Hilbert Class Field & Applications

Kirk Bonney

> The object of class field theory is to show how the abelian extensions of an algebraic number field K can be determined by elements drawn from a knowledge of K itself; or, if one prefers to present things in dialectical terms, how a field contains within itself the elements of its own transcending.
>
> *Chevalley (translated)*

1 Introduction

Class field theory is a deep and important collection of ideas in algebraic number theory which focuses on the characterization of abelian extensions of a local or global field K in terms of intrinsic properties of K. This theory forms the underpinnings of many modern areas of research. Most notably to myself, the Langlands program can be viewed as a series of generalizing conjectures for non-abelian class field theory. However, a competent understanding of even the basics of modern class field theory is a lofty goal for myself. The mission of this project is to take a small, first step towards this theory. We will investigate the Hilbert class field, a special case of class field theory, and see it applied to the question of when a rational prime p may be represented as

$$p = x^2 + ny^2$$

where x, y, and n are integers.

In particular, we follow §5 of Daniel Cox's *Primes of the Form x^2+ny^2* [2], where the primary objective is to prove the following theorem:

Theorem 1.1. *Let $n > 0$ be an integer satisfying the following condition: n squarefree, $n \neq 3 \bmod 4$. Then there is a monic irreducible polynomial $f_n(x) \in \mathbb{Z}[x]$ of degree $|C(\mathcal{O}_K)|$ such that if an odd prime p divides neither n nor the discriminant of $f_n(x)$, then*

$$p = x^2 + ny^2 \iff \begin{cases} (-n/p) = 1 \text{ and } f_n(x) \equiv 0 \bmod p \\ \text{has an integer solution.} \end{cases}$$

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

2 Background & Notation

This section establishes the background and notation necessary for proving theorem 1.1. For the entirety of the document, K is an algebraic number field and L is an algebraic extension of K, and we write $\mathcal{O}_K$ for the ring of integers of K.

2.1 Some results for quadratic extensions

Here we recount some basic facts about the behavior of primes in quadratic extensions for use in the proof of Theorem 1.1. First we recall the definition of the Legendre symbol (n/p). Let p be an odd rational prime, then

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & \text{if } n \text{ is a square modulo } p \\ -1 & \text{if } n \text{ is not a square modulo } p \\ 0 & \text{if } p|n. \end{cases}$$

We extend this definition to $p = 2$ by the following rule

$$\left(\frac{n}{2}\right) = \begin{cases} 1 & \text{if } n \equiv \pm 1 \bmod 8 \\ -1 & \text{if } n \equiv \pm 5 \bmod 8 \\ 0 & \text{if } n \equiv 0 \bmod 4. \end{cases}$$

Now we can state the results.

Proposition 2.1. *Proposition 5.16. Let K be a quadratic field of discriminant d_K, and let the nontrivial automorphism of K be denoted $\alpha \mapsto \alpha'$. Let p be a rational prime.*

(i) If $(d_K/p) = 0$ (i.e., $p \mid d_K$), 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 prime in $\mathcal{O}_K$.

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

Furthermore, the primes in (i)-(iii) above give all nonzero primes of $\mathcal{O}_K$.

Corollary 2.1. *Let K be a quadratic field of discriminant d_K and let p be a rational prime. Then:*

(i) p ramifies in K if and only if p divides d_K.

(ii) p splits completely in K if and only if $\left(\frac{d_K}{p}\right) = 1$.

2.2 The Hilbert Class Field

To begin, we prepare the necessary definitions for describing the Hilbert class field.

Definition 2.1. If L/K is Galois, we call L/K an *abelian extension* if $\mathrm{Gal}(L/K)$ is abelian.

We refer to a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ simply as a prime of K. In the next definition, we generalize the notion of a prime of K.

Definition 2.2. Let $\tau : K \to \mathbb{C}$ be an embedding. We say that τ is a *real infinite prime* if $\tau = \bar{\tau}$, where $\bar{\tau}$ indicates complex conjugation. When $\tau \neq \bar{\tau}$, we say that τ is a *complex infinite prime*.

To distinguish the previous definition from our usual notion of prime, we call an ideal $\mathfrak{p} \subset \mathcal{O}_K$ a *finite prime*, while we collectively refer to real and complex infinite primes as *infinite primes*. Why is this considered a generalization of a prime in the ideal sense? Given a finite prime $\mathfrak{p}$, we may define an absolute value $|\cdot|_P$ on K via

$$|a|_P = N(\mathfrak{p})^{-ord_{\mathfrak{p}}(a)},$$

where $N(\mathfrak{p})$ is the numerical, or absolute, norm $N(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}|$ and $ord_{\mathfrak{p}}(a)$ is the maximal power of $\mathfrak{p}$ containing in (a). Additionaly, for an infinite prime τ, we may define an absolute value $|\cdot|_\tau$ on K via

$$|a|_\tau = |\tau(a)|$$

where the unsubscripted $|\cdot|$ indicates the usual absolute value on $\mathbb{C}$. We remark that all absolute values on K arise in one of these two ways, with non-archimedean absolute values corresponding to finite primes, and archimedian absolute values corresponding to infinite primes. Thus finite and infinite primes are united by the perspective of absolute values.

Let $\mathfrak{p}$ be a finite prime of K. Consider the prime decomposition of $\mathfrak{p}$ in L/K

$$\mathfrak{p}/L = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i},$$

we say that $\mathfrak{p}$ is ramified in L if $e_i > 1$ for some i. Next, let τ be an infinite prime of K. We say that τ ramifies in L if τ is real and has an extenstion $\tilde{\tau} : L \to \mathbb{C}$ which is complex.

Definition 2.3. An algebraic extension L of a number field K is said to be *unramified* if all finite and infinite primes of K are unramified in L.

We are now in a position to define the Hilbert class field of K.

Theorem 2.1. *Given a number field K, there is a finite Galois extension L of K such that*

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

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

The field L of Theorem 2.1 is called the Hilbert class field of K and we denote it by $\mathcal{H}(K)$. It is the maximal unramified Abelian extension of K, thus it is unique.

Example 2.1. It is a theorem of Minkowski that $\mathbb{Q}$ has no non-trivial unramified extensions [5]. In particular, $\mathbb{Q}$ has no unramified abelian extensions, therefore $\mathcal{H}(\mathbb{Q}) = \mathbb{Q}$.

The previous example illustrates how restrictive the condition of unramified can be for extensions, however not every case is as trivial as $\mathbb{Q}$.

Example 2.2. Let $K = \mathbb{Q}(\sqrt{-5})$. Then $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ and we can show that it is not a PID. For example the ideal (2) factors as $\mathfrak{p}^2$ where $\mathfrak{p} = (2, 1 + \sqrt{-5})$.

When we add square root of -1 to K we obtain an unramified extension. Since $\mathbb{Q}(i)/\mathbb{Q}$ only ramifies at 2, $K(i)/K$ can only ramify at $\mathfrak{p}$. We can write $K(i) = K(\alpha)$ where $\alpha = (1+\sqrt{5})/2$, and the minimal polynomial $m_\alpha = x^2 - x - 1$ remains irreducible over L. Thus $\mathfrak{p}$ is not ramified in L.

K has two conjugate, infinite primes $\tau:\ a+\sqrt{-5} \mapsto a+\sqrt{-5}$ and $\bar{\tau}:\ a+\sqrt{-5} \mapsto a-\sqrt{-5}$. Since these are both complex, there is no way for an infinite prime of K to ramify. Since $K(i)/K$ is Abelian, it follows that $K(i) \subset \mathcal{H}(K)$.

Next, we recall the Artin symbol in order to state the main result of the Hilbert class field.

Definition 2.4. Let L/K be a Galois extension of number fields. Let $\mathfrak{p}$ be a prime of K unramified in L, and let $\mathfrak{P}$ be a prime of L containing $\mathfrak{p}$. It is a lemma that there exists a unique element σ of $\mathrm{Gal}(L/K)$ such that for all $\alpha \in \mathcal{O}_L$,

$$\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \bmod \mathfrak{P}.$$

We call this element the *Artin symbol* and write it as $((L/K)/\mathfrak{P})$ as it depends on the prime $\mathfrak{P}$.

Corollary 2.2. *Let $K \subset L$ 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 $\sigma \in \mathrm{Gal}(L/K)$, then

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

(ii) The order of $((L/K)/\mathfrak{P})$ is the inertial degree $f = f_{\mathfrak{P}|\mathfrak{p}}$.

(iii) $\mathfrak{p}$ splits completely in L if and only if $((L/K)/\mathfrak{P}) = 1$.

In our setting of Abelian extensions, the Artin symbol receives an important simplication. By part (i) of Corollary 2.2, the Artin symbol only depends on the the underlying prime $\mathfrak{p} = \mathcal{O}_k \cap \mathfrak{b}$. In these situations we can simply write $((L/K)/\mathfrak{p})$. It is also worth remarking that in the setting of unramified, Abelian extensions, $((L/K)/\mathfrak{p})$ exists for all $\mathfrak{p} \subset \mathcal{O}_K$. This key fact is part of why results surrounding the Hilbert class field may be stated in much simpler terms than those of general class field theory.

Let L/K be an unramified Abelian extension of number fields. Then, by the previous remark, we may extend the Artin symbol to a map on all ideals I_K of $\mathcal{O}_K$

$$\begin{aligned}\left(\frac{L/K}{\cdot}\right) : I_K &\longrightarrow \mathrm{Gal}(L/K),\\ \prod_{i=1}^{g} \mathfrak{p}_i^{e_i} &\longmapsto \prod_{i=1}^{g}\left(\frac{L/K}{\mathfrak{p}_i}\right)^{e_i}.\end{aligned}$$

What follows is the Artin Reciprocity Theorem for the Hilbert Class Field.

Theorem 2.2. *Let K be a number field and let $L = \mathcal{H}(K)$. Then the Artin map*

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

is surjective with kernel P_K, the principal ideals of $\mathcal{O}_K$. Therefore, the Artin map induces an isomorphism

$$\left(\frac{L/K}{\cdot}\right) : C(\mathcal{O}_K) \longrightarrow Gal(L/K).$$

The following corollary follows from Galois theory and gives us *class field theory for unramified Abelian extensions.*

Corollary 2.3. *Given a number field K, there is a one-to-one correspondence between unramified Abelian extensions M of K and subgroups of the ideal class group $C(\mathcal{O}_K)$. Furthermore, if the extension $K \subset M$ corresponds to the subgroup H, then the Artin map induces an isomorphism*

$$\left(\frac{L/K}{\cdot}\right) : C(\mathcal{O}_K)/H \longrightarrow Gal(M/K).$$

This corollary demonstrates what is meant by understanding extensions of K in terms of data intrinsic to K. The next result will be the key tool for getting started with the proof of theorem 1.1.

Corollary 2.4. *Let L be the HCF of a number field K, and let $\mathfrak{p}$ be a prime of K. Then,*

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

3 Proof of Theorem

Having established the Hilbert class field and class field theory for unramified abelian extensions, we are now ready to approach Theorem 1.1. In what follows, we discuss the main ideas for the proof of theoerem, but some details are omitted so the reader is referred to [2] if they desire a more complete exposition.

Proof. We sketch the proof of Theorem 1.1. The basic procedure is as follows:

- Relate the equation $p = x^2 + ny^2$ to the splitting behavior of p in $\mathcal{H}(\mathbb{Q}(\sqrt{-n}))$.
- Recharacterize the splitting behavior of rational primes p in the Hilbert class field to the existence of solutions to diophantine equations.
- Piece these together to obtain the desired proof.

The first result we need to proceed in the proof is the following connection between being a prime of the form $p = x^2 + ny^2$ and splitting behavior in a Hilbert class field.

Theorem 3.1. *Let $K = \mathbb{Q}(\sqrt{-n})$ where n is squarefree and $n \not\equiv 3 \bmod 4$ and let $L = \mathcal{H}(K)$. If p is an odd prime not dividing n, then*

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

Proof. The result follows from proving the following series of equivalences:

$$p = x^2 + ny^2 \iff p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}},\ \mathfrak{p} \neq \bar{\mathfrak{p}},\ \text{and } \mathfrak{p} \text{ is principal in } \mathcal{O}_K \tag{1}$$

$$\iff p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}},\ \mathfrak{p} \neq \bar{\mathfrak{p}},\ \text{and } \mathfrak{p} \text{ splits completely in } L \tag{2}$$

$$\iff p \text{ splits completely in } L. \tag{3}$$

For (1), if $p = x^2 + ny^2$ then we may factor p in $\mathcal{O}_K$ as $p = (x + \sqrt{-n}y)(x - \sqrt{-n}y)$, so the result follows if we write $\mathfrak{p} = (x + \sqrt{-n}y)\mathcal{O}_K$. Conversely, assuming $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$ with $\mathfrak{p} \neq \bar{\mathfrak{p}}$ and $\mathfrak{p}$ principal, we may write $\mathfrak{p} = (x + \sqrt{-n}y)$ for some $x, y \in \mathbb{Z}$ as $\mathcal{O}_K = \mathbb{Z}[\sqrt{-n}]$.

For (2), the equivalence follows directly from Corollary 2.4

For (3), we make use of the following lemma.

Lemma 3.1. *Let K be an imaginary quadratic extension of $\mathbb{Q}$, and let L be the HCF of K. Writing τ to denote complex conjugation, if $\tau(L) = L$ then L is Galois over $\mathbb{Q}$.*

The lemma tells us that L is Galois over Q, so if (p) ramifies as $\mathfrak{p}\bar{\mathfrak{p}}$ in $\mathcal{O}_K$, and both these ideals split completely over L, then p splits completely in L. □

This is an important step, as it tethers the equation $p = x^2 + ny^2$ to our new contraption, the Hilbert class field. Next we use the fact that when K is imaginary quadratic and L/K is Galois over $\mathbb{Q}$, there is a useful characterization of the splitting of primes of K in L.

Proposition 3.1. *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 $L = K(\alpha)$.

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

$$p \text{ splits completely in } L \iff \begin{cases} (d_K/p) = 1 \text{ and } f(x) \equiv 0 \bmod p \\ \text{has an integer solution.} \end{cases}$$

Via lemma 3.1 we established that L is Galois, so we can apply proposition 3.1 in out setting. Using part (i) there exists a real algebraic integer α such that $L = K(\alpha)$. Write $f_n(x) \in \mathbb{Z}[x]$ for the minimal polynomial of α and let p be an odd prime not dividing n or the discriminant of $f_n(x)$. By theorem 3.1 we have

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

and by proposition 3.1 part (ii) we have

$$\text{p splits completely in } L \iff \begin{cases} (-n/p) = 1 \text{ and } f_n(x) \equiv 0 \bmod p \\ \text{has an integer solution.} \end{cases}$$

Note that the condition $(d_K/p) = 1$ may be written as $(-n/p) = 1$ as $d_K = -4n$ and 4 is a square. Finally,

we show that $\deg f_n(x) = |C(\mathcal{O}_K)$. By theorem 2.2 we can write

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

□

4 Example

In general, it is difficult to calculate the Hilbert class field for an arbitrary number field K. However, by studying complex multiplication of elliptic curves we can unlock a family of examples. The following theorem is taken from Silverman's *Advanced Topics in Elliptic Curves* [6].

Theorem 4.1. *Let K be a quadratic imaginary field with ring of integers $\mathcal{O}_K$. Let $E/\mathbb{C}$ be an elliptic curve with End$(E) \simeq \mathcal{O}_K$. Write $j(E)$ for the j-invariant of E. Then $K(j(E))$ is the Hilbert class field of K.*

Example 4.1. Let us use the previous results to find which primes p may be written as $p = x^2 + ny^2$ for integers x and y. Given $K = \mathbb{Q}(\sqrt{-n})$, we can construct such an E by considering $\mathbb{C}/\mathbb{Z}[\sqrt{-n}]$ for example.

We examine the case for $n = 14$, so let $K = \mathbb{Q}(\sqrt{-14})$. It follows that $\mathcal{O}_K = \mathbb{Z}(\sqrt{-14})$. By Theorem 4.1, if we can find an elliptic curve E with $\mathrm{End}(E) = \mathbb{Z}(\sqrt{-14})$, then the Hilbert class field of K is $\mathbb{Q}(j(E))$. Using SageMath, we can find a j-invariant

$$j(E) = \frac{24531753960000}{15577}\gamma^7 + \frac{75517337448000}{15577}\gamma^6 + \frac{1147580275968000}{15577}\gamma^5 + \frac{2062639989144000}{15577}\gamma^4 + \frac{17801960425200000}{15577}\gamma^3 + \frac{6730855734456000}{15577}\gamma^2 + \frac{84943145452536000}{15577}\gamma - \frac{20718063777528000}{15577}.$$

where γ is a root of the polynomial

$$x^8 + 4x^7 + 62x^6 + 176x^5 + 1383x^4 + 2360x^3 + 12802x^2 + 9300x + 42953$$

corresponds to elliptic curves with End $= \mathbb{Z}[-14]$. By theorem 4.1, it follows that $\mathcal{H}(K) = \mathbb{Q}(j(E)) = \mathbb{Q}(\gamma)$. However,to apply Theorem 1.1 we want to know α where $\mathcal{H}(K) = K(\alpha)$. Again, using SageMath we can find that α is a root of $f_{14}(x) = x^4 + 2x^3 + x^2 + 2x + 1$. We will take $\alpha = \frac{1}{2}(-1 - \sqrt{2} - \sqrt{2\sqrt{2} - 1})$, which is a real root. Now we can apply theorem 1.1. Given a prime p not dividing 14 or disc$f$,

$$p = x^2 + 14y^2 \iff \begin{cases} (-14/p) = 1 \text{ and } f_{14}(x) \equiv 0 \bmod p \\ \text{has an integer solution.} \end{cases}$$

5 Conclusion/Towards HCF

In summary, we established the fundamentals of the Hilbert class field and saw how the Artin symbol provides an important correspondence between unramified Abelian extensions of a number field K and subgroups of the ideal class group $C(\mathcal{O}_K)$. Utilizing this theory we proved theorem 1.1, which gives us a partial answer to the question: when is a prime of the form $p = x^2 + ny^2$?

Investigating this theory provided me with a solid first expedition into the world of class field theory,

but many more journies lie ahead. For instance, I would like to better understand the role of infinite primes in the theory of Hilbert class fields. Past this, I want to begin understanding the basic premises of class field theory where ramification is studied. I am particularly interested in how theorem 4.1 generalizes: do higher genus arithmetic curves become involved? Also, why is non-abelian class field theory so difficult? It remains an open problem today and is believed to still be far out of reach...

References

[1] Jeff Achter. *605 Notes*.

[2] David A. Cox. *Primes of the form $p = x^2 + ny^2$: Fermat, class field theory, and complex multiplication*. John Wiley & Sons, Inc, Hoboken, New Jersey, second edition edition, 2013.

[3] Kiran Kedlaya. *Notes on class field theory*.

[4] J.S. Milne. *Class Field Theory*.

[5] Jürgen Neukirch. *Algebraic Number Theory*, volume 322 of *Grundlehren der mathematischen Wissenschaften*. Springer Berlin Heidelberg, Berlin, Heidelberg, 1999.

[6] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*, volume 151 of *Graduate Texts in Mathematics*. Springer New York, New York, NY, 1994.