From Hilbert Class Field Theory to Complex Multiplication

Shaunak Bhandarkar

Euler Circle, Palo Alto CA 94303, USA shaunak@gmail.com

Abstract. In this paper, we will explore Hilbert Class Field theory through the lens of Algebraic Number Theory. Using key concepts relating to ideals, Galois Theory, and number fields, we will work our way up to Complex Multiplication.

We will start by briefly reviewing ideals and number rings, exploring the basic properties that we will build upon later in the text. We define important terms, such as Dedekind Domains and introduce fundamental theorems such as unique factorization of ideals. Then, we build upon this by diving into number fields.

After this, we will make a connection between Galois Theory and number fields, exploring how ideals are affected by automorphisms in the Galois group. Basic knowledge of ideals and Galois Theory as well as certain results pertaining to them will arm us with the knowledge necessary to dive deeper into Algebraic Number Theory.

Next, we will move on to concepts in Algebraic Number Theory, and work with ideals in Dedekind domains. After introducing important definitions, such as the norm, we will explore ideals in number fields, touching upon Galois Theory along the way. This will aid us in covering ramification as well as the decomposition and inertial groups. These basic definitions, lemmas, and theorems will enable us to concretely describe the Hilbert Class Field.

After introducing the Hilbert Class Field, we will explore a particular application in Genus Theory. Then, we will introduce the Artin Symbol, a crucial element of class field theory and touch upon the preliminaries of Artin Reciprocity .

In the final section of the paper, we will aim to generalize what we have done so far, looking at quadratic fields from the complex multiplication perspective. This will involve proving important results in elliptic curve mathematics, such as the group-like properties of elliptic curves. We will conclude with parting remarks on the higher degree cases of complex multiplication, which remain open in mathematics.

Keywords: Class Field Theory · Algebraic Number Theory · Galois Theory

1 A Review of Number Fields and Ideals

Here, we assume the reader has basic knowledge of number fields. Thus, we begin by stating (without proof) some basic results in algebraic number theory that we will build off of. At its most basic level, number fields are extensions of $\mathbb{Q}$, but just like in $\mathbb{Q}$ itself, it is useful to have some concept of integers, much like $\mathbb{Z}$. To this end, for a number field K, we define O_K to be the ring of integers in K, that is, the ring of elements $\alpha \in K$ that are the roots of monic irreducible polynomials with coefficients in $\mathbb{Z}$. Essentially, O_K is the set of algebraic integers in K; it is easy to see that O_K is a ring. Moreover, one can see that its field of fractions is K and that it is finitely generated (in fact, it is a $\mathbb{Z}$-module).

Proposition 1.1. *Let a be a nonzero ideal in O_K. Then, $|O_K/a|$ is finite.*

In fact, this is what we call the norm of the ideal a, i.e., $N(a)$, which is finite.

Proposition 1.2. *The ring of integers O_K is a Dedekind Domain, which means that*

(i) If $a \in O_K$ is the root of a monic polynomial with coefficients in O_K, then $a \in O_K$ (i.e., O_K is integrally closed in K).

(ii) O_K is a Noetherian ring, meaning that if there is a chain of ideals in O_K such as $a_1 \subset a_2 \subset a_3 \subset ...$, then there is some positive integer n such that $a_n = a_{n+1} = a_{n+2} = ...$

(iii) Every nonzero prime ideal of O_K is maximal.

Theorem 1.3. *Let I be an ideal in some Dedekind Domain R. Then, there exists another ideal J such that the ideal IJ is principal.*

This theorem is essentially the foundation for the ideal class group, in which the identity consists of the principal ideals.

Theorem 1.4 (Unique Factorization of Ideals)**.** *For any ideal $a \in O_K$, we have $a = p_1 p_2 p_3 ... p_r$, where the p_i are prime ideals, not necessarily all distinct. This factorization into prime ideals is unique up to order.*

This theorem reveals the importance of Dedekind Domains; even if we do not have unique factorization of elements, we do have unique factorization of ideals. This will prove to be invaluable when we study prime decomposition in depth.

Now, we introduce the notion of ramification. Suppose K is a number field, L is an extension of K, and p is an ideal of O_K. Then pO_L is an ideal of O_L and we may write it as $pO_L = B_1^{e_1} B_2^{e_2} ... B_g^{e_g}$. Essentially, prime ideals can factor further in field extensions.

Definition 1.5. For each prime ideal B_i above, e_i is defined as the ramification index of that ideal. If even one of the e_i's is larger than 1, p is said to *ramify* in O_L. If all of the e_i's are equal to 1, p is said to *split* in O_L.

Definition 1.6. An interesting consequence of the previous definition is that for every ideal B_i lying over p, we have a residue field extension $O_K/p \subset O_L/B_i$. The degree of this field extension is denoted by f_i, and is known as the inertial degree of B_i over p.

These definitions are quite important. We will actually revisit the residue field extension described above when we discuss the decomposition and inertia groups.

Theorem 1.7. *Let $n = [L : K]$. We have the following interesting results:*

(i) For ideals I and J of O_K, we have $|O_K/I||O_K/J| = |O_K/IJ|$. This follows quickly from a variation of the Chinese Remainder Theorem.

(ii) For an ideal $IO_L \in O_L$, where $I \in O_K$, we have $|O_L/IO_L| = |O_K/I|^n$.

(iii) For an ideal $a \in O_K$, we have $|O_K/a| = N_{\mathbb{Q}}^K(a)$, where N denotes norm.

Now, we visit a beautiful theorem that will serve as an invaluable tool later.

Theorem 1.8. *From our factorization of p in O_L above, we have $\sum_{i=1}^{g} e_i f_i = [L : K]$.*

Proof. Let $n = [L : K]$. Then, we have $|O_L/pO_L| = |O_K/pO_K|^n$. Doing it another way, we have $|O_L/pO_L| = \prod |O_L/B_i|^{e_i} = \prod |O_K/pO_K|^{f_i e_i}$, using the definition of f_i. From this, it quickly follows that $n = \sum_{i=1}^{g} e_i f_i$.

Now, we are equipped with some of the basic tools to dive into Galois Theory.

2 A Hint of Galois Theory

In this section, we aim to explore some of the underlying theory behind prime decomposition. Naturally, this will touch upon Galois Theory. If we let L be a Galois extension of K, and let O_L and O_K, respectively, be their corresponding rings of integers, then it is easy to see that for any prime ideal P of O_K, $Gal(L/K)$ permutes the primes lying above P in O_L. However, we can say something even stronger.

Theorem 2.1. *$Gal(L/K)$ permutes the prime ideals lying above P transitively. That is, for any two prime ideals Q and Q' in O_L, there is a $\sigma \in Gal(L/K)$ such that $\sigma(Q) = Q'$.*

Proof. Aiming for a contradiction, suppose there is a prime ideal Q' for which none of the automorphisms in $Gal(L/K)$ map Q to Q'. Then, by the Chinese Remainder Theorem, we know there exists a solution, x, to the conqruences $x \equiv 0 \pmod{Q'})$ and $x \equiv 1 \pmod{\sigma(Q)})$ for any $\sigma \in Gal(L/K)$. Thus, if $\alpha \in O_L$ is such a solution, then $N_K^L(\alpha) \in K \cap Q' = P$. On the other hand, since for each $\sigma \in Gal(L/K)$, $\alpha \notin \sigma(Q)$, we also have that $\sigma^{-1}(\alpha) \notin Q$. But we know that the group formed by the inverses of the elements in the Galois group is just the Galois group, so $N_K^L(\alpha) = \prod_{\sigma \in Gal(L/K)} \sigma(\alpha) = \prod_{\sigma^{-1} \in Gal(L/K)} \sigma^{-1}(\alpha) \notin Q \in P$, so $N_K^L(\alpha) \notin P$. This is a contradiction, so the Galois group must be transitive!

Corollary 2.2. *Let $e(A|B)$ denote the ramification index of prime ideal A over B. Similarly, let $f(A|B)$ denote the inertial degree. If L is a Galois extension of K, and Q and Q' are two prime ideals in O_L lying above prime ideal P in O_K, then $e(Q|P) = e(Q'|P)$ and $f(Q|P) = f(Q'|P)$.*

Proof. Notice that $e(Q|P) = e(Q'|P)$ holds (given a Galois extension) from unique factorization and transitivity of the Galois group with respect to the prime ideals lying over P. Next, $f(Q|P) = f(Q'|P)$ follows from O_L/Q being isomorphic to O_L/Q'; this is because there is an element $\sigma \in Gal(L/K)$ that maps Q to Q' (showing surjectivity), and $ord(O_L/Q) = N_K^L(Q) = N_K^L(Q') = ord(O_L/Q')$ because Q and Q' are Galois conjugates. Thus, the homomorphism from O_L/Q to O_L/Q' is bijective, so we have an isomorphism. In particular, this means that the degree of the residue field extension O_L/Q over O_K/P is the same as that of O_L/Q' over O_K/P, i.e., their inertial degrees are the same.

Now, we come to a particularly deep theorem, in that it greatly allows us to describe primes that ramify in number fields.

Theorem 2.3. *An integer prime p divides the discriminant d of a number ring R if and only if p ramifies in R. In particular, there are only finitely many primes ramifying in R.*

3 Galois Theory Applied to Prime Decomposition

Recall that if the extension L/K is Galois, then the ramification indices of all the primes Q lying over a fixed prime P (of O_K) are equal; thus, we have that $PO_L = (Q_1Q_2...Q_r)^e$. Also, since e and f are the same for each Q_i, we have that $ref = n$.

Now, when we have a group acting on a set (in our case, $Gal(L/K)$), it is interesting to consider subgroups that stabilize particular elements. To this end, suppose we have a prime Q_i lying over P; now define the *decomposition group* to be

$$D(Q_i/P) = \{\sigma \in Gal(L/K) \mid \sigma(Q_i) = Q_i\} \subseteq Gal(L/K)$$

.

In fact, we can say something quite interesting right off the bat: if there is an automorphism $\sigma \in Gal(L/K)$ such that $\sigma(Q) = Q'$, then it is easy to see that $D(Q'/P) = \sigma D(Q/P)\sigma^{-1}$ (one can show this by proving injectivity followed by showing that both decomposition groups have equal orders). This fact actually means that the decomposition groups of the primes lying over P form a conjugacy class of $Gal(L/K)$!

However, to show both decomposition groups above have the same order, we have to calculate their orders first! We know that the orbit of the element Q_i is basically each Q_j for $1 \leq j \leq r$. By the so-called orbit-stabilizer theorem, the order of the stabilizer, that is, the decomposition group, is just the order of the Galois group - $n = ref$ - divided by the order, r; thus $|D(Q/P)| = ef$, which is true of any prime ideal Q lying over P.

Now, the most interesting thing about the decomposition group is its relation to the Galois group of residue fields. Since any $\sigma \in D(Q/P)$, $\sigma(Q) = Q$ induces an automorphism of the residue field O_L/P; for any $a + bQ \in O_L/Q$, the automorphism maps it to $\sigma(a + bQ) = \sigma(a) + \sigma(b)\sigma(Q) = a' + b'Q \in O_L/Q$. Moreover, since $\sigma \in Gal(L/K)$, σ fixes K; in particular, it fixes O_K and thus O_K/P as well. Thus, there is a natural homomorphism

$$D(Q/P) \longrightarrow Gal(O_L/Q : O_K/P)$$

. In fact, this homomorphism is surjective.

Because of this homomorphism, it is natural to wonder if we can create an isomorphism. Luckily, we can apply the first isomorphism theorem: if we let $I(Q/P)$ be the kernel of the homomorphism, then

$$D(Q/P)/I(Q/P) \cong Gal(O_L/Q : O_K/P)$$

. Since $I(Q/P)$ is the kernel, we can give it a more explicit definition:

$$I(Q/P) = \{\sigma \in D(Q/P) \mid \sigma(a) \cong a \pmod{Q} \text{ for all } a \in O_L\}$$

. This subgroup of the decomposition group is known as the *inertia group*.

To find the order of the inertia group, recall that $|D(Q/P)| = ef$ and $Gal(O_L/Q : O_K/P) = [O_L/Q : O_K/P] = f$, so $|I(Q/P)| = ef/f = e$. Just like with the decomposition group, the inertia groups of the ideals of the primes lying over P form a conjugacy class. The intriguing thing is that if $Gal(L/K)$ is abelian, each of these conjugacy classes only contain one element! Thus, the decomposition and inertia groups do not depend on the prime ideal lying above P in this case. Now, we can go even further to define L^I to be the *inertia field*, i.e., the fixed field of the inertia group acting on L/K. Similarly define L^D to be the *decomposition field*. Then, $[L : L^I] = |I(Q/P)| = e$ and $[L : L^D] = |D(Q/P)| = ef$ by definition. From this, we can also deduce that $[L^D : K] = \frac{ref}{ef} = r$. Now, we have the tower of fields $K \subset L^D \subset L^I \subset L$.

Proposition 3.1. *We make the following observations:*

(i) Every prime P of K splits into r primes in L^D, each with $e = 1$. Essentially, this is the "stage" where all the splitting occurs.

(ii) In the extension L^I/L^D, each of these r primes remains inert. In this "stage," nothing really goes on.

(ii) In the extension L/L^I, each of these primes finally ramifies (i.e., can be factored into a prime raised to the e^{th} power, where e is the ramification index of that prime.

Proof. When $Gal(L/K)$ is abelian, $D(Q/P)$ is normal, so by Galois Theory, L^D/K is Galois as well. We know that $[L : L^D] = |D(Q/P)| = ef$, but also that $[L : L^D] = e(Q|Q_D)f(Q|Q_D)$, where $e(Q|Q_D) \leq e$ and $f(Q|Q_D) \leq f$. Thus, they are equal, and so $e(Q_D|K) = e/e(Q|Q_D) = 1$. Similarly, $f(Q_D|K) = 1$, proving (i).

Next, we show that $f(Q|Q_I) = 1$ by showing that $Gal(O_L/Q : O_{L^I}/Q_I)$ is trivial. Essentially, consider $g(x) = \prod_{\sigma \in I(Q/P)} (x - \sigma(a))$, for some $a \in O_L/Q$ that corresponds to $\theta \in O_L/Q$. Observe that $g(x)$ actually has coefficients in O_{L^I}, and so $\bar{g}(x)$ obtained by taking the coefficients of $g(x)$ modulo Q actually has coefficients in O_{L^I}/Q_I. But observe that $\sigma(a) \cong a \cong \theta \pmod{Q}$, so $\bar{g}(x) = (x - \theta)^m$, where $m = |I(Q/P)|$. This means that every automorphism of the Galois group of these residue fields merely sends θ to itself, indicating that it is trivial; thus, $f(Q|Q_I) = 1$. Together with $f(Q_D|P) = 1$, we see that $f(Q_I|Q_D) = f$. From here, Galois Theory shows that $[L^I : L^D] = f$, so $e(Q_I|Q_D) = 1$, proving (ii). Thus, we are left with $e(Q|Q_I) = e$, proving (iii).

Corollary 3.2. *$D(Q/P)/I(Q/P) \cong Gal(O_L/Q : O_K/P)$, and so is cyclic of order f.*

Corollary 3.3. *We have the following statements:*

(i) L^D is the largest field whose inertial and ramification degrees are both 1.

(ii) L^D is the smallest field for which $Q \in O_L$ is the only prime lying over $Q_D \in O_L^D$.

(iii) L^I is the largest field whose ramification degree is 1.

(iv) L^I is the smallest intermediate field for which $Q \in O_L$ totally ramifies over Q_I, i.e., $e(Q|Q_I) = [L : L^I]$.

At last, we come to a theorem we will encounter again when we touch upon class field theory.

Theorem 3.4. *Let L and M be two extensions of the number field K. If the prime ideal $P \in O_K$ is unramified in both L and M, then it is unramified in the composite field LM. Moreover, if P splits completely (meaning ramification and inertial degrees are both 1), then it splits completely in LM.*

Proof. Since the corresponding primes lying over P in each of L and M have ramification index 1, they are subfields of the inertial field, the maximal field whose ramification index is 1. Thus, $L \cup M = LM$ is a subfield of the inertial field as well, meaning it is unramified.

For the second part, observe that L and M are subfields of the decomposition field this time, since the decomposition field is the maximal field whose ramification index and inertial degree is 1. Thus, LM is also a subfield of the decomposition field, and so P splits completely in it.

Before venturing any further, we now define the *Frobenius automorphism* - an invaluable tool for class field theory later.

Suppose that $K \subset L$ is unramified, meaning $I(Q/P) = 1$. This means $D(Q/P) \cong Gal(O_L/Q : O_K/P)$, which is a cyclic group of order f that is generated by the automorphism that sends every $x \in O_L/Q$ to

$x^{||P||}$, where $||P||$ denotes the norm of P. The corresponding automorphism $\phi \in D(Q/P)$ has the property that

$$\phi(x) \cong x^{||P||} \pmod{Q}$$

for every $x \in O_L$. Similar to before, the collective set of Frobenius automorphisms of prime ideals lying over P forms a conjugacy class. Then, if $Gal(L/K)$ is abelian, each prime Q lying over P has the same Frobenius automorphism, so by the Chinese Remainder Theorem, we have

$$\phi(x) \cong x^{||P||} \pmod{PO_L}$$

.

4 A Nice Algorithm to Factor Ideals

This section is devoted to proving one rather interesting theorem that we will touch upon later. The title of this section probably gives it away.

We start with our field extension $K \subset L$ of degree n; by the Primitive Element Theorem, we have some $\alpha \in L$, and actually, some $\alpha \in O_L$ of degree $[L : K] = n$, such that $L = K(\alpha)$. Now, we fix some prime P of O_K and for any $h \in O_K[x]$, let $\bar{h}$ be the corresponding polynomial in $(O_K/P)[x]$ due to reduction of coefficients mod P. Now, if $g(x)$ is the monic irreducible polynomial of α over K, then since α is algebraic, the coefficients of g are also algebraic, meaning they lie in O_K (they can all be written in terms of α and its conjugates). Thus, $g(x) \in O_K[x]$, and so $\bar{g}(x) \in (O_K/P)[x]$, where we can uniquely factorize it into distinct monic irreducible polynomials as

$$\bar{g}(x) = \bar{g_1}(x)^{e_1}\bar{g_2}(x)^{e_2}\cdots\bar{g_r}(x)^{e_r}$$

. At last, we are ready to state and prove our theorem:

Theorem 4.1. *Let p be the prime lying under P in $\mathbb{Z}$ such that $p \nmid |O_L/O_K(\alpha)|$. Then, the prime decomposition of PO_L is given by*

$$Q_1^{e_1}Q_2^{e_2}\cdots Q_r^{e_r}$$

where Q_i is the ideal $(P, g_i(\alpha))$ in O_L, i.e.

$$Q_i = PS + (g_i(\alpha))$$

Also, $f(Q_i|P)$ is the degree of g_i.

Proof. Let f_i be the degree of g_i, which is also the degree of $\bar{g_i}$. We will prove the following:

(i) For each Q_i, either $Q_i = O_L$ or O_L/Q_i is a field of order $|O_K/P|^{f_i}$.

(ii) $Q_i + Q_j = O_L$ whenever $i \neq j$.

(iii) $PO_L \mid Q_1^{e_1}Q_2^{e_2}\cdots Q_r^{e_r}$.

Assuming the result holds, we can prove our result; rearrange the ideals so that Q_1, Q_2, $\cdots$, Q_s are the proper ideals, and the rest are equal to O_L (in fact, we will prove that $r = s$). Clearly, each Q_i lies over P. By (i), we would have that $f_i = f(Q_i|P)$ as desired. (ii) shows us the Q_i are distinct and prime to one another. (iii) becomes $PS \mid Q_1^{e_1}Q_2^{e_2}\cdots Q_s^{e_s}$, so $PS = Q_1^{d_1}Q_2^{d_2}\cdots Q_s^{d_s}$, where each $d_i \leq e_i$. The ramification-inertial degree theorem tells us that $f_1d_1 + f_2d_2 + \cdots + f_sd_s = n$, but also the degree of $\bar{g}$ is easily seen to be $e_1f_1 + e_2f_2 + \cdots + e_rf_r = n$, meaning that $r = s$ and $d_i = e_i$, and we would have our result. It remains to prove these 3 statements.

Proof of (i): Let $F_i = ((O_K/P)[x])/\bar{g_i}$. Observe that this is a residue field with coefficients taken modulo P. Now, consider the homomorphism

$$O_K[x] \longrightarrow F_i$$

It is defined the obvious way - by reducing coefficients mod P and then reducing mod the ideal $(\bar{g_i})$. This map is surjective and it is not hard to see that the kernel of this map is the ideal (P, g_i). Thus, we have an isomorphism

$$O_K[x]/(P, g_i) \longrightarrow F_i$$

This actually means that (P, g_i) is a maximal ideal. Now, we can also map

$$O_K[x] \longrightarrow O_L$$

by the simple substitution $x \to \alpha$; this is a ring homomorphism. Clearly, (P, g_i) is contained in the kernel, and since it is maximal, the kernel must either be (P, g_i) or all of $O_K[x]$. If it is the latter, $Q_i = S$. In the case of the former, we show this map is surjective by proving $O_L = O_K[\alpha] + Q_i$; in fact, we can prove the even stronger statement $O_L = O_K[\alpha] + pO_L$. This follows because the index of $O_L = O_K[\alpha] + pO_L$ must be a common divisor of $|O_L/O_K(\alpha)|$ and $|O_L/pO_L|$. But their common divisor is just 1 since the latter is a power of p and the former is not divisible by p (refer to theorem statement above), so the index is 1. Thus, our map is onto, meaning $O_L/Q_i \cong O_K[x]/(P, g_i) \cong F_i$, which has order $|O_K/P|^{f_i}$.

Proof of (ii): Since the $\bar{g}_i$ are distinct in the domain $(O_K/P)[x]$, there exist h and k over $O_K[x]$ such that $\bar{g}_i\bar{h} + \bar{g}_j\bar{k} = 1$, so

$$g_ih + g_jk \cong 1 \pmod{P[x]}$$

, meaning that if we replace x with α, we obtain

$$g_i(\alpha)h(\alpha) + g_j(\alpha)k(\alpha) \cong 1 \pmod{PO_L}$$

. It follows that $1 \in (P, g_i, g_j) = Q_i + Q_j$, so the sum of these ideals must be S.

Proof of (iii): To make life easy, let $\gamma_i = g_i(\alpha)$. With $Q_i = (P, \gamma_i)$, it is evident that $Q_1^{e_1}Q_2^{e_2}\cdots Q_r^{e_r}$ is contained in, and thus divisible by, $(P, \gamma_1^{e_1}\gamma_2^{e_2}\cdots\gamma_r^{e_r})$. We claim that this ideal is just PO_L. To prove this, we will show that $\gamma_1^{e_1}\gamma_2^{e_2}\cdots\gamma_r^{e_r}$ is in PO_L. Clearly, since

$$\bar{g}(x) = \bar{g_1}(x)^{e_1}\bar{g_2}(x)^{e_2}\cdots\bar{g_r}(x)^{e_r}$$

we have

$$g(x) \cong g_1(x)^{e_1}g_2(x)^{e_2}\cdots g_r(x)^{e_r} \pmod{P[x]}$$

, so the simple substitution $x \to \alpha$ just like in (ii) gives us

$$g_1(\alpha)^{e_1}g_2(\alpha)^{e_2}\cdots g_r(\alpha)^{e_r} \cong \gamma_1^{e_1}\gamma_2^{e_2}\cdots\gamma_r^{e_r} \cong g(\alpha) \cong 0 \pmod{PO_L}$$

, as desired. This proves (iii), and we are done.

Why did we bother to prove this theorem? So that we would have the following corollary under our belt:

Corollary 4.2. *Let $K \subset L$ be a Galois extension, and let α be in O_L such that $L = K(\alpha)$. Let $f(x)$ be the monic minimal irreducible polynomial for α over K so that $f(x) \in O_K[x]$. If P is prime in O_K and f is separable modulo P, then we have the following results:*

(i) If $f(x) = f_1(x)f_2(x)\cdots f_r(x) \pmod{P}$, where each f_i is distinct and irreducible mod P, then $Q_i = (P, f_i(x))$ is a prime ideal of of O_L, $Q_i \neq Q_j$ for $i \neq j$, and

$$PO_L = Q_1Q_2\cdots Q_r$$

Furthermore, each of the f_i has degree f, where f is the inertial degree of the extension (unique because the extension is Galois).

(ii) P is unramified in L.

(iii) P splits completely in L if and only if $f(x) \cong 0 \pmod{P}$ has a solution $x \in O_K$.

Proof. Observe that (i) follows immediately from the theorem above; it is merely a special case. (ii) is an immediate consequence of (i) because each prime lying over P has ramification index 1. Finally, (iii) also follows quickly because it implies each f_i is monic, meaning $f = 1$, so this, along with $e = 1$, tells us that P splits completely in L.

5 Introduction to Quadratic Fields

Let us now apply some of our theory to quadratic number fields - fields of the form $K = \mathbb{Q}(\sqrt{N})$, where $N \neq 0, 1$ is a squarefree integer. Its discriminant, d_K, is defined to be N if $N \cong 1 \pmod 4$ and $4N$ otherwise. Using the discriminant, one can show that the ring of integers in K, O_K is $\mathbb{Z}[\frac{d_K + \sqrt{d_K}}{2}]$. Now, we describe the behavior of prime ideals in O_K.

Proposition 5.1. *Let K be a quadratic number field of discriminant d_K, and let $\alpha \to \alpha^{'}$ be the nontrivial automorphism of its Galois group (over $\mathbb{Q}$). Let p be a prime in $\mathbb{Z}$. Also, let (a/p) denote the Legendre symbol, where p is prime.*
(i) If $(d_K/p) = 0$, then $pO_K = P^2$, for a prime ideal $P \in O_K$.
(ii) If $(d_K/p) = 1$, then $pO_K = PP'$, where $P \neq P'$ are primes in O_K.
(iii) If $(d_K/p) = -1$, then p remains prime in O_K.

Proof. For (i), let $P = (p, \sqrt{d_K})$. Squaring this ideal shows that it is indeed equal to p. Moreover, it is seen to be prime by applying the theorem $ref = n = [K : \mathbb{Q}] = 2$.

For part (ii), if $(d_K/p) = 1$, then $x^2 \cong d_K \pmod p$ has a solution, meaning $f(x) = x^2 - d_K$ is separable mod p and congruent to 0 modulo P for a suitable $x \in \mathbb{Z}$. Thus, by part (iii) of the corollary from Section 5, p splits completely in K, i.e., $p = PP'$. For part (iii), if $(d_K/p) = -1$, then $f(x) = x^2 - d_K$ is irreducible mod p, so part (ii) of the corollary from Section 5 tells us that p remains prime in K.

Corollary 5.2. *Let K be a quadratic field with discriminant d_K and p be a prime in $\mathbb{Z}$.*
(i) p ramifies in K if and only if $p \mid d_K$.
(ii) p splits completely in K if and only if $(d_K/p) = 1$.

6 Introduction to Hilbert Class Field Theory

We begin with some basic definitions.

Definition 6.1. We call an extension $K \subset L$ *abelian* if it is Galois and $Gal(L/K)$ is abelian.

Next, note that prime ideals of O_K are *finite primes.* To make Hilbert class field theory work out, we also define infinite primes.

Definition 6.2. A *real infinite prime* is an embedding $\sigma : K \to \mathbb{R}$, while a *complex infinite prime* is a pair of complex conjugate embeddings $\sigma, \bar{\sigma} : K \to \mathbb{C}$. An infinite prime $\sigma \in K$ is said to *ramify* in L if it is real but has an extension to L that is complex. Thus, an extension $K \subset L$ is *unramified* if all finite and infinite primes do not ramify.

Now, we are ready to state a theorem that indicates the existence of the Hilbert class field. For now, we will not prove it, so feel free to take it as a definition.

Theorem 6.3. *Given a number field K, there is a finite Galois extension L such that L is an unramified abelian extension of K and any unramified extension of K lies in L.*

The field L above is called the *Hilbert class field* of K and is clearly unique. To unlock the full power of this field, we relate it to the Artin symbol (discussed later). As a first step, we revisit the Frobenius automorphism.

Lemma 1. *Let P be a prime of O_K unramified in L. If Q is a prime of O_L containing P, then there is a unique element $\sigma \in Gal(L/K)$ such that for any $a \in O_L$,*

$$\sigma(a) \cong a^{N(P)} \pmod Q$$

where $N(P) = |O_K/P|$ is the norm of P.

Proof. This lemma essentially asks us to prove the existence of the Frobenius automorphism. To do this, we make use of $D(Q|P)$ and $I(Q|P)$, the decomposition and inertia groups. Recall that any $\sigma \in D(Q|P)$ induces an automorphism $\bar{\sigma}$ of $Gal(O_L/Q : O_K/P)$. Since P is unramified in L, the inertia group is trivial, meaning that $D(Q|P) \cong Gal(O_L/Q : O_K/P)$. The structure of the latter Galois group is quite clear: since it is finite and O_K/P consists of $N(P) = q$ elements, it is actually cyclic with the canonical generator $x \mapsto x^q$; thus, there is a unique element of $D(Q|P)$ that maps to the Frobenius automorphism, meaning it contains an element σ such that

$$\sigma(a) \cong a^{N(P)} \pmod{Q}$$

for all $a \in O_L$. It is clearly unique by the nature of this isomorphism.

Now, we visit a powerful tool - one that we will constantly rely upon going forwards.

Definition 6.4. The unique element σ of the previous lemma is known as the *Artin symbol*, named after famous mathematician Emil Artin. It is denoted by $(\frac{L/K}{Q})$ and satisfies the crucial property

$$(\frac{L/K}{Q})(a) \cong a^{N(P)} \pmod{Q}$$

, where $P = Q \cap O_K$.

The Artin symbol has the following useful properties:

(i) If $\phi \in Gal(L/K)$, then $(\frac{L/K}{\phi(Q)}) = \phi(\frac{L/K}{Q})\phi^{-1}$. (This is similar to conjugacy class formed by decomposition groups.)

(ii) The order of $(\frac{L/K}{Q})$ is just $f = f(Q|P)$, the inertial degree. This follows from the Artin symbol being the generator of a cyclic group of order f.

(iii) P splits completely in L if and only if $(\frac{L/K}{Q}) = 1$. Both conditions are equivalent to $e = f = 1$, and so are equivalent themselves.

In fact, (i) tells us that if L is an abelian extension of K, then the conjugacy class of the Artin symbols is trivial, meaning it does not depend on the prime Q_i lying over P. Thus, we may denote it by $(\frac{L/K}{P})$ in this case.

We can go even further! The Artin symbol actually generalizes the n^{th} degree Legendre symbol.

Theorem 6.5. *Let K be a number field containing a primitive n^{th} root of unity, and let $a \in O_K$ and P be a prime ideal of O_K for which $na \notin P$. Now, let $L = K(\sqrt[n]{a})$; this is an abelian extension of K. Then, we have*

$$(\frac{L/K}{P})(\sqrt[n]{a}) = (\frac{a}{P})_n \sqrt[n]{a}$$

Proof. First, we observe that $f(x) = x^n - a$ is separable modulo P. In fact, f is separable if and only if P does not divide the discriminant of f. The discriminant of f, when computed, is seen to be a power of n, so only primes dividing n divide the discriminant. Luckily, for us, P cannot divide the discriminant due to the condition $na \notin P$. Thus, f is separable mod P. By the corollary in Section 5, we learn that P is unramified in L. Then, we can take some prime Q lying over P and invoke the Artin symbol:

$$(\frac{L/K}{P})(\sqrt[n]{a}) = (\sqrt[n]{a})^{N(P)} \pmod{Q} \text{ and}$$

$$a^{\frac{N(P)-1}{n}} \cong (\frac{a}{P}) \pmod{P}\text{, meaning}$$

$$(\frac{L/K}{P})(\sqrt[n]{a}) \cong (a^{\frac{N(P)-1}{n}})^n \sqrt[n]{a} \cong (\frac{a}{P})_n \sqrt[n]{a} \pmod{Q}$$

as desired.

Now, when $K \subset L$ is an unramified abelian extension, things are even nicer: every finite prime of O_K is unramified in O_L, so it has an Artin symbol! To exploit this, let I_K be the set of fractional ideals of O_K. Then, for any $a \in I_K$, a can be uniquely factored into a product of prime ideals:

$$a = \prod_1^r P_i^{r_i}$$

and we may define the generalized Artin symbol to be

$$(\frac{L/K}{a}) = \prod_1^r (\frac{L/K}{P_i})^{r_i}$$

The Artin symbol thus defines a homomorphism

$$(\frac{L/K}{a}) : I_K \longrightarrow Gal(L/K)$$

This homomorphism is known as the *Artin map*. We will revisit this ever-so-important result in depth when we explore Artin Reciprocity.

7 Genus Theory for Field Discriminants

This is a bit of a side topic, but it is crucial because it touches upon the power of the Hilbert class field. Moreover, it produces the same results as Genus Theory (relating to binary quadratic forms and their genera) using deeper underlying mechanisms.

We will start with a few deep theorems (of class field theory) that we will explore (and prove parts of) in depth later.

Definition 7.1. Recall that the *ideal class group*, $C(O_K)$, is the group consisting of classes of ideals of I_K. In particular, the set of principal ideals is the identity, and the inverse law holds because for any ideal $I \in O_K$, there is a $J \in O_K$ such that IJ is principal. In fact, we can go even further and define $C(O_K)$ as the quotient group I_K/P_K, where P_K denotes the set of principal ideals in I_K.

Theorem 7.2. *If L is the Hilbert class field of K, then the Artin map is surjective and its kernel consists of the set of principal ideals of I_K, P_K. In particular, since $I_K/P_K \cong C(O_K)$, we have the isomorphism*

$$C(O_K) \cong Gal(L/K)$$

This theorem, at the very least, gives us an idea of where the term "class field" comes from! We also have the following important corollary:

Corollary 7.3. *Given a number field K, there is a one-to-one correspondence between the unramified abelian extensions M of K and the subgroups H of $C(O_K)$. Furthermore, if the extension $K \subset M$ corresponds to $H \subset C(O_K)$, then we have the isomorphism*

$$C(O_K)/H \cong Gal(M/K)$$

This corollary is very reminiscent of the Fundamental Theorem of Galois Theory; it is deduced based on that same logic.

Corollary 7.4. *If L is the Hilbert class field of K and P is a prime ideal in K, then P splits completely in L if and only if P is a principal ideal.*

Proof. Observe that P splits completely in L if and only if $(\frac{L/K}{P}) = 1$. Since the Artin map induces the isomorphism $C(O_K) \cong Gal(L/K)$, the trivial element of $Gal(L/K)$, $(\frac{L/K}{P})$, corresponds to the trivial element of $C(O_K)$, P_K. This directly implies that P is principal.

We now get to an important theorem of the quadratic field case.

Theorem 7.5. *Let K be an imaginary quadratic field. Then, we have the following two results:*

(i) If $f(x,y) = ax^2 + bxy + cy^2$ is a primitive positive definite quadratic form of discriminant d_K, then $(a, \frac{-b+\sqrt{d_K}}{2})$ is an ideal of O_K.

(ii) The map sending $f(x,y)$ to $(a, \frac{-b+\sqrt{d_K}}{2})$ induces an isomorphism between $C(O_K)$ and $C(d_K)$, the form class group. Thus, the order of $C(O_K)$ is just $h(d_K)$, the class number.

Now, we get to the main theorem of genus theory, which we shall prove using the Hilbert class field.

Definition 7.6. The principal genus of $C(d_K)$ maps to a subgroup of $C(O_K)$. Then, under the isomorphism

$$C(O_K)/H \cong Gal(M/K)$$

this subgroup determines a unique field M known as the *genus field* of K.

Theorem 7.7. *Let K be an imaginary quadratic field of discriminant $d_K < 0$. Moreover, let μ denote the number of primes dividing d_K and let $p_1, p_2, \cdots, p_r$ be the odd primes dividing d_K so that $\mu = r$ or $\mu = r+1$. Also, define $p_i^* = (-1)^{p_i - 1} p_i$. Then:*

(i) The genus field of K is the maximal unramified extension of K which is an abelian extension of $\mathbb{Q}$.

(ii) The genus field of K is $M = K(\sqrt{p_1^*}, \sqrt{p_2^*}, \cdots, \sqrt{p_r^*})$.

(iii) The number of primitive positive definite binary quadratic forms of discriminant d_K is $2^{\mu-1}$.

(iv) The principal genus of $C(d_K)$ consists of the squares of classes.

Proof. We shall prove (i), (ii), (iii), and part of (iv). To start, let L be the Hilbert class field of K and let M be the unramified abelian extension of K corresponding to $C(O_K)^2 \subset C(O_K)$. We claim that M is the maximal unramified extension of K that is abelian over $\mathbb{Q}$.

To see why, let M' be an unramified abelian extension over $\mathbb{Q}$. Then, M' is abelian over K as well, meaning that we have the following hierarchy of fields:

$$\mathbb{Q} \subset K \subset M' \subset L$$

Additionally, note that $G = Gal(L/\mathbb{Q})$ is Galois since $\tau \in G$, where τ denotes complex conjugation (why?). This directly implies that the intersection of all fixed fields of automorphisms is none other than $\mathbb{Q}$, meaning L is Galois over $\mathbb{Q}$. Then, since M' is abelian over $\mathbb{Q}$, we have $[G,G] \subseteq Gal(L/M')$, where $[G,G]$ is the commutator subgroup of G. Also, since $[G,G] \subseteq Gal(L/K)$ since the latter has index 2 in G. Thus

$$[G,G] \subseteq Gal(L/M') \subseteq Gal(L/K)$$

From this, it follows that the maximal unramified abelian extension over $\mathbb{Q}$ is the one that corresponds to $[G,G]$! Using the Artin Map above, we know that $Gal(L/K)$ corresponds to $C(O_K)$, so it remains to show that $[G,G]$ corresponds to $C(O_K)^2$.

Next, since $\tau \in G$, we may say $G \cong Gal(L/K) \times \mathbb{Z}/2\mathbb{Z}$, where $\mathbb{Z}/2\mathbb{Z}$ acts by conjugation by τ. Then, under conjugation by τ, an ideal of $C(O_K)$ is sent to its conjugate because for $P \in O_K$, we have

$$(\frac{L/K}{\tau(P)}) = \tau(\frac{L/K}{P})\tau^{-1}$$

However, for any ideal $a \in O_K$, $a\bar{a}$ is principal meaning that $\mathbb{Z}/2\mathbb{Z}$ actually acts by sending an element of $C(O_K)$ to its inverse.

Now, $C(O_K)^2$ is a normal subgroup (any subgroup of $C(O_K)$ is), so we have

$$G/C(O_K)^2 \cong (C(O_K) \times \mathbb{Z}/2\mathbb{Z})/C(O_K)^2 \cong C(O_K)/C(O_K)^2 \times \mathbb{Z}/2\mathbb{Z}$$

Observe that $C(O_K)/C(O_K)^2$ is abelian; since $(ab)^{-1} = b^{-1}a^{-1} = ba$, it is abelian (here we exploit the fact that a and b are their own inverses). It follows that $G/C(O_K)^2$ is abelian, and so $[G,G] \subseteq G/C(O_K)^2$. To prove the reverse inclusion, note that for $a \in C(O_K)$,

$$(a,1)(1,\tau)(a,1)^{-1}(1,\tau)^{-1} = (a^2, 1)$$

where τ is just the nontrivial element of $\mathbb{Z}/2\mathbb{Z}$. Thus, $[G, G] = C(O_K)^2$, so (i) is proved.

For (ii), we note that $K \subset K(\sqrt{p_i^*})$ is unramified since this is a quadratic extension with $p_i | d_K$ and $p_i^* \cong 1 \pmod 4$ (details left to the reader!), so the composite field $M* = K(\sqrt{p_1^*}, \sqrt{p_2^*}, \cdots, \sqrt{p_r^*})$ is unramified as well, meaning $M* \subseteq M$. To show the opposite inclusion, note that $\mathbb{Q} \subset M \subset L$ correspond to $G \supset C_K^2 \supset 1$ by the Fundamental Theorem of Galois Theory. Thus

$$Gal(M/\mathbb{Q}) \cong Gal(L/\mathbb{Q})/Gal(L/M) \cong G/C(O_K)^2 \cong C(O_K)/C(O_K)^2 \times \mathbb{Z}/2\mathbb{Z}$$

and since $C(O_K)/C(O_K)^2 \cong (\mathbb{Z}/2\mathbb{Z})^x$ (order of the quotient group is a power of 2), we have that

$$Gal(M/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^m$$

for some m. This means that $M = K(\sqrt{a_1}, \sqrt{a_2}, \cdots, \sqrt{a_m})$, meaning each a_i must be a product of some of the p_i's, meaning that $M*$ actually contains M; thus, the two must be equal (proving (ii)).

In fact, writing M as $M = \mathbb{Q}(\sqrt{d_K}, \sqrt{p_1^*}, \sqrt{p_2^*}, \cdots, \sqrt{p_r^*})$, one can see that $[M : \mathbb{Q}] = 2^\mu$ (divide into cases where d_K is congruent to 1 and 0 modulo 4, respectively). From this, it follows that

$$[C(O_K) : C(O_K)^2] = \frac{1}{2}[G : C(O_K)^2] = \frac{1}{2}[M : \mathbb{Q}] = 2^{\mu-1}$$

which proves (iii).

To partially prove (iv), we compute the Artin Map

$$(\frac{L/K}{\cdot}) : I_K \longrightarrow Gal(M/K)$$

If we let $K_i = K(\sqrt{p_i^*})$, then M is the compositum of the K_i's, meaning we have the natural injection

$$Gal(M/K) \longrightarrow \prod_{i=1}^{r} Gal(K_i/K)$$

Furthermore, we may identify $Gal(K_i/K)$ as ± 1, so the Artin Map gives us the homomorphism $\phi : I_K \longrightarrow (\pm 1)^r$.

Now, we claim that if a is an ideal of O_K prime to $2d_K$, then $\phi(a)$ can be computed with the Legendre symbol as

$$\phi(a) = ((\frac{N(a)}{p_1}), (\frac{N(a)}{p_2}), \cdots, (\frac{N(a)}{p_r}))$$

It suffices to show that

$$(\frac{K_i/K}{p_i})\sqrt{p_i} = (\frac{N(a)}{p_i})\sqrt{p_i}$$

Letting B be a prime in O_{K_i} and $\sigma = (\frac{K_i/K}{p_i})$, we have

$$\sigma(p_i) \cong (\sqrt{p_i^*})^{N(p)} \cong (p_i^*)^{\frac{N(p)-1}{2}} \sqrt{p_i^*} \pmod B$$

. Since $N(p) = p$ or p^2, we can separately check each case to see that the expression is equivalent to $(\frac{N(a)}{p_i})\sqrt{p_i}$.

From this, we can make interesting statements, similar to those obtained from regular genus theory; for example, if $d_K \cong 0 \pmod 4$, then we can see that

$$C(O_K)/C(O_K)^2 \cong (\pm 1)^r$$

8 A Journey through Artin Reciprocity

The time has come to dive deeper into the realm of Artin Reciprocity, which we will jump straight into. While we will not provide a full proof, we aim to prove partial results as well as special cases of Artin Reciprocity.

Definition 8.1. We define P_F, m^+ as the set of principal ideals of F that have positive norm and are $\cong 1 \pmod{m}$.

Definition 8.2. We define $N_F^K(m)$ as the set of norms of I_F that are prime to m.

Theorem 8.3 (Consistency Property). *Suppose $F \subseteq L \subseteq K$ and $F \subseteq E \subseteq K$ are number fields with K/F abelian. Let P be a prime ideal of O_F that is unramified in K and Q be a prime ideal dividing P in O_K. Then the prime over Q in L is $Q \cap L = Q_L$ and similarly, the prime over Q in E is Q_E. Then*

$$(\frac{K/E}{Q_E})|_L = (\frac{L/F}{P})^f$$

where $|_L$ denotes restriction to L and $f = f(Q_E|P)$.

Proof. Let $\sigma_P = (\frac{L/F}{P})$ so that for any $\alpha \in O_L$, $\sigma(\alpha) \cong (\alpha)^{N(P)} \pmod{Q_L}$. Now, let ${}_{Q_E} = (\frac{K/E}{Q_E})$ so that ${}_{Q_E}(\alpha) \cong (\alpha)^{N(Q_E)} \pmod{Q}$ for all $\alpha \in O_K$. Then, if $\alpha \in O_L$, ${}_{Q_E}(\alpha) \cong (\alpha)^{N(Q_E)} \pmod{Q \cap L}$; since $Q \cap L = Q_L$, we have ${}_{Q_E}|_L(\alpha) \cong (\alpha)^{N(Q_E)} \pmod{Q_L}$. Now, $N(Q_E) = N(p)^f$, so

$$\sigma_P^f(\alpha) \cong (\alpha)^{N(P)^f} \cong (\alpha)^{N(Q_E)} \cong_{Q_E} |_L(\alpha) \pmod{Q_L}$$

It follows that $\sigma_P^f =_{Q_E} |_L$, as desired.

By the consistency property, we have

$$(\frac{K/E}{Q_E})|_L = (\frac{L/F}{P})^f = (\frac{L/F}{P^f}) = (\frac{L/F}{N_E^F(Q_E)})$$

so multiplicativity gives

$$(\frac{K/E}{U})|_L = (\frac{L/F}{N_E^F(U)})$$

where U is any fractional ideal in $I_E(m)$, the set of fractional ideals of E that are prime to m, where m, the *modulus*, is the product of all the ramified primes in E.

Corollary 8.4. *Using the same terminology as above,*

$$(\frac{K/F}{P})|_L = (\frac{L/F}{P})$$

Proof. Simply let $E = F$ in the theorem above!

Corollary 8.5. *We have*

$$(\frac{K/E}{Q_E}) = (\frac{K/F}{N_E^F(Q_E)})$$

Proof. Simply let $L = K$ in the theorem above!

Corollary 8.6. *We have that*

$$N_F^K(m) \subseteq ker(A : I_F(m) \longrightarrow Gal(K/F))$$

Proof. Letting $L = K = E$ gives

$$(\frac{K/F}{N_K^F(Q)}) = (\frac{K/K}{Q})|_K = 1$$

Thus, if U is any ideal of K prime to the ramifying primes in K/F, then factoring U gives

$$(\frac{K/F}{N_K^F(U)}) = 1$$

and the result follows.

Theorem 8.7 (Artin Reciprocity). *Let K/F be an abelian extension of number fields, and let m be an ideal of O_F that is divisible by all the ramifying primes. Let $G = Gal(K/F)$. Then*

(i) The homomorphism $A : I_F(m) \longrightarrow G$ is surjective.

(ii) $N_K^F(m) \subseteq ker(A)$.

(iii) The ideal m can be chosen so that it is divisible only by the ramifying primes and satisfies $P_F, m^+ \subseteq ker(A)$.

9 Into the Realm of Complex Multiplication and Beyond

A lot of the mathematics we have done up to this point take the existence of the Hilbert class field for granted - how do we even compute the Hilbert class field? Luckily, we have an interesting method to do so (at least for quadratic number fields): Complex Multiplication. This essentially exploits the group property of elliptic curves as well as features such as the j-invariant to actually compute the Hilbert class field. Although beyond the scope of this text (at the moment), Complex Multiplication forms a rather beautiful connection between algebraic number theory and the theory of elliptic curves. Still, much is unknown about computing the Hilbert Class Fields of higher degree number fields.

References

1. Cox, D.: Primes of the Form $x^2 + ny^2$. 2nd edn. Wiley-Interscience (1997)
2. Marcus, D.: Number Fields. 2nd edn. Springer International Publishing (2018)
3. Ireland, K., Rosen, M.: A Classical Introduction to Modern Number Theory. 2nd edn. Springer New York (1982)
4. Artin, M.: Algebra. 2nd edn. Pearson (2010)