ELLIPTIC CURVES AND THE HILBERT CLASS FIELD

ERIC YIN

Abstract. This paper goes over some basic class field theory and elliptic curve theory, discussing in particular the interplay between the ideal class group of algebraic number fields and their relation to the endomorphism ring of an elliptic curve over the complex numbers. By the end, we will describe the Hilbert class field of imaginary quadratic fields and their connection with their associated elliptic curves.

Contents

Introduction

1. Class Groups and Class Numbers

1.1. Preliminaries on Algebraic Integers.

The journey through number theory roughly follows two paths. On one, we study algebraic equations and their solution sets; linear and quadratic Diophantine equations have been studied since antiquity, and many of Fermat's various theorems can be interpreted through the perspective of rational solutions to polynomials. As it turns out, degree 1 polynomials and degree 2 polynomials are fairly simple to fully understand, and their rational solutions can be easily described. This is where we find solutions to famous equations such as the Pythagorean equation, which correspond to rational points on a circle (note $a^2 + b^2 = c^2$ for integers a, b, c if and only if $(\frac{a}{c})^2 + (\frac{b}{c})^2 = 1$, so $(\frac{a}{c}, \frac{b}{c})$ is an integer

Date: August 28, 2024.

point of the unit circle). Thus, we turn to the next rank of equations in terms of difficulty, elliptic curves, which have provided a rich field of study.

On the other path, we find the influence of algebra, and in particular commutative algebra, where the theory of rings infiltrates when describing prime numbers and prime factorization (as well as the lack thereof). It is also on this path that we find class field theory, which aims to describe abelian extensions of algebraic number fields. Of course, these paths are not distinct as this description may make it seem, and there is a plethora of connections between these paths. In this paper, we explore one specific place in which these paths intersect, the Hilbert class field, and provide the requisite background to build up to that result.

In Section 1 we build up a preliminary understanding of the ring theory needed in this paper, defining fractional ideals and the ideal class group, as well as exploring the class groups of various quadratic fields. In Section 2, we switch to the other path temporarily, and build up a preliminary understanding of elliptic curves and the structure of their endomorphism rings over general fields. In Section 3, we describe in particular how the algebraic structure of an elliptic curve corresponds to the analytic structure of the complex numbers. In Section 4, we tie these paths together by describing elliptic curves with complex multiplication, and specifically elliptic curves with endomorphism rings isomorphic to the ring of integers of the imaginary quadratic fields we discussed in Section 1.3. In Section 5, we build up a preliminary understanding of class field theory and describe how the Hilbert class field arises naturally out of the study of elliptic curves.

Definition 1.1. Let K be an algebraic number field, a finite extension of the rational numbers $\mathbb{Q}$. Then, we define the *ring of integers* R_K as the set of roots of monic polynomials $x^n + a_{n-1}x^{n-1} + ... + a_0$ with coefficients in $\mathbb{Z}$.

Alternatively, R_K is the *integral closure* of $\mathbb{Z}$ in K.

Example 1.2. Some common examples of algebraic number fields and their rings of integers are as follows:

a) If $K = \mathbb{Q}$, then $R_K = \mathbb{Z}$ as one might expect.
b) If $K = \mathbb{Q}[i]$, then $R_K = \mathbb{Z}[i]$.
c) In general, if $K = \mathbb{Q}[\sqrt{D}]$ for some squarefree $D \equiv 1 \mod 4$, then $R_K = \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right]$, as we can see that $\frac{1+\sqrt{D}}{2}$ is a root of the equation $x^2 - x - \frac{D-1}{4}$.
d) On the other hand, if $K = \mathbb{Q}[\sqrt{D}]$ for some squarefree $D \not\equiv 1 \mod 4$, then $R_K = \mathbb{Z}[\sqrt{D}]$.
e) If $K = \mathbb{Q}[\zeta_n]$ where ζ_n is a primitive nth root of unity, then $R_K = \mathbb{Z}[\zeta_n]$.

Since $\mathbb{Z}$ is a principal ideal domain (PID), it has prime elements p such that the ideals generated by p are both irreducible and prime. As a consequence of this, unique factorization holds: every integer can be factored into a product of primes and units, which are unique up to rearrangement. However, this property does not necessarily hold for all number fields, as the below example shows.

Example 1.3. Consider $\mathbb{Q}(\sqrt{-5})$, and its ring of integers $\mathbb{Z}[\sqrt{-5}]$. We have the classic example that $6 = 2 \cdot 3 = (1 - \sqrt{-5})(1 + \sqrt{-5})$, where each of $2, 3, 1 - \sqrt{-5}$, and $1 + \sqrt{-5}$ are irreducible. It is also easy to show through the field norm over $\mathbb{Q}$ that the only units of this field are ±1, so these are distinct prime factorizations of 6, and thus $\mathbb{Q}(\sqrt{5})$ is not a unique factorization domain (UFD), which implies it is not a PID.

We can show that for any algebraic number field K, the ring of integers R_K is a Dedekind domain, as defined below.

Definition 1.4. A ring R is a *Dedekind domain* if the following conditions hold:

a) R is Noetherian.
b) R is integrally closed, i.e. R is an integral domain and $R_{\mathrm{Frac}(R)} = R$, where $\mathrm{Frac}(R)$ is the fraction field of R.
c) Every nonzero prime ideal of R is maximal.

These properties are not hard to verify for any ring of integers R_K: R_K is integrally closed by definition, R_K is Noetherian as it is a finitely generated R module, and we can show that for every prime ideal $\mathfrak{p}$ of R_K, $R_K/\mathfrak{p}$ is a finite integral domain and thus a field, so $\mathfrak{p}$ is maximal. Then, the following properties hold:

Proposition 1.5. *Let R be a Dedekind domain. Then,*

a) Every proper ideal in R factors into a product of prime ideals uniquely up to rearrangement.
b) If R is a UFD, then R is a PID.

For a proof of this, see See [5] §9.3. From this second property we know that any ring of integers R_K is a UFD if and only if it is a PID. An example of factorization of proper ideals into prime ideals when prime factorization itself fails is as below:

Example 1.6. Once again consider $\mathbb{Q}(\sqrt{-5})$ and its ring of integers $\mathbb{Z}[\sqrt{-5}]$. Note that while 6 can be factored into irreducibles in multiple distinct ways, the ideal (6) factors uniquely through the prime ideals $(2, 1-\sqrt{-5})$, $(3, 2+\sqrt{-5})$, and $(3, 2-\sqrt{-5})$, and we can show that:

$$(2) = (2, 1-\sqrt{-5})^2,\ (3) = (3, 2+\sqrt{-5})(3, 2-\sqrt{-5}),$$
$$(1+\sqrt{-5}) = (2, 1-\sqrt{-5})(3, 2+\sqrt{-5}),\ (1-\sqrt{-5}) = (2, 1-\sqrt{-5})(3, 2-\sqrt{-5}),$$

and thus

$$(6) = (2)(3) = (1+\sqrt{-5})(1-\sqrt{-5}) = (2, 1-\sqrt{-5})^2(3, 2+\sqrt{-5})(3, 2-\sqrt{-5}).$$

1.2. **Fractional Ideals and the Class Group.** From here, for an algebraic number field K and its ring of integers R_K, we would like to measure the degree of failure of unique prime factorization. To do this, we introduce the concept of a fractional ideal.

Definition 1.7. Let K be an algebraic number field and R_K its field of fractions. A subset $\mathfrak{a} \subset K$ is a *fractional ideal* if there exists some nonzero $c \in R_K$ such that $c\mathfrak{a}$ is an ideal of R_K.

Equivalently, $\mathfrak{a}$ is a nonzero finitely generated R_K-submodule of K

As an example, we can consider the fractional ideal $(\alpha) = \alpha R_K$ for any nonzero $\alpha \in K$, since $\alpha^{-1}(\alpha) = \alpha^{-1}\alpha R_K = R_K$. We call fractional ideals of the form (α) *principal*. Just as with ideals, we can define multiplication of two fractional ideals $\mathfrak{a}$ and $\mathfrak{b}$ as $\mathfrak{a}\mathfrak{b} = \{\sum_i a_i b_i : a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\}$. Since there is a unique prime ideal decomposition of proper ideals in R_K, as it is a Dedekind domain, one might similarly expect a decomposition of fractional ideals into proper ideals, and in fact such a decomposition does exist.

Theorem 1.8. *Let K be an algebraic number field and R_K be its ring of integers. Then, any fractional ideal $\mathfrak{a}$ of R_K can be written as:*

$$\mathfrak{a} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}...\mathfrak{p}_n^{e_n},$$

where $\mathfrak{p}_1, ..., \mathfrak{p}_n$ are prime ideals of R_K and $e_1, ..., e_n \in \mathbb{Z}$, such that $\mathfrak{p}^{-e} = \{x \in K : x\mathfrak{p}^e \subset R_K\}$.

In fact, the converse also holds, any product $\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}...\mathfrak{p}_n^{e_n}$ of prime ideals is a fractional ideal of R_K. The proof of this theorem follows from the existence of a unique decomposition of proper ideals into prime ideals in Dedekind domains. Thus, we can use this to show that the set of fractional ideals of R_K forms a commutative group under multiplication as defined above, with identity element R_K and inverses given by $\mathfrak{a}^{-1} = \{x \in K : x\mathfrak{a} \subset R_K\}$. Note that the set of principal fractional ideals of R_K forms a subgroup, as for any principal fractional ideal (α), its inverse is (α^{-1}), which is also principal. Thus, we can now define the class group.

Definition 1.9. Let K be an algebraic number field, and R_K its ring of integers. The *ideal class group* of K, denoted as $Cl(K)$, is the quotient of the group of fractional ideals of R_K by the subgroup of principal fractional ideals of R_K. The *class number* of K is $|Cl(K)|$.

We claim that the ideal class group is finite for any algebraic number field, so the class number is well defined. We will roughly justify this claim for the case where K is an imaginary quadratic field, but the general case can be found in [2] §6.4. For another perspective, note that $Cl(K)$ is the cokernel of the map from $K^\times$ to the group of fractional ideals of R_K given by $\alpha \mapsto (\alpha)$.

If all ideals are principal, all fractional ideals are similarly principal as all prime ideals are principal. Thus, in a PID, we have the following proposition.

Proposition 1.10. *The ideal class group $Cl(K)$ is trivial (i.e. a group of one element) if and only if R_K is a PID.*

Since unique factorization into primes holds only when R_K is a PID, this means that the ideal class group and class number act as a measure of the failure of unique prime factorization, and the ideal class group is trivial if and only if unique prime factorization holds. We dive more into the implications of this through the simplest extensions of the rationals: quadratic fields.

1.3. Class Groups of Imaginary Quadratic Fields.

Let $K = \mathbb{Q}(\sqrt{D})$ for some squarefree D in $\mathbb{Z}$. We call K a quadratic field, and as in Example 1.2, we know that the ring of integers R_K of such a field takes the form:

$$R_{\mathbb{Q}(\sqrt{D})} = \begin{cases} \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right] & \text{if } D \equiv 1 \mod 4 \\ \mathbb{Z}[\sqrt{D}] & \text{otherwise.} \end{cases}$$

If an algebraic number field has an embedding into $\mathbb{R}$, we say that it is real, otherwise, we say that it is imaginary. In the case of quadratic fields, we have the expected result: $\mathbb{Q}(\sqrt{D})$ is real if $D > 0$ and imaginary if $D < 0$. Turning our attention to the class numbers of real and imaginary quadratic fields, we find two claims that are both interesting in their own right:

Conjecture 1.11. *(From Gauss) There are infinitely many real quadratic fields of class number 1.*

A list of currently known real quadratic fields with class number 1 is given by OEIS sequence A003172, and it is now known that for prime p, the probability that $\mathbb{Q}(\sqrt{p})$ has class number 1 is roughly 75.446% (see [6]). However, the conjecture that there are infinitely many real quadratic fields with class number one is still unproven.

On the other hand, for imaginary quadratic fields, we have:

Theorem 1.12. *The only imaginary quadratic fields with class number 1 are:*

$$\mathbb{Q}(\sqrt{-1}),\ \mathbb{Q}(\sqrt{-2}),\ \mathbb{Q}(\sqrt{-3}),\ \mathbb{Q}(\sqrt{-7}),\ \mathbb{Q}(\sqrt{-11}),\ \mathbb{Q}(\sqrt{-19}),$$

$$\mathbb{Q}(\sqrt{-43}),\ \mathbb{Q}(\sqrt{-67}),\ \mathbb{Q}(\sqrt{-163}).$$

Also originally a conjecture by Gauss, this was proven by Baker and Stark in 1966. The fact that there are only finitely many imaginary quadratic fields with class number 1 is almost startling in contrast to the real case. For the remainder of this section, we will provide a method to compute the class number of imaginary quadratic fields.

Definition 1.13. A group homomorphism $\chi : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}^\times$ is called a *Dirichlet character* modulo N. The *Dirichlet L function* $L(s, \chi)$ is defined as:

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

where $\chi(n)$ is defined as $\chi(n \mod N)$ if $\gcd(n, N) = 1$ and 0 otherwise.

Let $K = \mathbb{Q}\sqrt{D}$, an imaginary quadratic field, so $D < 0$ is squarefree. Let $N = |D|$ if $D \equiv 1 \mod 4$ and $N = |4D|$ otherwise. Then, K is contained in the cyclotomic field $\mathbb{Q}(\zeta_N)$, and we can find a Dirichlet character $\chi : \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \cong \mathbb{Z}/N\mathbb{Z}^\times \to \mathbb{C}^\times$.

Theorem 1.14. *Let K be an imaginary quadratic field and let N and χ be defined as above. Let h_K be the class number of K and w_K the number of roots of unity contained in K. Then,*

$$h_K = -\frac{w_K}{2N} \sum_{a=1}^{N} a\chi(a)$$

For a proof, see [2] §7.5. This formula is derived from a more general formula known as the *class number formula*, which in the imaginary case reduces to:

$$h_K = -\frac{w_K}{2} L(0, \chi).$$

by using the property that $L(0,\chi) = -\frac{1}{N}\sum_{a=1}^{N} a\chi(a)$. From this, we can see that since an imaginary quadratic extension of $\mathbb{Q}$ contains only finitely many roots of unity (4 for $\mathbb{Q}(\sqrt{-1})$, 6 for $\mathbb{Q}(\frac{1+\sqrt{-3}}{2})$, and 2 for every other imaginary quadratic field), the class number of an imaginary quadratic field must be finite.

2. Elliptic Curves

2.1. **Preliminaries on Elliptic Curves.** To begin, we will set up some notation to discuss elliptic curves. Let K be a field, and $\overline{K}$ be its algebraic closure. We can define affine n-space as $\mathbb{A}^n = \{P = (a_1, ..., a_n) \mid a_1, ..., a_n \in \overline{K}\}$ and projective n-space as $\mathbb{P}^n = \mathbb{A}^{n+1}/\sim$, where $\sim$ is the equivalence relation $(a_0, ..., a_n) \sim (b_0, ..., b_n)$ if there exists some $\lambda \in K^\times$ such that $a_i = \lambda b_i$ for all $i = 0, ..., n$ (i.e. $P \sim Q$ if $P = \lambda Q$). Finally, we can define homogenous coordinates on $\mathbb{P}^n$, $[X_0, ..., X_n]$, as well as a collection of maps $\phi_i : U_i \subset \mathbb{P}^n \to \mathbb{A}^n$, where $U_i = \{[X_0, ..., X_n] : X_i \neq 0\}$ and

$$[X_0, ..., X_n] \mapsto \left(\frac{X_0}{X_i}, ..., \frac{X_{i-1}}{X_i}, \frac{X_{i+1}}{X_i}, ..., \frac{X_n}{X_i}\right).$$

With this in place, we can define an elliptic curve as the subset of $\mathbb{P}^3 = \{[X, Y, Z]\}$ satisfying the following equation:

$$F(X, Y, Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 = 0,$$

under the condition that the resulting curve is nonsingular (i.e. there exists no $[X, Y, Z]$ such that $\frac{\partial F}{\partial X} = \frac{\partial F}{\partial Y} = \frac{\partial F}{\partial Z} = 0$). Notice that if $Z = 0$, then there is only one point that satisfies this equation, $[0, 1, 0]$. We will call this point O, the base point of an elliptic curve. Every other point of an elliptic curve thus lies in U_3 and can be mapped to $\mathbb{A}^2$, sending $[X, Y, Z]$ to $(X/Z, Y/Z)$. If we let $x = X/Z$ and $y = Y/Z$, we get the *Weierstrass equation* of an elliptic curve,

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Then, we can complete the square by using the substitution $y \mapsto \frac{1}{2}(y - a_1x - a_3)$ to achieve a simpler form:

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6,$$

where $b_2 = a_1^2 + 4a_4$, $b_4 = 2a_4 + a_1a_3$, and $b_6 = a_3^2 + 4a_6$.

Finally, if $\text{char}(\overline{K}) \neq 2, 3$, we can perform the substitution $(x, y) \mapsto \left(\frac{x-3b_2}{36}, \frac{y}{108}\right)$ to achieve the form:

$$E : y^2 = x^3 - 27c_4x - 54c_6,$$

where $c_4 = b_2^2 - 24b_4$ and $c_6 = -b_2^3 + 36b_2b_4 - 216b_6$. Since for the purposes of this paper we focus on elliptic curves over the complex numbers, we will mostly use this form of the Weierstrass equation for what follows. Thus, we can describe an elliptic curve E as the set of points that satisfy the above equation along with the base point O corresponding to a point at infinity. If the elliptic curve is defined over a field K (i.e. has coefficients in K), then we can define $E(K)$ as the set of points $E \cap \mathbb{A}^n(K) = E \cap \{P = (a_1, ..., a_n) \mid a_1, ..., a_n \in K\}$.

Definition 2.1. For the sake of simplicity, we define the constant b_8 as follows:

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,$$

With this, we can define the *discriminant* Δ and the *j-invariant* $j(E)$ of an elliptic curve E as follows:

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,$$

$$j(E) = \frac{c_4^3}{\Delta}.$$

We also have the relations:

$$1728\Delta = c_4^3 - c_6^2,\ j(E) = 1728\frac{c_4^3}{c_4^3 - c_6^2},$$

which follow by using the substitutions above.

We can first ask which Weierstrass equations correspond to an elliptic curve. As it turns out, the condition is incredibly simple:

Proposition 2.2. *The curve given by a Weierstrass equation is singular if and only if the discriminant $\Delta = 0$.*

This can be easily derived by checking when the base point O and the point $(0,0)$ are singular, as for any (x_0, y_0) satisfying a Weierstrass equation, the translation $(x,y) \mapsto (x + x_0, y + y_0)$ leaves the discriminant constant. Thus, elliptic curves are given by Weierstrass equations with nonzero discriminant. Next, we can ask when two different Weierstrass equations correspond to the same elliptic curve. The degree of uniqueness of the Weierstrass equation is given by the following proposition:

Proposition 2.3. *For a Weierstrass equation of the form $E : y^2 = x^3+Ax+B$, the only change of variables preserving this form are of the form $x = u^2x'$, $y = u^3y'$, for $u \in \overline{K}^\times$. Then, we have the following:*

$$A = u^4A',\ B = u^6B'\ \Delta = u^{12}\Delta',\ j(E) = j(E'),\ \omega = u^{-1}\omega'.$$

As shown above, two isomorphic elliptic curves have the same j-invariant. In fact, the converse is also true: any two elliptic curves with the same j-invariant will be isomorphic. The precise definition of isomorphic will be established later when morphisms of elliptic curves are discussed. To build up to that, we will first discuss the group structure of an elliptic curve.

2.2. **The Group Law.**

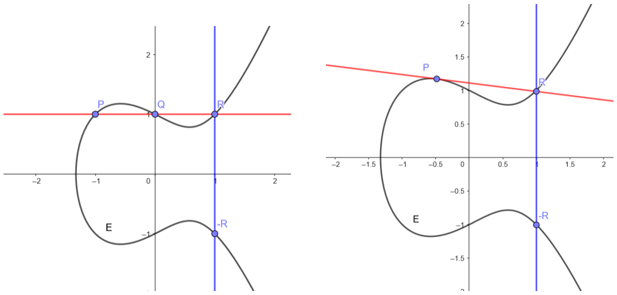
The image of an elliptic curve is particularly easy to draw in $\mathbb{R}^2$, and thus for the sake of visualization, we will portray elliptic curves over $\mathbb{R}$ in this section. However, the results hold for elliptic curves over an arbitrary field.

Note that for any elliptic curve, the intersection of an elliptic curve and a line consists of at most 3 points (including the base point O). Thus, we can define a group law on the elliptic curve as follows:

Definition 2.4. (The Group Law on an Elliptic Curve) Let P, Q be points on an elliptic curve E. Then, the line passing through P, Q will intersect E at another point, R. Similarly, the line passing through R and O will pass E at another point, $\ominus R$ (the justification for use of the minus sign will be apparent soon). We define a binary operation on E as follows:

$$P \oplus Q = \ominus R,$$

where $\ominus R$ is constructed as above. In the case where $P = Q$, we take the tangent line through P instead of the secant line through P, Q, and continue as above.



(A) $P \oplus Q = \ominus R$ for $P \neq Q$ (B) $P \oplus P = \ominus R$

Figure 1. Demonstration of the group law on the elliptic curve given by Weierstrass equation $y^2 = x^3 - x + 1$. Recall that the base point O is given by the point at ∞ in this image.

We can (somewhat laboriously) geometrically verify that this operation forms an abelian group on E with origin O by showing the associativity, commutativity, and the existence of inverses. As may be expected, $\ominus R$ is geometrically the inverse of R in this definition. However, instead we can also define this group operation algebraically by using the Weierstrass equation.

Consider the elliptic curve E given by Weierstrass equation:

$$F(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0.$$

First, consider $P = (x_0, y_0)$. To calculate $\ominus P$, we simply need to find the other point on the line passing through P and O, given by $x - x_0 = 0$. Plugging in, we find $F(x_0, y)$ is a quadratic in y, and therefore has two roots in $\overline{K}$, one of which must be y_0. Thus, the other root must give $\ominus P = (x_0, y_0')$, and writing out $F(x_0, y) = a(y - y_0)(y - y_0')$ will show that $y_0' = -y_0 - a_1x_0 - a_3$, so:

$$\ominus P = (x_0, -y_0 - a_1x_0 - a_3).$$

Now that we can find inverses, we can write out the full group law, as for any collinear P, Q, R in E, we have that $P \oplus Q = \ominus R$. It remains to express R in terms of P and Q. Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$. Then, the line through these points, assuming $x_1 \neq x_2$, is given by $y = \lambda x + \nu$, where $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ and $\nu = y_1 - \lambda x_1 = \frac{y_1x_2 - y_2x_1}{x_2 - x_1}$. We similarly have that $F(x, \lambda x + \nu)$ is now a cubic in x, so it must have three roots in $\overline{K}$, two of which correspond to x_1 and x_2. This third root, x_3, gives us $R = (x_3, \lambda x_3 + \nu)$. More explicitly, we can once again solve for x_3 by setting $F(x, \lambda x + \nu) = a(x - x_1)(x - x_2)(x - x_3)$, which yields:

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2,$$
$$y_3 = -(\lambda + a_1)x_3 - \nu - a_3.$$

We can apply the negation formula above to give us an explicit form of $P \oplus Q = \ominus(x_3, y_3)$.

Finally, we have the case that $x_1 = x_2$. If $y_2 = 2y_1 + a_1x_1 + a_3$, then $Q = \ominus P$, and $P \oplus Q = O$. Otherwise, we have that the tangent line has formula $y = \lambda x + \nu$, with $\lambda = \frac{3x_1^2+2a_2x_1+a_4-a_1y_1}{2y_1+a_1x+a_3}$ and $\nu = \frac{-x_1^3+a_4x_1+2a_6-a_3y_1}{2y_1+a_1x-1+a_3}$. The equations for x_3 and y_3 still follow as above, and we have that $P \oplus P = \ominus(x_3, y_3)$.

Proposition 2.5. $E(K)$ *(the points of the elliptic curve in affine K-space) is closed under this group operation.*

Using the algebraic formulas for the group law, we can see that they only use field operations, and thus points in K stay in K. We then have that $E(K)$ is a subgroup of E.

The last part of the group law algorithm hints at a "multiplication-by-m" map for $m \in \mathbb{Z}$, given by:

$$[m] : E \to E, \quad [m]P = \underbrace{P \oplus P \oplus .... \oplus P}_{m \text{ times}} \text{ for } m > 0,$$

where the cases $m = 0$ and $m < 0$ are given by $[0]P = O$ and $[m]P = \ominus[-m]P$, respectively.

2.3. **Endomorphisms of Elliptic Curves.** The multiplication-by-m map on an elliptic curve E will be our prototypical example of an endomorphism of E, a morphism from E to itself. To more precisely describe the endomorphisms of an elliptic curve, we must first define what we wish morphisms of elliptic curves to satisfy.

Let $E_1, E_2 \subset \mathbb{P}^n$ be curves, and $\overline{K}(E_1)$, $\overline{K}(E_2)$ be their function fields. Then, we have the following notions:

Definition 2.6. A *rational map* $\phi : E_1 \to E_2$ is a map of the form $\phi = [f_0, ..., f_n]$ for $f_0, ..., f_n \in \overline{K}(E_1)$ and for every point where $f_0, ..., f_n$ are all defined, $\phi(P) = [f_0(P), ..., f_n(P)] \in E_2$.

A rational map $\phi : E_1 \to E_2$ is *regular* at a point $P \in E_1$ if there exists some $g \in \overline{K}(E_1)$ such that for all i, gf_i is defined at P, and there exists some i such that $gf_i(P) \neq 0$.

A rational map that is regular at every point is called a *morphism.* As can be expected, an *isomorphism* is a morphism that is invertible on both sides: i.e. a morphism $\phi : E_1 \to E_2$ such that there exists a morphism $\psi : E_2 \to E_1$ satisfying the condition that $\phi \circ \psi$ and $\psi \circ \phi$ are the identity maps on E_2 and E_1, respectively.

These definitions are built for the more general class of algebraic varieties, which we do not use here for brevity. For curves specifically, we end up with a much stricter condition on morphisms.

Theorem 2.7. *([3] §II.2.3) If $\phi : E_1 \to E_2$ is a morphism of curves, then it is either constant or surjective.*

When viewing elliptic curves simply as curves, then this is the appropriate notion to use when discussing isomorphic curves. However, if we view elliptic curves with their group structure, then we need the stronger notion of isogeny.

Definition 2.8. A morphism $\phi : E_1 \to E_2$ between elliptic curves E_1 and E_2 is an *isogeny* if $\phi(O) = O$.

As is evident from the previous theorem, any isogeny of elliptic curves is either constant or surjective, and any constant isogeny $E_1 \to E_2$ must be the map that takes E_1 to the basepoint of E_2. Furthermore, while it is not immediately obvious, it turns out that every isogeny is also a group homomorphism from E_1 to E_2 (see [3] §III.4.8), so these are the appropriate maps for the perspective of elliptic curves as groups.

For an elliptic curve E, we can now consider the set of isogenies from E to itself, or in other words, the set of endomorphisms $\mathrm{End}(E)$. Note that since elliptic curves are abelian groups, their endomorphisms should also be an additive abelian group, with $(\phi + \psi)(P) = \phi(P) \oplus \psi(P)$ for all $\phi, \psi \in \mathrm{End}(E)$ and $P \in E$, with the additive identity being the constant endomorphism. We can also check that the composition of two endomorphisms of E is once again an endomorphism of E, and so $\mathrm{End}(E)$ becomes a ring with addition as defined above and multiplication defined as composition. Most ring axioms are evident through the properties of the group law on elliptic curves and morphisms of curves, and distributivity in particular follows from the fact that endomorphisms are group homomorphisms. An easy example of an endomorphism that we have already encountered is as follows:

Proposition 2.9. *For any elliptic curve E, the multiplication-by-m map $[m] : E \to E$ as defined above is an isogeny for any $m \in \mathbb{Z}$ and is nonconstant if m is nonzero.*

Both the zero map [0] which sends all points to O and the identity map [1] are morphisms, and we can show inductively that $[m]$ is a morphism for any other $m \in \mathbb{Z}$. Since $[m](O) = O$ by definition for all m, we also have that $[m]$ is an isogeny.

To show that the multiplication-by-m is nonconstant for nonzero m, we can show directly that there are only finitely many points with degree dividing m for any nonzero m (i.e. points such that $[m](P) = O$) using the group law formulas derived above. For more details, see [3] §III.4.2.

Corollary 2.10. *For any elliptic curve E, the endomorphism ring* $\mathrm{End}(E)$ *is an integral domain with characteristic zero.*

Addition and multiplication of multiplication-by-m maps acts as expected, with $[m] + [n] = [m + n]$ and $[m][n] = [mn]$, so we can embed $\mathbb{Z}$ into $\mathrm{End}(E)$ by sending $m \mapsto [m]$, thus showing that $\mathrm{End}(E)$ is a ring of characteristic zero. Furthermore, $\mathrm{End}(E)$ has no zero divisors as all nonzero endomorphisms are surjective, and the composition of surjective morphisms cannot be zero.

For some elliptic curves, the endomorphism ring consists solely of these multiplication-by-m maps, so $\mathrm{End}(E) \cong \mathbb{Z}$. One example of such an elliptic curve is $y^2 = x^3 + x + 2$, a Weierstrass equation with nonzero discriminant. However, as will be discussed further below, some elliptic curves have what is known as complex multiplication, an endomorphism ring larger than $\mathbb{Z}$. This will serve as our main point of reintroduction of the ideal class group that we began this paper with.

3. Elliptic Curves over the Complex Numbers

Before that, we discuss the specific case of an elliptic curve over the complex numbers: $E(\mathbb{C})$. While the results in this area are interesting, the computations for these results are largely analytic and thus not as relevant for this paper, so this section will roughly follow Silverman's treatment in chapter 6 of Arithmetic of Elliptic Curves [3]. Let Λ be a lattice over the complex numbers, or in other words, a set $\Lambda = \{a\omega_1 + b\omega_2 \mid a, b \in \mathbb{Z}\}$ where ω_1 and ω_2 are $\mathbb{R}$-linearly dependent. The goal of this section is to describe the relationship between the space of an elliptic curve over $\mathbb{C}$ and $\mathbb{C}/\Lambda$ as well as the association between elliptic curves and lattices Λ.

To do this, we first consider functions over $\mathbb{C}/\Lambda$. By necessity, functions over $\mathbb{C}/\Lambda$ are *doubly-periodic*: they have two linearly independent periods ω_1 and ω_2. Meromorphic functions of this sort are called *elliptic functions*, and through Liouville's theorem we can show that holomorphic functions that are doubly periodic are constant, and thus not very interesting. To construct some interesting elliptic functions, we must turn to the *Weierstrass $\wp$-function.*

Definition 3.1. Fix a lattice $\Lambda \subset \mathbb{C}$. The *Weierstrass $\wp$-function* with respect to that lattice is defined as:

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{z^2 + w^2} - \frac{1}{w^2} \right).$$

Associated with it (and the lattice Λ) is the *Eisenstein series* of weight $2k$:

$$G_{2k}(\Lambda) = \sum_{\omega \in \Lambda \setminus \{0\}} \omega^{-2k}.$$

This is often shortened to G_{2k} when the lattice is evident from context.

We can summarize the well-definedness and basic properties of these objects in the following proposition:

Proposition 3.2. *([3] §VI.3.1) Fix any lattice $\Lambda \subset \mathbb{C}$.*

a) The series defining the Weierstrass $\wp$-function converges absolutely and uniformly on any compact subset of $\mathbb{C} \setminus \Lambda$, and defines a even doubly-periodic meromorphic function on $\mathbb{C}$ with a double pole at every lattice point of Λ and no other poles.

b) The Eisenstein series G_{2k} is absolutely convergent for all $k > 1$.

Note that we could not use a single-poled function, since the residue around each lattice point of a doubly-periodic function must be zero due to the periodicity of the function. From the definition alone, these $\wp$-functions do not seem very interesting beyond the fact that they demonstrate the existence of elliptic functions through construction. However, we have the following theorem:

Theorem 3.3. *([3] §VI.3.2) Let $\Lambda \subset \mathbb{C}$ be a lattice. Then, every elliptic function is a rational combination of $\wp$ and $\wp'$.*

This is something very special; if we are to believe that $\mathbb{C}/\Lambda$ is associated with some elliptic curve, then elliptic functions should be associated with the function field of the curve. In this sense, $\wp$ and $\wp'$ seem to represent something as fundamental as x and y in a Weierstrass equation, and in fact we can show this relationship explicitly. Through some computation, we find that the Laurent series of $\wp(z)$ about $z = 0$ has the following form:

$$\wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty} (2k+1) G_{2k+2} z^{2k},$$

and by comparing terms, we find that $\wp$ and $\wp'$ satisfy

$$\wp'(z)^2 = 4\wp(z)^3 - 60G_4\wp(z) - 140G_6,$$

which is a Weierstrass equation. For the sake of notation, we set $g_2(\Lambda) = 60G_4(\Lambda)$ and $g_3 = 140G_6(\Lambda)$.

Theorem 3.4. *([3] §VI.3.6) Let $\Lambda \subset \mathbb{C}$ be a lattice, and $g_2 = g_2(\Lambda)$, $g_3 = g_3(\Lambda)$ be the associated quantities.*

a) The discriminant of the Weierstrass equation $y^2 = 4x^3 - g_2x - g_3$ is nonzero, so it represents an elliptic curve.
b) Let $E(\mathbb{C})$ be the curve with Weierstrass equation $y^2 = 4x^3 - g_2x - g_3$. Then, the map given by:

$$\phi : \mathbb{C}/\Lambda \to E(\mathbb{C})$$

$$z \mapsto [\wp(z), \wp'(z), 1]$$

is an isomorphism.

It is important to note that what is meant by isomorphism here is not an isomorphism of curves as in previous chapters, but rather an isomorphism of complex manifolds (in particular Riemann surfaces). Furthermore, this is also an isomorphism of the underlying groups of $\mathbb{C}/\Lambda$ and $E(\mathbb{C})$. Thus, every lattice can be associated with an elliptic curve $E/\mathbb{C}$. In the reverse direction, we have the Uniformization theorem:

Theorem 3.5. *([3] §VI.5.1) For any complex numbers A, B satisfying $4A^3 - 27B^2 \neq 0$, there exists a unique lattice $\Lambda \subset \mathbb{C}$ satisfying $g_2(\Lambda) = A$ and $g_2(\Lambda) = B$.*

For uniqueness, we turn to investigating maps between $\mathbb{C}/\Lambda_1$ and $\mathbb{C}/\Lambda_2$ for two lattices Λ_1 and Λ_2. If there exists some α such that $\alpha\Lambda_1 \subset \Lambda_2$, there is a natural map $\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ defined by $\phi(z) = \alpha z$, and as it turns out, these are the only holomorphic maps between $\mathbb{C}/\Lambda_1$ and $\mathbb{C}/\Lambda_2$.

Theorem 3.6. *([3] §VI.4.1) For any lattices Λ_1 and Λ_2 in $\mathbb{C}$ and elliptic curves E_1 and E_2 corresponding to those lattices, the following sets have a natural bijective correspondence:*

a) $\{\alpha \in \mathbb{C} \mid \alpha\Lambda_1 \subset \Lambda_2\}$
b) $\{$Holomorphic maps between $\mathbb{C}/\Lambda_1$ and $\mathbb{C}/\Lambda_2$ that fix the origin$\}$.
c) $\{$Isogenies between E_1 and $E_2\}$.

A corollary of this is that two elliptic curves $E_1(\mathbb{C})$ and $E_2(\mathbb{C})$ are isomorphic if and only their corresponding lattices Λ_1 and Λ_2 satisfy $\alpha\Lambda_1 = \Lambda_2$ for some $\alpha \in \mathbb{C}$, as only then are there nonconstant isogenies in both directions. We call two lattices that satisfy this condition *homothetic*, so we find that isomorphic elliptic curves correspond uniquely with lattices up to homothety. This equivalence between elliptic curves over $\mathbb{C}$ and lattices in $\mathbb{C}$ can be summarized in the following way:

Theorem 3.7. *([3] §VI.5.3) The following categories are equivalent:*

a) Objects: Elliptic curves over $\mathbb{C}$
Maps: Isogenies
b) Objects: Lattices $\Lambda \subset \mathbb{C}$, up to homothety
Maps: Hom$(\Lambda_1, \Lambda_2) = \{\alpha \in \mathbb{C} : \alpha\Lambda_1 \subset \Lambda_2\}$

4. Elliptic Curves with Complex Multiplication

Let $E(\mathbb{C})$ be an elliptic curve over the complex numbers, let Λ be the corresponding lattice with generators ω_1 and ω_2, and let $\operatorname{End}(E)$ be its isomorphism ring.

Theorem 4.1. *One of the following is true:*

a) $\operatorname{End}(E) \cong \mathbb{Z}$

b) $K = \mathbb{Q}(\omega_1/\omega_2)$ *is an imaginary quadratic extension of* $\mathbb{Q}$*, and* $\operatorname{End}(E)$ *is isomorphic to a* $\mathbb{Z}$*-lattice contained within* $\mathbb{Q}(\omega_1/\omega_2)$*. In other words,* $\operatorname{End}(E)$ *is an order within* $\mathbb{Q}(\omega_1/\omega_2)$

This theorem roughly follows from the fact that for any lattice Λ $(\omega_1/\omega_2)\Lambda = \mathbb{Z} + \mathbb{Z}\tau$ for some $\tau \in \mathbb{C} \setminus \mathbb{R}$. Then, we can use results from the previous section to realize that every $\alpha \in \operatorname{End}(E)$ corresponds to some $a + b\tau$ for some integers a and b, while $\alpha\tau$ corresponds to some $c + d\tau$ for some integers c and d. Thus, we can find a monic quadratic in $\mathbb{Z}$ that is satisfied by α, showing that $\operatorname{End}(E)$ is an order, and if $\operatorname{End}(E) \not\subset \mathbb{Z}$, then we can find an irreducible quadratic in $\mathbb{Z}$ that is satisfied by τ, so $\mathbb{Q}(\tau)$ is a quadratic field.

With this theorem, given any elliptic curve $E(\mathbb{C})$, we can find the corresponding lattice Λ and the associated imaginary quadratic field K that contains $\operatorname{End}(E)$. In particular, we know that $\operatorname{End}(E)$ must be contained within the ring of integers R_K, which is the maximal order of K.

Now, we can ask the question, for a ring R, what elliptic curves have endomorphism ring isomorphic to R? Let $\mathscr{E}(R)$ be the set of elliptic curves over the complex numbers up to isomorphism with $\operatorname{End}(E) \cong R$. From before, we know $\mathscr{E}(R)$ is equivalent to the set of lattices Λ with $\operatorname{End}(E_\Lambda) \cong R_K$. For the sake of simplicity, we will focus on the case where the endomorphism ring is integrally closed, so $\operatorname{End}(E) \cong R_K$ for an imaginary quadratic field K.

First, from Theorem 4.1 (b) we have that if $\operatorname{End}(E) \cong R_K$, we have that the corresponding lattice Λ must be contained in K. Note that for any imaginary quadratic field $\mathbb{Q}(\sqrt{D})$, the corresponding ring of integers $\mathbb{Z}[\sqrt{D}]$ (or $\mathbb{Z}[\frac{1-\sqrt{D}}{2}]$ if $D \equiv 1 \mod 4$) is a lattice in the complex numbers with generators 1 and $\sqrt{D}$ (or $\frac{1-\sqrt{D}}{2}$, respectively). Similarly, any fractional ideal $\mathfrak{a} \subset \mathbb{Q}(\sqrt{D})$ is also a lattice in $\mathbb{C}$ when embedding $\mathfrak{a} \subset K \subset \mathbb{C}$. Then, we have that $\operatorname{End}(E_\mathfrak{a}) \cong \{\alpha \in \mathbb{C} \mid \alpha\mathfrak{a} \subset \mathfrak{a}\} = R_K$ as $\mathfrak{a}$ is a fractional ideal in $K \subset \mathbb{C}$.

However, since elliptic curves generated by homothetic lattices are isomorphic-$E_\mathfrak{a} \cong E_{c\mathfrak{a}}$ for nonzero $c \in K$-this suggests that we should instead be looking at the class group of K, quotienting out the fractional ideals of K by the principal fractional ideals of K. This information can be summarized in the following proposition:

Proposition 4.2. *([4] §II.1.2) Let* Λ *be a lattice with* $E_\Lambda \in \mathscr{E}(R_K)$*, and let* $\mathfrak{a}$*,* $\mathfrak{b}$ *be fractional ideals in* K*. Then:*

a) $\mathfrak{a}\Lambda$ *is a lattice in* $\mathbb{C}$*.*

b) The elliptic curve $E_{\mathfrak{a}\Lambda}$ *satisfies* $\operatorname{End}(E_{\mathfrak{a}\Lambda}) \cong R_K$*.*

c) $E_{\mathfrak{a}\Lambda} \cong E_{\mathfrak{b}\Lambda}$ *if the image of* $\mathfrak{a}$ *and* $\mathfrak{b}$ *in* $Cl(R_K)$ *are equal.*

Thus, we can define a simply transitive action of $Cl(R_K)$ *on* $\mathscr{E}(R_K)$ *as:*

$$\bar{\mathfrak{a}} * E_\Lambda = E_{\mathfrak{a}^{-1}\Lambda}.$$

To round off this section, we will take one final pass at $\mathscr{E}(R_K)$. First, we have the following theorem:

Theorem 4.3. *Let $E(\mathbb{C})$ be an elliptic curve with complex multiplication by R_K for some quadratic imaginary field K. Then, $j(E)$ is an algebraic integer. Conversely, if $j(E)$ is not an algebraic integer, then* $\operatorname{End}(E) \cong \mathbb{Z}$.

The proof for this is complicated and can be found in [4] §V.6.3, but it is not too difficult to prove that $j(E)$ must be an algebraic number (i.e. in $\overline{\mathbb{Q}}$) by using the fact that for all field automorphisms σ of $\mathbb{C}$, $\operatorname{End}(E^\sigma) \cong \operatorname{End}(E)$ through the natural map $\operatorname{End}(E) \to \operatorname{End}(E^\sigma)$ with $\phi \mapsto \phi^\sigma$. As a side note, we claimed above that the elliptic curve given by $y^2 = x^3 + x + 2$ did not have complex multiplication. We can justify why that is the case here: the j-invariant of this curve can be computed to be $\frac{432}{7}$, which is not an algebraic integer.

As a result of the weaker form of the theorem, we have the following:

Proposition 4.4. *For any R_K as above, $\mathscr{E}(R_K)$ is isomorphic to the set of elliptic curves defined over $\overline{\mathbb{Q}}$ with* $\operatorname{End}(E) \cong R_K$ *quotiented by isomorphism over $\overline{\mathbb{Q}}$.*

Denote the latter set as $\mathscr{E}_{\overline{Q}}(R_K)$, and recall that $\mathscr{E}(R_K)$ was defined with elliptic curves over $\mathbb{C}$. Since there are embeddings $\overline{Q} \subset \mathbb{C}$, we only need to show that the natural map $\mathscr{E}_{\overline{Q}}(R_K) \to \mathscr{E}(R_K)$ is bijective, which we can do by using the fact that $j(E) \in \overline{Q}$.

Using all the above, for any imaginary quadratic field K, there is an action by $\operatorname{Gal}(\overline{K}/K) = \operatorname{Gal}(\overline{\mathbb{Q}}/K)$ on $\mathscr{E}(R_K)$, in which $\sigma \in \operatorname{Gal}(\overline{K}/K)$ acts on $E \in \mathscr{E}(R_K)$ by sending it to E^σ (or more specifically it sends the isomorphism class of a curve E to the isomorphism class of E^σ). However, from above, we have an action of $Cl(R_K)$ on $\mathscr{E}(R_K)$ that is simply transitive, so for every E and σ as above there is a unique $\overline{\mathfrak{a}} \in Cl(R_K)$ such that $\overline{\mathfrak{a}} * E = E^\sigma$. With this, we can define the following map:

$$F : \operatorname{Gal}(\overline{K}/K) \to Cl(R_K),$$

as the map satisfying $E^\sigma = F(\sigma) * E$ for all $\sigma \in \operatorname{Gal}(\overline{K}/K)$. As may be expected, this map has the following nice properties:

Proposition 4.5. *([4] §II.2.4) The map F as defined above satisfies the following properties:*

a) F is independent of the choice of E
b) F is a group homomorphism.

To check that F is a homomorphism for any fixed E, we note that for any $\sigma, \tau \in \operatorname{Gal}(\overline{K}/K)$:

$$F(\sigma\tau) * E = E^{\sigma\tau} = F(\tau) * (F(\sigma) * E) = (F(\tau)F(\sigma)) * E,$$

and we are done as $Cl(R_K)$ is abelian. Checking if F is independent of E turns out to be more difficult and can be found in Silverman [4], since there is an analytical component of the definition of F that must be dealt with.

5. Class Field Theory and the Hilbert Class Field

Let K be a totally imaginary number field, an algebraic number field that cannot be embedded in the reals, and let L be a finite and normal abelian extension of K, an extension with abelian Galois group $\mathrm{Gal}(L/K)$. We have as before the rings of integers R_K and R_L of K and L, respectively. Consider a prime ideal $\mathfrak{p}$ in R_K. In R_L, the ideal $\mathfrak{p} \cdot R_L$ decomposes into prime ideals $p_1^{e_1}...p_n^{e_n}$, with two distinct possibilities:

Definition 5.1. Let $\mathfrak{p}$ be a prime ideal in R_K which factors as $p_1^{e_1}...p_n^{e_n}$ in R_L, where $p_1, ..., p_n$ are distinct prime ideals in R_L. Then,

a) $\mathfrak{p}$ is called *unramified* if $e_1 = e_2 = ... = e_n = 1$. If $n = [L : K]$, then $\mathfrak{p}$ is said to *split completely.*

b) $\mathfrak{p}$ is called *ramified* otherwise, if there exists some i such that $e_i \geq 2$.

Let $\mathfrak{p} \in R_K$ be an unramified prime ideal and $p \in R_L$ be a prime ideal that divides $\mathfrak{p} \cdot R_L$. Then, we have that $R_K/\mathfrak{p}$ and R_L/p are finite fields, and since there are natural embeddings $R_K \subset R_L$ and $\mathfrak{p} \subset p$, we find an embedding of finite fields $R_K/\mathfrak{p} \subset R_L/p$. On one hand, the Galois group of this field extension $\mathrm{Gal}((R_L/p)/(R_K/\mathfrak{p}))$ is generated by the Frobenius automorphism, $x \mapsto x^{N_{K/\mathbb{Q}}\mathfrak{p}}$. On the other hand, elements of $\mathrm{Gal}(L/K)$ also act naturally on R_L/p so long as they fix p, so there is a homomorphism $\{\sigma \in \mathrm{Gal}(L/K) \mid p^\sigma = p\} \to \mathrm{Gal}((R_L/p)/(R_K/\mathfrak{p}))$.

Definition 5.2. Let $\mathfrak{c}$ be an ideal of R_K that is divisible by all primes that ramify in L/K, and let $I(\mathfrak{c})$ be the group of fractional ideals relatively prime to $\mathfrak{c}$. The *Artin Map* is defined for any $\mathfrak{a} = \prod \mathfrak{p}^{n_\mathfrak{p}} \in I(\mathfrak{c})$ as:

$$(\cdot, L/K) : I(\mathfrak{c}) \to \mathrm{Gal}(L/K)$$
$$(\mathfrak{a}, L/K) := \prod_{\mathfrak{p}} \sigma_{\mathfrak{p}}^{n_\mathfrak{p}}$$

The Artin map satisfies an important property known as Artin reciprocity:

Proposition 5.3. *([4] §II.3.1) With notation as above, there exists an ideal $\mathfrak{c} \subset R_K$, divisible only by the primes in K that ramify in L, such that $((\alpha), L/K) = 1$ for all $\alpha \in K^\times$ satisfying $\alpha \equiv 1 \mod \mathfrak{c}$.*

Since for any two ideals $\mathfrak{c}_1$ and $\mathfrak{c}_2$ that satisfy Artin reciprocity, $\mathfrak{c}_1 + \mathfrak{c}_2$ satisfies Artin reciprocity as well, we can identify the maximal ideal that satisfies Artin reciprocity. This ideal is the *conductor* of L/K, denoted as $\mathfrak{c}_{L/K}$. We can define the group of principal ideals congruent to 1 modulo $\mathfrak{c}$, $P(\mathfrak{c})$, which Artin reciprocity states will be a subgroup of the kernel.

The most significant case here is the case where L/K contains no ramified primes. We can designate the maximal unramified abelian extension as the *Hilbert Class Field H* of K, so that any other unramified abelian extension can be embedded into H. In H, since all primes are unramified, the conductor $\mathfrak{c}_{H/K}$ must be the unit ideal, since it cannot be divisible by any prime. Furthermore, $I(\mathfrak{c}_{H/K})$ is the group of all the fractional ideals of K, and $P(\mathfrak{c}_{H/K})$ is the group of all the nonzero principal ideals of K. By the maximality of the conductor and Artin reciprocity, we claim that the kernel of the Artin map is precisely $P(\mathfrak{c}_{H/K})$, so the Artin map induces an isomorphism between the ideal class group of K, the quotient $I(\mathfrak{c}H/K)/P(\mathfrak{c}H/K)$, and the Galois group of the Hilbert class field over K, $\mathrm{Gal}(H/K)$. Thus, $[H : K]$ is precisely the class number h_K.

Theorem 5.4. *Let $E(\mathbb{C})$ be an elliptic curve representing an isomorphism class in $\mathscr{E}(R_K)$. Then, $K(j(E))$ is the Hilbert class field H of K.*

We will provide a sketch of the proof of this theorem. Recall from section 4 that for any $E \in \mathscr{E}(R_K)$ we have a map $F : \mathrm{Gal}(\overline{K}/K) \to Cl(R_K)$. Let L be the fixed field of $\ker F$, so $\mathrm{Gal}(\overline{K}/L) = \ker F$. Since $Cl(R_K)$ acts simply transitively on $\mathscr{E}(R_K)$, we find that for all $\sigma \in \mathrm{Gal}(\overline{K}/L)$, $E^\sigma = F(\sigma) * E = 1 * E = E$ with F defined as before, which implies that $j(E^\sigma) = j(E)^\sigma = j(E)$, so $K(j(E)) \subset L$. Conversely, every element $\sigma \in \mathrm{Gal}(\overline{K}/K)$ that fixes $j(E)$ must also satisfy $F(\sigma) * E = E$, so $\ker F \subset \mathrm{Gal}(\overline{K}/K(j(E)))$, so by Galois correspondence, $L = K(j(E))$. Since F maps $\mathrm{Gal}(L/K)$ injectively into $Cl(R_K)$, $\mathrm{Gal}(L/K)$ must be abelian, so $L = K(j(E))$ is an abelian extension of K.

Now, we wish to show that L is unramified. To do this, we look at the composition of the Artin map with F:

$$I(\mathfrak{c}_{L/K}) \xrightarrow{(\cdot, L/K)} \mathrm{Gal}(L/K) \xrightarrow{F} Cl(R_K).$$

Here, we claim that this composition satisfies $F((\mathfrak{a}, L/K)) = \overline{\mathfrak{a}}$ for all $\mathfrak{a} \in I(\mathfrak{c}_{L/K})$: in other words, this composition is the natural projection into the ideal class group. From here, we find that every principal ideal $(\alpha) \in I(\mathfrak{c}_{L/K})$ is mapped to 1, not just the ideals which are congruent to 1 modulo $\mathfrak{c}_{L/K}$. By definition of the conductor and injectivity of F, we must have that every principal ideal is congruent to 1 modulo $\mathfrak{c}_{L/K}$ and thus $\mathfrak{c}_{L/K} = (1)$.

Finally, we wish to show that L is maximal. To show this, we only need to show that $[L : K] = [H : K] = h_K$. However, since we have that the natural projection $I((1)) \to Cl(R_K)$ is surjective, F must be surjective, and thus is an isomorphism between $\mathrm{Gal}(L/K)$ and $Cl(R_K)$, so $[L : K] = h_K$, and we are done.

Acknowledgments

I would like to thank my wonderful mentor Jinyue Luo for all her help this summer for topics both in and outside this paper. I would also like to thank Andrea Bourque for her willingness to answer my questions at even the most inopportune times, as well as a friend that shall remain unnamed for being a cat.

References

[1] Kato, K., et al. Number Theory 1: Fermat's Dream. American Mathematical Society, 2000.

[2] Kato, K., et al. Number Theory 2: Introduction to Class Field Theory. American Mathematical Society, 2011.

[3] Silverman, Joseph. The Arithmetic of Elliptic Curves. Springer International Publishing, 2009.

[4] Silverman, Joseph. Advanced Topics in the Arithmetic of Elliptic Curves. Springer International Publishing, 1994.

[5] Atiyah, M., & Macdonald, I.. Introduction to Commutative Algebra. CRC Press, 2018.

[6] Riele, Herman te, & Williams, Hugh. New Computations Concerning the Cohen-Lenstra Heuristics. Experimental Mathematics 12 (1): 99–113. doi:10.1080/10586458.2003.10504715.