}$ induces an isomorphism $I_K(f) \cong I(\mathcal{O},f)$, and the inverse map is given by $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_K$.

Proof. For proof, see Cox[1, Proposition 7.20]. □

The first isomorphism comes from Proposition 3.4.9. To prove the second isomorphism, note from Lemma 3.4.12 that $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_K$ induces an isomorphism $I(\mathcal{O},f) \cong I_K(f)$. We need to show that under this isomorphism $P(\mathcal{O},f)$ gets mapped to $P_{K,\mathbb{Z}}(f)$.

We need to first show that for $\alpha \in \mathcal{O}_K$,

$$\alpha \equiv a(f\mathcal{O}_K) \text{ for } a \in \mathbb{Z} \text{ and } gcd(a,f) = 1 \iff \alpha \in \mathcal{O},\ gcd(\text{Nm}(\alpha),f) = 1.$$

Assume $\alpha \equiv a(f\mathcal{O}_K)$, $a \in \mathbb{Z}$ and $gcd(a,f) = 1$. One can check that $\text{Nm}(\alpha) \equiv a^2(f)$ (see Cox[1, Exercise 7.27]). Thus $gcd(\text{Nm}(\alpha),f) = gcd(a^2,f) = 1$. Because $f\mathcal{O}_K \subset \mathcal{O}$, we have that $\alpha \in \mathcal{O}$.

On the other hand, let $\alpha \in \mathcal{O} = [1,f\omega_K]$ with norm prime to f. Write $\alpha = a + bf\omega_K$, thus $\alpha \equiv a(f\mathcal{O}_K)$. Since $gcd(\text{Nm}(\alpha),f) = 1$ and $\text{Nm}(\alpha) \equiv a^2(f)$, $gcd(a,f) = 1$. Thus this proves that

$$\alpha \equiv a(f\mathcal{O}_K) \text{ for } a \in \mathbb{Z} \text{ and } gcd(a,f) = 1 \iff \alpha \in \mathcal{O},\ gcd(\text{Nm}(\alpha),f) = 1.$$

We know that $P(\mathcal{O},f)$ is generated by ideal $\alpha\mathcal{O}$ such that $gcd(\alpha,f) = 1$. Thus under the isomorphism $I(\mathcal{O},f) \cong I_K(f)$, $P(\mathcal{O},f)$ is mapped to the corresponding ideals $\alpha\mathcal{O}_K$. By the equivalence above, we have that $P(\mathcal{O},f)$ is mapped to $P_{K,\mathbb{Z}}(f)$. □

Before going into the general statements of class field theory, we need a statement which gives us the equation for computing $h(\mathcal{O})$:

Theorem 3.4.13 Let $\mathcal{O}$ be the order of conductor f in an imaginary quadratic field K. Then

$$h(\mathcal{O}) = \frac{h(\mathcal{O}_K)f}{[U(\mathcal{O}_K):U(\mathcal{O})]}\prod_{p|f}\Big(1 - \Big(\frac{d_K}{p}\Big)\frac{1}{p}\Big)$$

Proof. For proof, see Cox[1, Theorem 7.24]. □

3.5 Theorems of Class Field Theory

Having studied the basic theorems of Hilbert Class Field and orders in imaginary quadratic fields, we present a classic formulation of class field theory, which describes the notion of Abelian extension of number fields in terms of *generalized ideal class groups*. Before stating the main theorems, we need to define the notion of a *modulus*. Given a number field K, a modulus in K is a formal product

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$$

over all primes $\mathfrak{p}$, finite or infinite, of K, where the exponents satisfy:

(i) $n_{\mathfrak{p}} \geq 0$, and at most finitely many are nonzero.

(ii) $n_{\mathfrak{p}} = 0$ wherever $\mathfrak{p}$ is a complex infinite prime.

(ii) $n_{\mathfrak{p}} \leq 1$ whenever $\mathfrak{p}$ is a real infinite prime.

A modulus $\mathfrak{m}$ thus can be written as $\mathfrak{m}_0\mathfrak{m}_\infty$ where $\mathfrak{m}_0$ is an $\mathcal{O}_K$-ideal and $\mathfrak{m}_\infty$ is a product of distinct real infinite primes of K. In the case of an imaginary quadratic field, the modulus is simply an ideal of $\mathcal{O}_K$.

Definition 3.5.1 Given a modulus $\mathfrak{m}$, we define $I_K(\mathfrak{m})$ to be the subgroup of I_K generated by $\mathcal{O}_K$-ideals that are relatively prime to $\mathfrak{m}$ (i.e., relatively prime to $\mathfrak{m}_0$). We define $P_{K,1}(\mathfrak{m})$ to be the subgroup of $I_K(\mathfrak{m})$ generated by the principal ideals $\alpha\mathcal{O}_K$, where $\alpha \in \mathcal{O}_K$ satisfies:

$$\alpha \equiv 1(\mathfrak{m}_0) \text{ and } \sigma(\alpha) > 0 \text{ for every real infinite prime } \sigma \text{ dividing } \mathfrak{m}_\infty.$$

Definition 3.5.2 A subgroup $\mathrm{H} \subset I_K(\mathfrak{m})$ is called a *congruence subgroup* for $\mathfrak{m}$ if

$$P_{K,1}(\mathfrak{m}) \subset \mathrm{H} \subset I_K(\mathfrak{m}).$$

And the quotient

$$I_K(\mathfrak{m})/\mathrm{H}$$

is called a *generalized ideal class group* for $\mathfrak{m}$.

So far, we've seen two examples of generalized ideal class groups. One easily checks that for $\mathfrak{m} = 1$, $P_{K,1}(1) = P_K$. Thus, P_K is a congruence subgroup and $C(\mathcal{O}_K) = I_K/P_K$ is a generalized ideal class group. Similarly, let $\mathcal{O}$ be an order of conductor f in an imaginary quadratic field K. By Proposition 3.4.11, we have

$$C(\mathcal{O}) \cong I_K(f)/P_{K,\mathbb{Z}}(f).$$

Equivalently, if we set modulus $\mathfrak{m} = f\mathcal{O}_K$, then we have

$$P_{K,1}(f\mathcal{O}_K) \subset P_{K,\mathbb{Z}}(f) \subset I_K(f) = I_K(f\mathcal{O}_K)$$

and thus $P_{K,\mathbb{Z}}(f)$ is a congruence subgroup for $f\mathcal{O}_K$, and $C(\mathcal{O})$ is the corresponding generalized ideal class group.

Having defined the notions above, now we state the three main theorems of class field theory. The basic idea is that the generalized ideal class groups are the Galois groups of all Abelian extensions of K, and the Artin map provides the isomorphism between them. Similar to how we defined the Artin map into the Galois group of the Hilbert class field extension in section 1.2, there exists a map into the Galois group of any Abelian extension:

$$\Phi_{\mathfrak{m}}\colon I_K(\mathfrak{m}) \longrightarrow \mathrm{Gal(L/K)}.$$

And we have the following theorems:

Theorem 3.5.3 (*Artin Reciprocity Theorem*) Let $\mathrm{K} \subset \mathrm{L}$ be an Abelian extension, and let $\mathfrak{m}$ be a modulus divisible by all primes of K, finite or infinite, that ramify in L. Then:

(i) The Artin map $\Phi_{\mathfrak{m}}$ is surjective.

(ii) If the exponents of the finite primes $\mathfrak{m}$ are sufficiently large, then $\ker(\Phi_{\mathfrak{m}})$ is a congruence subgroup for $\mathfrak{m}$ and consequently the isomorphism

$$I_K(\mathfrak{m})/\ker(\Phi_{\mathfrak{m}}) \cong \mathrm{Gal(L/K)}$$

shows that Gal(L/K) is a generalized ideal class group for the modulus $\mathfrak{m}$.

Theorem 3.5.4 (*Conductor Theorem*) Let K $\subset$ L be an Abelian extension. Then there is a modulus $\mathfrak{f} = \mathfrak{f}$(L/K) such that

(i) A prime of K, finite or infinite, ramifies in L *iff* it divides $\mathfrak{f}$.

(ii) Let $\mathfrak{m}$ be a modulus divisible by all primes of K which ramify in L. Then $\ker(\Phi_{\mathfrak{m}})$ is a congruence subgroup for $\mathfrak{m}$ *iff* $\mathfrak{f}|\mathfrak{m}$.

Theorem 3.5.5 (*Existence Theorem*) Let $\mathfrak{m}$ be a modulus of K, and let H be a congruence subgroup for $\mathfrak{m}$. Then there is a unique Abelian extension L of K, all of whose ramified primes, finite or infinite, divide $\mathfrak{m}$, such that if

$$\Phi_{\mathfrak{m}}\colon I_K(\mathfrak{m}) \longrightarrow \mathrm{Gal(L/K)}$$

is the Artin map of K $\subset$ L, then

$$\mathrm{H} = \ker(\Phi_{\mathfrak{m}}).$$

For proofs of the above three theorems, see Janusz[2, Chapter 5]. The next step is to understand them by indicating how they are used. We start by showing the proofs of Kronecker-Weber Theorem and the existence of Hilbert class field, using class field theory. Before that, we may need a key tool which would be involved in both proofs:

Corollary 3.5.6 Let L and M be Abelian extensions of K. Then L $\subset$ M *iff* there is a modulus $\mathfrak{m}$, divisible by all primes of K ramified in M, such that

$$P_{K,1}(\mathfrak{m}) \subset \ker(\Phi_{M/K,\mathfrak{m}}) \subset \ker(\Phi_{L/K,\mathfrak{m}}).$$

Proof. To prove this, we need the following lemma:

Lemma 3.5.7 Let K $\subset$ L be an Abelian extension, and let $\mathfrak{m}$ be a modulus for which the Artin map $\Phi_{\mathfrak{m}}$ is defined. If $\mathfrak{n}$ is another modulus and $\mathfrak{m}|\mathfrak{n}$, then

$$P_{K,1}(\mathfrak{m}) \subset \ker(\Phi_{\mathfrak{m}}) \Longrightarrow P_{K,1}(\mathfrak{n}) \subset \ker(\Phi_{\mathfrak{n}}).$$

Proof. Let $\alpha\mathcal{O}_K \in P_{K,1}(\mathfrak{n})$. We want to show that $\Phi_{\mathfrak{n}}(\alpha\mathcal{O}_K) = 1 \in \mathrm{Gal(L/K)}$. By definition, $\alpha \equiv 1(\mathfrak{n}_0)$ and $\sigma(\alpha) > 0$ for every real infinite prime σ dividing $\mathfrak{n}_\infty$. But $\mathfrak{m}|\mathfrak{n}$, so $\alpha \equiv 1(\mathfrak{m}_0)$ and $\sigma(\alpha) > 0$ for every real infinite prime σ dividing $\mathfrak{m}_\infty$. Thus, $\alpha\mathcal{O}_K \in P_{K,1}(\mathfrak{m})$ and we have

$$\Phi_{\mathfrak{m}}(\alpha\mathcal{O}_K) = 1 \in \mathrm{Gal(L/K)}.$$

But $\Phi_{\mathfrak{n}}(\alpha\mathcal{O}_K) = \Phi_{\mathfrak{m}}(\alpha\mathcal{O}_K)$ since they are both mapped to $\left(\frac{L/K}{\alpha\mathcal{O}_L}\right)$. Thus,

$$\Phi_{\mathfrak{n}}(\alpha\mathcal{O}_K) = 1 \in \mathrm{Gal(L/K)}.$$

□

Having proved this lemma, we first assume L $\subset$ M. Let r: Gal(M/K) $\longrightarrow$ Gal(L/K) be the restriction map. By Artin Reciprocity Theorem and the lemma above, there exists a modulus $\mathfrak{m}$ such that $\ker(\Phi_{L/K,\mathfrak{m}})$ and $\ker(\Phi_{M/K,\mathfrak{m}})$ are congruence subgroups for $\mathfrak{m}$. Then, by uniqueness of the Artin map, $r \circ \Phi_{M/K,\mathfrak{m}} = \ker(\Phi_{L/K,\mathfrak{m}})$, thus $\ker(\Phi_{M/K,\mathfrak{m}}) \subset \ker(\Phi_{L/K,\mathfrak{m}})$ follows.

On the other hand, assume $P_{K,1}(\mathfrak{m}) \subset \ker(\Phi_{M/K,\mathfrak{m}}) \subset \ker(\Phi_{L/K,\mathfrak{m}})$. Then, under the map $\Phi_{M/K,\mathfrak{m}}\colon I_K(\mathfrak{m}) \longrightarrow \mathrm{Gal(M/K)}$, the subgroup $\ker(\Phi_{L/K,\mathfrak{m}}) \subset I_K(\mathfrak{m})$ is sent to a subgroup H $\subset$ Gal(M/K). By Galois theory, H corresponds to an intermediate field K $\subset L' \subset$ M. The first part of the proof shows that $\ker(\Phi_{L'/K,\mathfrak{m}}) = \ker(\Phi_{L/K,\mathfrak{m}})$. By uniqueness of Abelian extension in the Existence Theorem, L $= L' \subset$ M. Thus, the desired result follows. □

We can now prove Kronecker-Weber Theorem, which classifies all Abelian extensions of $\mathbb{Q}$:

Theorem 3.5.8 (*Kronecker-Weber*) Let L be an Abelian extension of $\mathbb{Q}$. Then there is a positive integer m such that L $\subset \mathbb{Q}(\zeta_m)$, where ζ_m is the *m'th* root of unity.

Proof. Before proving this, we need to show $P_{\mathbb{Q},1}(\mathfrak{m}) = \ker(\Phi_{\mathbb{Q}(\zeta_m)/\mathbb{Q},\mathfrak{m}})$. Recall as a basic fact in cyclotomic field that for the modulus $\mathfrak{m} = m_\infty$ (where ∞ is the real infinite prime of $\mathbb{Q}$), any prime not dividing $\mathfrak{m}$ is unramified in $\mathbb{Q}(\zeta_m)$. Thus the Artin map:

$$\Phi_{\mathbb{Q}}(\mathfrak{m})\colon I_{\mathbb{Q}}(\mathfrak{m}) \longrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong U(\mathbb{Z}/m\mathbb{Z})$$

is defined. $\Phi_{\mathbb{Q}}(\mathfrak{m})$ can be described as follows: given $\frac{a}{b}\mathbb{Z} \in I_{\mathbb{Q}}(\mathfrak{m})$

$$\Phi_{\mathbb{Q}}(\mathfrak{m})(\tfrac{a}{b}\mathbb{Z}) = \bar{a}\bar{b}^{-1} \in U(\mathbb{Z}/m\mathbb{Z})$$

And thus it is obvious that

$$P_{\mathbb{Q},1}(\mathfrak{m}) = \ker(\Phi_{\mathbb{Q}(\zeta_m)/\mathbb{Q},\mathfrak{m}}).$$

By the Artin Reciprocity Theorem, there exists a modulus $\mathfrak{m}$ such that $P_{\mathbb{Q},1}(\mathfrak{m}) \subset \ker(\Phi_{L/\mathbb{Q},\mathfrak{m}})$, assuming $\mathfrak{m} = m_\infty$. Since we've shown above that $P_{\mathbb{Q},1}(\mathfrak{m}) = \ker(\Phi_{\mathbb{Q}(\zeta_m)/\mathbb{Q},\mathfrak{m}})$, we have

$$P_{\mathbb{Q},1}(\mathfrak{m}) = \ker(\Phi_{\mathbb{Q}(\zeta_m)/\mathbb{Q},\mathfrak{m}}) \subset \ker(\Phi_{L/\mathbb{Q},\mathfrak{m}}).$$

Thus, by Corollary 3.5.6, we easily have L $\subset \mathbb{Q}(\zeta_m)$. □

As another consequence of class field theory, we can now give a proof of the existence of Hilbert Class Field given in Theorem 3.1.3:

Theorem 3.5.9 The Hilbert class field L is the maximal unramified Abelian extension of K.

Proof. Given L unramified, let M be another unramified extension of K. Then, part (i) of the conductor theorem implies that $\mathfrak{f}$(M/K) = 1. And part (ii) of the theorem implies that $\ker(\Phi_{M/K,1})$ is a congruence subgroup for modulus 1. Thus

$$P_K \subset \ker(\Phi_{M/K,1})$$

By definition of Hilbert class field, this implies

$$P_K = \ker(\Phi_{L/K,1}) \subset \ker(\Phi_{M/K,1})$$

which, by Corollary 3.5.6, implies that M $\subset$ L. □

3.6 $p = x^2 + ny^2$ for infinitely many n's (2)

Recall from section 3.1 and 3.2 that we provided a partial solution to the question of which primes can be represented by the form $x^2 + ny^2$ in the case that n is positive, square-free and satisfies $n \not\equiv 3(4)$. In this section, we provide theoretical preparations for the solutions of the rest of positive n's which do not meet these criteria. In the next section, we give an application of the theory to describe the set of all primes of the form $x^2 + 27y^2$. The main object that we study in this section is a generalization of Hilbert class field called the ring class field of an order $\mathcal{O}$. First, we need some notations:

Recall from the previous section that if K is a number field, then an ideal $\mathfrak{m}$ of $\mathcal{O}_K$ can be treated as a modulus. We've defined $I_K(\mathfrak{m})$ and $P_{K,1}(\mathfrak{m})$ (see Definition 3.5.1). In this section, $\mathfrak{m}$ will usually be a principal ideal $\alpha\mathcal{O}_K$, and the above groups can be written simply as $I_K(\alpha)$ and $P_{K,1}(\alpha)$.

To define a ring class field of an order $\mathcal{O}$ with conductor f in an imaginary quadratic field K, observe that first of all we have from Proposition 3.4.11 that

$$C(\mathcal{O}) \cong I_K(f)/P_{K,\mathbb{Z}}(f)$$

with $P_{K,\mathbb{Z}}(f)$ is the subgroup of $I_K(f)$ generated by the principal ideals $\alpha\mathcal{O}_K$ where $\alpha \equiv a(f\mathcal{O}_K)$ for some $a \in \mathbb{Z}$. Further, since

$$P_{K,1}(f) \subset P_{K,\mathbb{Z}}(f) \subset I_K(f),$$

$C(\mathcal{O})$ is a generalized ideal class group for modulus $f\mathcal{O}_K$. Then, by the Existence Theorem, there exists a unique Abelian extension L/K such that all ramified primes divide $f\mathcal{O}_K$ and

$$\ker(\Phi_{L/K,f\mathcal{O}_K}) = P_{K,\mathbb{Z}}(f)$$

for $\Phi_{L/K,f\mathcal{O}_K}$ being the Artin map of K $\subset$ L. Thus,

$$C(\mathcal{O}) \cong I_K(f)/P_{K,\mathbb{Z}}(f) \cong \text{Gal(L/K)}$$

and consequently [L:K] = $h(\mathcal{O})$. This extension L is called a *ring class group* for the order $\mathcal{O}$. It is the generalized ideal class field for modulus $f\mathcal{O}_K$. Having the necessary definition, we give the following main theorem which answers for all n, the question of when a prime p is of the form $x^2 + ny^2$ for all n:

Theorem 3.6.1 Let $n > 0$ be an integer. Then there is a monic irreducible polynomial $f_n(x) \in \mathbb{Z}[x]$ of degree $h(-4n)$ such that if an odd prime p divides neither n nor the discriminant of $f_n(x)$, then

$$p = x^2 + ny^2 \text{ for some integers } x \text{ and } y \iff \begin{cases} (-n/p) = 1, \\ \exists a \in \mathbb{Z}, f_n(a) \equiv 0(p) \end{cases}$$

Furthermore, $f_n(x)$ may be taken to be the minimal polynomial of a real algebraic integer α for which $\mathrm{L} = \mathrm{K}(\alpha)$ is the ring class field of the order $\mathbb{Z}[\sqrt{-n}]$ in the imaginary quadratic field $\mathrm{K} = \mathbb{Q}(\sqrt{-n})$. Finally, if $f_n(x)$ is any monic integer polynomial that satisfies the above conditions and equivalence, then it is irreducible over $\mathbb{Z}$ and is the minimal polynomial of a primitive element of the ring class field L described above.

Proof. To prove this, we need the following fact on ring class fields:

Lemma 3.6.2 Let L be the ring class field of an order $\mathcal{O}$ in the imaginary quadratic field $\mathrm{K} = \mathbb{Q}(\sqrt{-n})$. Then L is Galois over $\mathbb{Q}$ and its Galois group over $\mathbb{Q}$ can be written as the semidirect product:

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

where the $\bar{1} \in \mathbb{Z}/2\mathbb{Z}$ acts on $\mathrm{Gal}(\mathrm{L}/\mathrm{K})$ by sending σ to σ^{-1}.

Proof. First of all, we want to show $\tau(\mathrm{L}) = \mathrm{L}$, where τ denotes complex conjugation. Note that $\tau(f\mathcal{O}_K) = f\mathcal{O}_K$ and $\tau(P_{K,\mathbb{Z}}(f)) = P_{K,\mathbb{Z}}(f)$, and we have (because $\ker(\Phi_{L/K,f\mathcal{O}_K}) = P_{K,\mathbb{Z}}(f)$)

$$\ker(\Phi_{\tau(L)/K,f\mathcal{O}_K}) = \tau(\ker(\Phi_{L/K,f\mathcal{O}_K})) = \tau(P_{K,\mathbb{Z}}(f)) = P_{K,\mathbb{Z}}(f).$$

And thus $\ker(\Phi_{\tau(L)/K,f\mathcal{O}_K}) = \ker(\Phi_{L/K,f\mathcal{O}_K})$. By uniqueness part in the Existence Theorem, we have $\tau(\mathrm{L}) = \mathrm{L}$.

Thus, similar to the proof of Lemma 3.2.3, we have that L is Galois over $\mathbb{Q}$. Thus we have the exact sequence

$$1 \longrightarrow \mathrm{Gal}(\mathrm{L}/\mathrm{K}) \longrightarrow \mathrm{Gal}(\mathrm{L}/\mathbb{Q}) \longrightarrow \mathrm{Gal}(\mathrm{K}/\mathbb{Q})(\cong\mathbb{Z}/2\mathbb{Z}) \longrightarrow 1.$$

Since $\tau \in \mathrm{Gal}(\mathrm{L}/\mathbb{Q})$, $\mathrm{Gal}(\mathrm{L}/\mathbb{Q})$ is a semidirect product $\mathrm{Gal}(\mathrm{L}/\mathrm{K}) \rtimes \mathbb{Z}/2\mathbb{Z}$, where the nontrivial element of $\mathbb{Z}/2\mathbb{Z}$ acts by conjugation by τ. For a prime $\mathfrak{p}$ of K, we know from Corollary 1.2.5 that

$$\tau\left(\tfrac{L/K}{\mathfrak{p}}\right)\tau = \left(\tfrac{L/K}{\tau(\mathfrak{p})}\right) = \left(\tfrac{L/K}{\bar{\mathfrak{p}}}\right)$$

Thus, under the isomorphism $I_K(f)/P_{K,\mathbb{Z}}(f) \cong \mathrm{Gal}(\mathrm{L}/\mathrm{K})$, conjugation by τ corresponds to the usual action of τ on $I_K(f)$. But for any such $\mathfrak{p}$, $\mathfrak{p}\bar{\mathfrak{p}} = \mathrm{Nm}(\mathfrak{p})\mathcal{O}_K \in P_{K,\mathbb{Z}}(f)$. Thus conjugation by τ gives $\bar{\mathfrak{p}}$ the inverse of $\mathfrak{p}$ in $I_K(f)/P_{K,\mathbb{Z}}(f)$ (and thus in $\mathrm{Gal}(\mathrm{L}/\mathrm{K})$. Thus the lemma is proved. □

Now, similar to the proof given for Theorem 3.2.1, our first step is to prove the following equivalence, the proof of which mimicks the proof for Theorem 3.2.2:

Theorem 3.6.3 Let $n > 0$ be an integer. Let L be the ring class field of the order $\mathcal{O} = \mathbb{Z}[\sqrt{-n}]$ in $\mathrm{K} = \mathbb{Q}(\sqrt{-n})$. If p is an odd prime not dividing n, then

$$p = x^2 + ny^2 \iff p \text{ splits completely in L.}$$

Proof. The discriminant of $\mathcal{O}$ is -4n. We know that -4n = $f^2 d_K$ where f is the conductor of the order. Let p be an odd prime not dividing n, then p does not divide $f^2 d_K$, and thus p is unramified in K. We need the following equivalences:

$p = x^2 + ny^2$

$\iff p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$, $\mathfrak{p} \neq \bar{\mathfrak{p}}$, and $\mathfrak{p} = \alpha\mathcal{O}_K$, $\alpha \in \mathcal{O}$

$\iff p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$, $\mathfrak{p} \neq \bar{\mathfrak{p}}$, $\mathfrak{p} \in P_{K,\mathbb{Z}}(f)$

$\iff p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$, $\mathfrak{p} \neq \bar{\mathfrak{p}}$, $((\mathrm{L}/\mathrm{K})/\mathfrak{p}) = 1$

$\iff p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$, $\mathfrak{p} \neq \bar{\mathfrak{p}}$, $\mathfrak{p}$ splits completely in L

$\iff p$ splits completely in L.

For the first equivalence, suppose $p = x^2 + ny^2 = (x + y\sqrt{-n})(x - y\sqrt{-n})$. Let $\mathfrak{p} = (x + y\sqrt{-n})\mathcal{O}_K$, note that $(x + y\sqrt{-n}) \in \mathcal{O}$. We also have that $(x + y\sqrt{-n})\mathcal{O}_K \neq (x - y\sqrt{-n})\mathcal{O}_K$ since p is unramified in K. Conversely, if $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$ and $\mathfrak{p} = (x + y\sqrt{-n})\mathcal{O}_K$, it follows that $p = x^2 + ny^2$. Note also that the second equivalence follows immediately from Proposition 3.4.11.

To prove the third and fourth equivalence, note that the third equivalence follows immediately from the isomorphism under the Artin map: $I_K(f)/P_{K,\mathbb{Z}}(f) \cong \mathrm{Gal}(\mathrm{L}/\mathrm{K})$. The fourth equivalence follows from Corollary 1.2.5. Finally, recall that L is Galois over $\mathbb{Q}$. Thus, the proof of the final equivalence is the same as the proof for Lemma 3.2.4. And we are done. □

Now we are ready to prove the main equivalence of Theorem 3.6.1. To begin, note that since L is Galois over $\mathbb{Q}$, by Theorem 3.2.5 there is a real algebraic integer α such that L = K(α).

By the same theorem, we know that since p splits completely in L, (-n/p) = 1 and $f_n(x)$ has an integer solution mod p for p dividing neither n nor the discriminant of $f_n(x)$, $f_n(x)$ being the minimal integer polynomial of α over K. Note also that the degree of $f_n(x)$ is [L:K] = $h(\mathcal{O})$ = h(-4n). And thus we've proved the main equivalence for our theorem.

The final part of the theorem says that all monic integer polynomials that satisfy the equivalence condition are the minimal irreducible polynomials for some primitive elements α such that L = K(α).

To prove this, let $f_n(x)$ be a monic integer polynomial of degree h(-4n) that satisfies the equivalence condition of Theorem 3.6.1. Let $g(x)$ be the irreducible component of $f_n(x)$ over K. Let M = K(α) be a field extension generated by the root of $g(x)$. Then, if we show L $\subset$ M, we have:

$$h(\text{-}4n) = [\text{L:K}] \leq [\text{M:K}] = \deg(g(x)) < \deg(f_n(x)) = h(\text{-}4n)$$

and thus L = M and $f_n(x)$ is the minimal polynomial for α a primitive element of L over K.

To prove L $\subset$ M, we need the following fact:

Proposition 3.6.3 Let M and L be finite extensions of K. Then L $\subset$ M *iff* $\tilde{\mathcal{S}}_{M/\mathbb{Q}} \subset \mathcal{S}_{L/\mathbb{Q}}$, where

$$\mathcal{S}_{L/\mathbb{Q}} = \{p \text{ prime: } p \text{ splits completely in L}\}$$
$$\tilde{\mathcal{S}}_{M/\mathbb{Q}} = \{p \text{ is unramifed in L and } f(\mathfrak{P}|p) = 1 \text{ for some prime } \mathfrak{P} \text{ of M}\}.$$

Proof. For proof, see Cox[1, Proposition 8.20]. □

We thus want to show $\tilde{\mathcal{S}}_{M/\mathbb{Q}} \subset \mathcal{S}_{L/\mathbb{Q}}$. Note that $\mathcal{S}_{L/\mathbb{Q}}$ is the set of all primes that satisfy the equivalence condition of Theorem 3.6.1.

Thus we suppose that $p \in \tilde{\mathcal{S}}_{M/\mathbb{Q}}$. Then, $f(\mathfrak{P}|p) = 1$ for some prime $\mathfrak{P}$ of M$\}$. Let $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$, then

$$1 = f(\mathfrak{P}|p) = f(\mathfrak{P}|\mathfrak{p})f(\mathfrak{p}|p).$$

And thus $f(\mathfrak{p}|p) = 1$ which says that p splits completely in K. Also, since $f_n(x) \equiv 0$ ($\mathfrak{P}$) has a solution in $\mathcal{O}_M$ because $\alpha \in \mathcal{O}_M$ and $f_n(\alpha) = g(\alpha) = 0$, and since $f(\mathfrak{P}|p) = 1$ implies (by definition of inertia degree) that $\mathbb{Z}/p\mathbb{Z} \cong \mathcal{O}_M/\mathfrak{P}$, we know that $f_n(x) \equiv 0$ (p) has an integer solution. Thus,

$$p \text{ splits completely in K and } f_n(x) \equiv 0 \ (p) \text{ has an integer solution.}$$

Thus, $p \in \mathcal{S}_{L/\mathbb{Q}}$ and $\tilde{\mathcal{S}}_{M/\mathbb{Q}} \subset \mathcal{S}_{L/\mathbb{Q}}$. Thus L $\subset$ M and the proof of the final part of Theorem 3.6.1 is done. □

3.7 Example: $p = x^2 + 27y^2$

Thus we have the solution for $p = x^2 + ny^2$ for all possible n's. We finish the paper by giving one example of using ring class field to solve for the above quadratic form. We begin by finding the ring class field of order $\mathbb{Z}[\sqrt{-27}]$:

Proposition 3.7.1 The ring class field of the order $\mathbb{Z}[\sqrt{-27}] \subset$ K = $\mathbb{Q}(\sqrt{-3})$ is L = K($\sqrt[3]{-2}$).

Proof. Let L be the ring class field of the order $\mathbb{Z}[\sqrt{-27}] \subset$ K = $\mathbb{Q}(\sqrt{-3})$. Then, we know the following facts from class field theory:

(i) [L:K] = |Gal(L/K)| = $h(\mathcal{O})$. By Theorem 3.4.13, one easily computes $h(\mathcal{O}) = 3$.

(ii) By Lemma 3.6.2, L is Galois over $\mathbb{Q}$, and Gal(L/$\mathbb{Q}$) is isomorphic to the symmetric group S_3 because Gal(L/K) $\cong \mathbb{Z}/3\mathbb{Z}$ by (i).

(iii) All primes of K that ramify in L divides $6\mathcal{O}_K$ because the conductor of $\mathbb{Z}[\sqrt{-27}]$ is 6 ($\mathcal{O}_K$ = $\mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$).

To proceed, note that K contains a primitive cube root of unity $\zeta_3 = \frac{-1+\sqrt{-3}}{2}$. Thus, by Kummer theory, any cubic Galois extension of K is of the form K($\sqrt[3]{u}$) for some $u \in$ K. More precisely, we want to show the following statement:

Proposition 3.7.2 If M is a cubic extension of K = $\mathbb{Q}(\sqrt{-3})$ with Gal(M/$\mathbb{Q}$) $\cong S_3$, then M = K($\sqrt[3]{m}$) for some cubefree positive integer m.

Proof. We know that M is Galois over $\mathbb{Q}$ and that the complex conjugation $\tau \in \mathrm{Gal}(M/\mathbb{Q})$. Also, if σ is a generator of $\mathrm{Gal}(L/K) \cong \mathbb{Z}/3\mathbb{Z}$, $\mathrm{Gal}(L/\mathbb{Q}) \cong S_3$ which implies that $\tau\sigma\tau = \sigma^{-1}$.

By Theorem 3.2.5, there exists a real algebraic integer α such that $L = K(\alpha)$. We define $u_i \in M$ as

$$u_i = \alpha + \zeta^i\sigma^{-1}(\alpha) + \zeta^{2i}\sigma^{-2}(\alpha),\ i = 0,1,2.$$

where ζ is the primitive cube root of unity. Then, u_i are algebraic integers satisfying $\sigma(u_i) = \zeta^i u_i$. Because $\tau\sigma\tau = \sigma^{-1}$, we have $\tau(u_i) = u_i$ and thus all u_i are real. Note that u_0 is fixed by both τ and σ, and thus $u_0 \in \mathbb{Z}$. Similarly, u_1^3 and $u_2^3 \in \mathbb{Z}$.

If $u_1 \neq 0$, we claim that $M = K(u_1)$. To show this, note that [M:K] = 3 and thus $M \neq K(u_1)$ when $u_1 \in K$. Since $u_1 \in \mathbb{R}$, u_1 is fixed by both σ and τ and is thus an integer. This contradicts the fact that $\sigma(u_1) = \zeta u_1$. Thus if $m = u_1^3 \in \mathbb{Z}$, $M = K(u_1) = K(\sqrt[3]{m})$.

Similarly, we can show that if $u_2 \neq 0$, then $M = K(u_2)$. The remaining case is to show when $u_1 = u_2 = 0$. A simple application of Cramer's rule shows that

$$\alpha = \frac{u_1+u_2+u_3}{3}$$

which shows that $\alpha \in K$ and is thus rational (since we've assumed $\alpha \in \mathbb{R}$). This completes the proof of Proposition 3.7.2. □

The next step is to use ramification of $K \subset L = K(\sqrt[3]{m})$ to restrict m. It is easy to show that any prime of K dividing m ramifies in L. By (iii) above, all primes of K ramified in L divide $6\mathcal{O}_K$, and thus 2 and 3 are the only integer primes dividing m. Thus m can only be one of the following integers:

$$2,\ 3,\ 4,\ 6,\ 9,\ 12,\ 18,\ 36.$$

And one can easily show that the only four fields satisfying conditions (i) through (iii) are

$$K(\sqrt[3]{2}),\ K(\sqrt[3]{3}),\ K(\sqrt[3]{6}),\ K(\sqrt[3]{12}).$$

To further limit the candidates for the correct field, we need to use Theorem 3.6.1. By the theorem, the correct field gives a minimal polynomial $f_{27}(x)$ which has an integer solution modulo p. Since each of the four fields above gives a minimal polynomial, we can use this condition to check whether the polynomial has such a solution.

For the field $K(\sqrt[3]{3})$, for instance, the minimal polynomial of $\sqrt[3]{3}$ over K is $f_{27}(x) = x^3$ - 3. Choose $p = 31$ since $31 = 2^2 + 27 \times 1^2$. Using a computer, one can show that $x^3 \equiv 3$ (31) has no integer solution. Thus, $K(\sqrt[3]{3})$ is not our desired field.

Similarly, one can show that $K(\sqrt[3]{6})$ and $K(\sqrt[3]{12})$ do not satisfy Theorem 3.6.1. And thus $L = K(\sqrt[3]{2})$. □

Once we know the ring class field of order $\mathbb{Z}[\sqrt{-27}]$, we use Theorem 3.6.1 to get the final solution for $p = x^2 + 27y^2$:

Theorem 3.7.3 If $p > 3$ is a prime, then

$$p = x^2 + 27y^2 \iff \begin{cases} p \equiv 1(3), \\ \exists a \in \mathbb{Z}, x^3 \equiv 2(p). \end{cases}$$

Proof. By Proposition 3.7.1, the ring class field of the order $\mathbb{Z}[\sqrt{-27}]$ is $K(\sqrt[3]{2})$, $K = \mathbb{Q}(\sqrt{-3})$. Since $\sqrt[3]{2}$ is a real algebraic integer, whose minimal polynomial is $f_{27}(x) = x^3$ - 2 as shown in the proof above, by Theorem 3.6.1 we know that

$$x^3 \equiv 2 \text{ (p) and } (-27/p) = 1.$$

The latter is equivalent to the condition

$$p \equiv 1 \text{ (3)}.$$

Since the discriminant of $f_{27}(x)$ is $-2^2 \cdot 3^3$, the only primes that ramify in the extension are 2 and 3. And thus we have the condition that p is a prime greater than 3. □

Acknowledgements. I want to thank my mentor, Shiva Chidambaram, for his guidance and support throughout the program. I would also like to thank Doctor Antoni Rangachev, who encourages me to choose my paper topic in algebraic number theory. Finally, I want to thank Professor Peter May for organizing the REU program.

References

[1] Cox, David. *Primes of the Form $x^2 + ny^2$*. John Wiley & Sons, Inc. 1989.
[2] G. Janusz, *Algebraic Number Fields*. Academic Press, New York, 1973.
[3] Ireland and Rosen. *A Classical Introduction to Modern Number Theory*. Springer-Verlag, New York Inc. 1982.
[4] Lang, Serge. *Algebraic Number Theory*. Springer-Verlag, New York Inc. 1994.
[5] Marcus, Daniel. *Number Fields*. Springer-Verlag, New York Inc. 1977.
[6] Milne, James. *Algebraic Number Theory*. http://www.jmilne.org/math/CourseNotes/ANT.pdf