Kronecker's Jugendtraum

Abhishek Shivkumar

I. INTRODUCTION

Our inquiry here is guided by the classical Kronecker-Weber Theorem.

Theorem 1 (Kronecker-Weber) *Every finite abelian extension of $\mathbb{Q}$ is contained within some cyclotomic field.*

This is a startling fact; every algebraic integer with abelian Galois group can be expressed as the $\mathbb{Q}$-linear sum of roots of unity. Hilbert's 12th problem asked for the analogue of roots of unity for base number fields other than $\mathbb{Q}$, the algebraic numbers which would generate the abelian extensions; the theory of complex multiplication, is one of a few cases where this problem has been completely solved. In particular, Kronecker postulated that the abelian extensions of imaginary quadratic number fields ($\mathbb{Q}(\sqrt{-D})$ for D square-free and positive) are generated by the values of *elliptic* (or doubly periodic) functions at certain points, resulting in the following, which we will prove:

Theorem 2 *Let $E/\mathbb{C}$ be an elliptic curve with complex multiplication by $\mathcal{O}_K$, where $K/\mathbb{Q}$ is an imaginary quadratic number field, then $K(j(E))$ is the Hilbert class field of K.*

The proof of this theorem, which is essentially a Kronecker-Weber theorem for imaginary quadratic fields, will require some amount of class field theory, as well as background on the structure of elliptic curves and on modular forms. The discussion here is distilled primarily from [2], with additional background from the other references.

II. BACKGROUND

A. Elliptic Curves and Lattices

A preliminary notion required to understand the theory of complex multiplication is the equivalence between lattices in $\mathbb{C}$ (up to some equivalence) and elliptic curves over $\mathbb{C}$. The essential idea is simple: $\mathbb{C}$ is a plane, and quotienting by the embedded $\mathbb{Z}^2$ with basis $(1, i)$ yields a torus via the ordinary geometric arguments; however, our choice of $\mathbb{Z}^2$ was somewhat arbitrary. We could have chosen, say, $(1, e^{i\pi/4})$ which also defines a lattice, albeit a non-square one. It turns out that different lattices (up to a notion of equivalence, which we will define) produce different complex structures on the resulting torus, in fact, infinitely many distinct complex structures.

First, we must define lattices in $\mathbb{C}$ and the equivalence relation among them (homothety); for our purposes, a lattice is a free abelian subgroup of rank 2 in $\mathbb{C}$; this can concretely be thought of as an embedded copy of $\mathbb{Z}^2$ (as a group) in $\mathbb{C}$, but to actually define it as such would encode the information of a canonical basis for the lattice, which is not necessary and leads to some extra work in classifying equivalent embeddings. We say that two lattices Λ_1 and Λ_2 are *homothetic* if there is a number $c \in \mathbb{C}^*$ such that $\Lambda_1 = c\Lambda_2$. If we set L to be the set of lattices in $\mathbb{C}$, then we claim that the set $L/\mathbb{C}^*$ is in bijection with the set of elliptic curves over $\mathbb{C}$ up to isomorphism respecting the complex structure.

Given a lattice Λ up to homothety, to produce an elliptic curve, we need the *Weierstrass $\wp$ function*:

$$\wp(z;\Lambda) = \frac{1}{z^2} + \sum_{\substack{\omega\in\Lambda\\ \omega\neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right)$$

with accompanying *Eisenstein series of weight* $2k$

$$G_{2k}(\Lambda) = \sum_{\substack{\omega\in\Lambda\\ \omega\neq 0}} \frac{1}{\omega^{2k}}$$

We take for granted that G_{2k} (we will generally suppress reference to the lattice Λ going forward) is absolutely convergent for $k > 1$, that $\wp(z)$ converges uniformly and absolutely on compacta of $\mathbb{C} \setminus \Lambda$, and that $\wp$ is an even elliptic function (elliptic here meaning that $\wp(z) = \wp(z + \omega)$ for all $\omega \in \Lambda$). Note that $\wp(z)$ can be written as a Laurent series as

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

To see this, note that

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \frac{1}{\omega^2} \sum_{n=1}^{\infty} (n+1)\frac{z^n}{\omega^n}$$

and back-substitute. One may use this formula to show that $\wp$ satisfies the differential equation

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

by calculating leading terms for the Laurent series of each term, and then noting that

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

is a holomorphic elliptic function, and therefore constant (by Liouville's theorem), and is in fact 0. Set $g_2 = 60G_4$ and $g_3 = 140G_6$.

Now, let $E/\mathbb{C}$ be an elliptic curve, with group law as shown in Figure 1; one can show that the group law $E \times E \to E$ is

given locally by rational functions, so E in fact possesses the structure of a complex Lie group (a complex manifold with locally complex analytic group law). Via standard theorems in the study of Lie groups, one can also see that the quotient $\mathbb{C}/\Lambda$ is a complex Lie group as well.

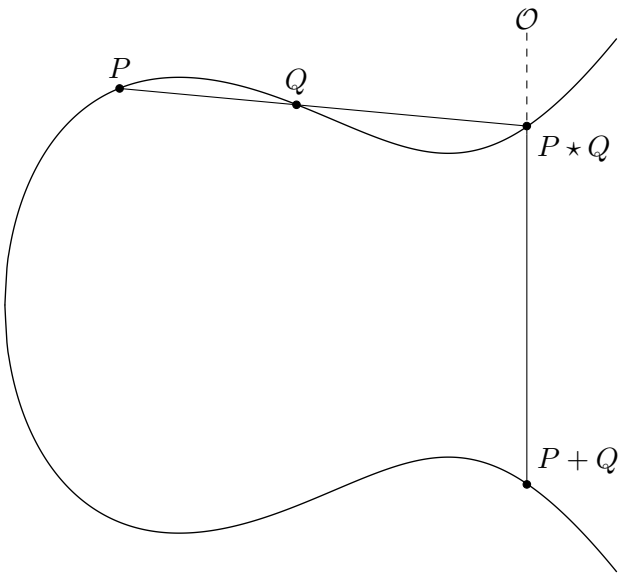

FIG. 1. The group structure on elliptic curves in projective space (with $\mathcal{O}$ the point at ∞)

We will also need the fact that $\frac{dx}{y}$ is a holomorphic nonvanishing differential on E (presented in Legendre form as $y^2 = x(x-1)(x-\lambda)$); to see this, note that $\mathrm{div}(dx) = (0) + (1) + (\lambda) - 3(\infty) = \mathrm{div}(y)$, from which it follows that $\frac{dx}{y}$ is both holomorphic and nonvanishing.

Proposition 3 *Given a lattice Λ with associated quantities g_2, g_3 as above, $\Delta = g_2^3 - 27g_3^2$ is nonzero, and therefore $E/\mathbb{C}$ given by*

$$y^2 = 4x^3 - g_2 x - g_3$$

is an elliptic curve. Moreover, there is a complex analytic isomorphism of complex Lie groups $\varphi : \mathbb{C}/\Lambda \to E(\mathbb{C})$ given by $\varphi(z) = [\wp(z), \wp'(z), 1]$.

Proof: First, since $\wp'$ is an (odd) elliptic function with respect to the same lattice, this map is well-defined. To see that Δ is nonzero, pick a basis ω_1, ω_2 for Λ, and set $\omega_3 = \omega_1 + \omega_2$. Since $\wp'$ is odd and elliptic,

$$\wp'\left(\frac{\omega_i}{2}\right) = -\wp'\left(-\frac{\omega_i}{2}\right) = -\wp'\left(\frac{\omega_i}{2}\right)$$

from which it follows that $\wp'\left(\frac{\omega_i}{2}\right) = 0$. By the differential equation satisfied by $\wp$, we can see that $4x^3 - g_2 x - g_3$ vanishes at $x = \wp'\left(\frac{\omega_i}{2}\right)$ for all i. It suffices to show that these three values are distinct so that our elliptic curve is nonsingular and $\Delta \neq 0$. To see this, note that $\wp(z) - \wp(\omega_i/2)$ is even, and therefore has a zero of order at least two at $z = \omega_i/2$; but $\wp$ is of order two (has two poles in an appropriate fundamental parallelogram), and therefore does not have any other zeros in the given fundamental domain, from which it follows that our three zeros are distinct.

To see that φ is an isomorphism of complex Lie groups, we first show that it is a bijection. For surjectivity, let $(x, y) \in E(\mathbb{C})$ and consider $\wp(z) - x$ which is a nonconstant elliptic function and therefore has a zero a (the number of zeros and poles of an elliptic function are equal, and nonconstant elliptic functions have poles). Then, by assumption,

$$4\wp(a)^3 - g_2\wp(a) - g_3 = y^2 = \wp'(a)^2$$

so, replacing a with $-a$ if necessary (since $\wp'$ is odd), we have that $y = \wp'(a)$ as desired. For injectivity, suppose $\varphi(z_1) = \varphi(z_2)$; assuming $2z_1 \notin \Lambda$, $\wp(z) - \wp(z_1)$ is elliptic of order 2 and vanishes at z_1, $-z_1$, and z_2. Since an order 2 elliptic function has two zeros, some two of these three are equal modulo Λ, and $z_1 \neq -z_1$ by the assumption that $2z_1 \notin \Lambda$, so $z_2 = \pm z_1$. Then,

$$\wp'(z_1) = \wp'(z_2) = \pm\wp'(z_1)$$

implies that $z_1 = z_2$. If $2z_1 \in \Lambda$, then $\wp(z) - \wp(z_1)$ is even and has a double zero at z_1, and vanishes at z_2, from which we may again conclude that $z_1 = z_2$.

To see that φ is a complex diffeomorphism, we need only show that φ^* is bijective on cotangent spaces; to that end, recall that $\frac{dx}{y}$ is holomorphic and nonvanishing on $E(\mathbb{C})$ (and therefore generates the cotangent space at each point), with

$$\varphi^* \frac{dx}{y} = \frac{d\wp(z)}{\wp'(z)} = dz$$

where the latter equality is the chain rule. Clearly, dz is holomorphic and nonvanishing on $\mathbb{C}/\Lambda$, from which the result follows.

We will omit the check that φ is a group homomorphism, which relies on the Weierstrass σ-function and the fact that the field of elliptic functions with respect to a given lattice is $\mathbb{C}(\wp(z), \wp'(z))$. ■

With this result alone, we can see that there is a map from $L/\mathbb{C}^*$ (lattices up to homothety) to the space of elliptic curves up to isomorphism; in fact, though we will not show it, this map is bijective, and two elliptic curves are isomorphic over $\mathbb{C}$ iff their lattices are homothetic.

Moreover, this bijection is in fact an equivalence of categories, between the category of elliptic curves $E/\mathbb{C}$ with group homomorphisms as maps, and the category of lattices with $\mathrm{Hom}(\Lambda_1, \Lambda_2) = \{\alpha \in \mathbb{C} : \alpha\Lambda_1 \subseteq \Lambda_2\}$. Note that it turns out that any complex analytic map of elliptic curves fixing the point at infinity (the neutral element, the identity of the group operation) is in fact a group homomorphism, so we are not artificially restricting our maps here to move from analysis to algebra.

This result allows us to more easily study the endomorphism rings (addition is pointwise, multiplication is com-

position) of elliptic curves; we know that for any $E/\mathbb{C}$, $[m] : E \to E$ is an endomorphism for all $m \in \mathbb{Z}$, so $\mathrm{End}(E)$ always contains $\mathbb{Z}$. However, given a lattice L associated to E, we know that

$$\mathrm{End}(E) = \{\alpha \in \mathbb{C} : \alpha L \subseteq L\}$$

In fact, we can say more:

Definition 4 (Orders) *Given L a $\mathbb{Q}$-algebra with $[L : \mathbb{Q}] = d$, an order in L is a subring $\mathcal{O}$ which as an abelian group is isomorphic to $\mathbb{Z}^d$.*

If L is commutative, then there exists a unique maximal order. Equivalently (for our purposes), if $K/\mathbb{Q}$ is a number field (and therefore a $\mathbb{Q}$-algebra), a subring $\mathcal{O}$ is an order if it is finitely generated as a $\mathbb{Z}$-module and $\mathcal{O} \otimes \mathbb{Q} = K$, and the maximal order in this case is $\mathcal{O}_K$.

Theorem 5 *If $\mathrm{End}(E)$ is larger than $\mathbb{Z}$, then, given generators ω_1, ω_2 for the lattice Λ associated to E, $\mathbb{Q}\left(\frac{\omega_2}{\omega_1}\right)$ is an imaginary quadratic extension of $\mathbb{Q}$ and $\mathrm{End}(E)$ is isomorphic to an order $\mathcal{O}$ in $\mathbb{Q}\left(\frac{\omega_2}{\omega_1}\right)$. In this case, we say that E has complex multiplication by $\mathcal{O}$.*

Proof: Let $\tau = \frac{\omega_2}{\omega_1}$; multiplying Λ by τ^{-1} shows that we may write $\Lambda = \mathbb{Z} \oplus \tau\mathbb{Z}$ (up to homothety). Let $\mathcal{O} = \{\alpha \in \mathbb{C} : \alpha\Lambda \subseteq \Lambda\} = \mathrm{End}(E)$; then for any $\alpha \in \mathcal{O}$, there exist $a, b, c, d \in \mathbb{Z}$ (since nonintegers cannot preserve an integral lattice) such that

$$\alpha = a + b\tau \quad \alpha\tau = c + d\tau$$

Eliminating τ, this becomes

$$\alpha^2 - (a + d)\alpha + (ad - bc) = 0$$

so $\mathcal{O}$ consists of elements integral over $\mathbb{Z}$, and is therefore an integral extension of $\mathbb{Z}$. Assuming $\mathcal{O}$ is bigger than $\mathbb{Z}$, let $\alpha \in \mathcal{O} \setminus \mathbb{Z}$, so $b \neq 0$, and eliminating α in our equations above yields

$$b\tau^2 + (a - d)\tau - c = 0$$

from which it follows that $\mathbb{Q}(\tau)$ is an imaginary quadratic extension of $\mathbb{Q}$ since $\tau \notin \mathbb{R}$; moreover, since $\mathcal{O} \subset \mathbb{Q}(\tau)$, and $\mathcal{O}$ is integral over $\mathbb{Z}$, $\mathcal{O}$ is an order in $\mathbb{Q}(\tau)$. ■

The above results justify the rather unimaginative term "complex multiplication" which is often used to describe the of study elliptic curves whose endomorphism rings are larger than $\mathbb{Z}$: all the endomorphisms of a complex elliptic curve correspond to multiplication by complex numbers α. Note that this result only holds for complex elliptic curves, to which we have restricted our study; in the general case, elliptic curves over arbitrary fields may also have an order in a quaternion algebra as their endomorphism ring.

B. The j-invariant

There is a standard (but not entirely canonical) way to associate a complex number τ to an elliptic curve which amounts to manipulating the lattice associated to the curve; in particular, given $E/\mathbb{C}$, choose a basis ω_1, ω_2 for the corresponding lattice Λ such that $\mathrm{Im}(\omega_1/\omega_2) > 0$ (by swapping ω_1 and ω_2, if necessary). Then Λ is homothetic to $\frac{\omega_1}{\omega_2}\mathbb{Z} \oplus \mathbb{Z}$, and this suggests looking at $\mathbb{H}$ (the upper half plane in $\mathbb{C}$) as a classifying space for elliptic curves. Clearly, we have a map $\mathbb{H} \to L/\mathbb{C}^*$ given by $\tau \mapsto \Lambda_\tau := \tau\mathbb{Z} \oplus \mathbb{Z}$, but this map is not injective.

Lemma 6 *Let $\tau_1, \tau_2 \in \mathbb{H}$. Then the corresponding lattices $\Lambda_{\tau_1}, \Lambda_{\tau_2}$ are homothetic iff there exists $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ such that $\tau_2 = \frac{a\tau_1 + b}{c\tau_2 + d}$.*

The proof of this lemma consists of a sequence of unenlightening calculations, so we omit it here. Note, however, that $-I$ acts trivially upon $\mathbb{H}$:

$$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \tau = \frac{-\tau}{-1} = \tau$$

This leads us to define the following:

Definition 7 (Modular Group) *The modular group written $\Gamma(1)$ or $\mathrm{PSL}_2(\mathbb{Z})$ is the quotient group $\mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$.*

It is easy to see that $\pm I$ are the only elements in $\mathrm{SL}_2(\mathbb{Z})$ fixing $\mathbb{H}$: if $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ satisfies $\gamma\tau = \tau$ for all $\tau \in \mathbb{H}$, then

$$\frac{a\tau + b}{c\tau + d} = \tau \iff c\tau^2 + (d - a)\tau - b = 0$$

for all τ. Because there are more than two elements of $\mathbb{H}$, this quadratic must be identically 0, so $c = b = 0$ and $a = d$. Moreover, $ad = a^2 = 1$ by the determinant constraint, from which it follows that $a = d = \pm 1$.

Therefore, $\Gamma(1)$ is the group whose action on $\mathbb{H}$ corresponds to homothety on the set of lattices or isomorphism on the set of elliptic curves, e.g, $\mathbb{H}/\Gamma(1)$ is in bijection with elliptic curves over $\mathbb{C}$ up to isomorphism.

Definition 8 (The j-invariant) *Given an elliptic curve E written in the form*

$$y^2 = 4x^3 - g_2x - g_3$$

define

$$j(E) = 1728\frac{g_2^3}{\Delta} = 1728\frac{g_2^3}{g_2^3 - 27g_3^2}$$

The prefactor 1728 can be omitted in our case, as it is included to resolve some issues that arise when dealing with

elliptic curves over a field of characteristic 2 or 3. The purpose of the above discussion is to see that j is in fact a function on the upper half plane, given by $\tau \mapsto j(E(\tau))$ where E is the elliptic curve associated to τ. By this definition, j is manifestly well-defined under the action of $\Gamma(1)$, and is therefore a *modular function.* Since $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right) \in \Gamma(1)$ corresponds to $\tau \mapsto \tau + 1$, j is $\mathbb{Z}$-translation invariant, (e.g $j(\tau+1) = j(\tau)$), and can be shown to be meromorphic with a simple pole, therefore admitting a Fourier expansion in a neighborhood of $q = e^{2\pi i \tau} = 0$:

$$j(\tau) = q^{-1} + 744 + 196884q + 21493760q^2 + \cdots$$

The j-invariant is important for our study, as we will see that arithmetic facts about elliptic curves with complex multiplication correspond to arithmetic facts about the values of certain modular functions and forms, including j. In particular, over $\mathbb{C}$, the j-invariant is a complete invariant for elliptic curves; e.g, $E = E'$ iff $j(E) = j(E')$.

C. Class Field Theory

Class field theory, loosely, is the study of abelian extensions of number fields, of which complex multiplication is a specific case where many results can be made explicit. In this section, we will attempt to state, without proof, the bare minimum background in class field theory required to state and/or prove the results we want to further explore.

Let K be a totally imaginary number field, L a finite Galois extension of K with abelian Galois group G (henceforth referred to as an abelian extension). Let $\mathfrak{p}$ be an unramified prime of K, $\mathfrak{P}$ in L above $\mathfrak{p}$, with corresponding residue field extension $(\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})$ (which is Galois, as we saw in lecture). There is a natural (surjective) homomorphism from the decomposition group $D_{\mathfrak{P}}$ (the stabilizer of $\mathfrak{P}$ in G) to $G' = \mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p}))$ given by restriction. G' is cyclic generated by the Frobenius automorphism $x \mapsto x^{N_{K/\mathbb{Q}}(\mathfrak{p})}$; since $\mathfrak{p}$ is unramified iff the inertia group is trivial, there is a unique $\sigma_{\mathfrak{p}} \in \mathrm{Gal}(L/K)$ mapping to the Frobenius automorphism, satisfying (and uniquely determined by)

$$\sigma_{\mathfrak{p}}(x) \equiv x^{N_{K/\mathbb{Q}}(\mathfrak{p})} \pmod{\mathfrak{P}} \text{ for all } x \in \mathcal{O}_L$$

Let $\mathfrak{c}$ be an ideal in $\mathcal{O}_K$ divisible by all primes which ramify in L/K, and let $I(\mathfrak{c})$ be the group of fractional ideals of K relatively prime to $\mathfrak{c}$.

Definition 9 (The Artin Symbol) *Define* $(-, L/K) : I(\mathfrak{c}) \to \mathrm{Gal}(L/K)$ *by*

$$(\mathfrak{a}, L/K) = \left(\prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}, L/K\right) := \prod_{\mathfrak{p}} \sigma_p^{n_{\mathfrak{p}}}$$

where $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$.

The Artin map, in this formulation, just glues together the local information of $\sigma_{\mathfrak{p}}$ at each unramified prime. It is a relevant quantity because of the following important fact:

Theorem 10 (Weak Artin Reciprocity) *With L/K a finite abelian extension of number fields, there exists an ideal $\mathfrak{c} \subset \mathcal{O}_K$ divisible by only the primes of K which ramify in L, such that $((\alpha), L/K) = 1$ for all $\alpha \in K^*$ satisfying $\alpha \equiv 1 \pmod{\mathfrak{c}}$.*

Note that if Artin reciprocity holds for ideals $\mathfrak{c}_1$ and $\mathfrak{c}_2$, then it vacuously holds for $\mathfrak{c}_1 + \mathfrak{c}_2$, so there exists an ideal maximal with respect to the property that Artin reciprocity holds; we call this ideal the conductor of L/K, denoted $\mathfrak{c}_{L/K}$.

To at least partially justify the use of the term "reciprocity" here, we will show that quadratic reciprocity follows from Artin reciprocity via straightforward calculations. Consider $\mathbb{Q}(\sqrt{p^*}) := \mathbb{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}}p}\right) \subseteq \mathbb{Q}(\zeta_p)$ where $\zeta_p = e^{\frac{2\pi i}{p}}$ for some odd prime p; to see that this containment holds, recall that

$$\sqrt{(-1)^{\frac{p-1}{2}}p} = \sum_{k=0}^{p-1} \zeta_p^{k^2}$$

which follows by a mod 4 analysis and the fact that

$$\sum_{k=0}^{p-1} \zeta_p^{k^2} = \sum_{k=0}^{p-1} \left(1 + \left(\frac{k}{p}\right)\right) \zeta_p^k$$

(this from the proof that all quadratic extensions are contained in some cyclotomic extension, a special case of the Kronecker-Weber theorem). Therefore, our setup is a number field an an extension of it: $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{p^*}) \subseteq \mathbb{Q}(\zeta_p)$; moreover, since all quadratic extensions are Galois, and $\mathbb{Q}(\zeta_p)$ is abelian with Galois group $(\mathbb{Z}/(p))^\times \cong \mathbb{Z}/(p-1)$, we may conclude that $\mathbb{Q}(\sqrt{p^*}) \subseteq \mathbb{Q}(\zeta_p)$ is abelian Galois as well. This allows us consider the Artin map with respect to only primes in $\mathbb{Z}$, as the (distinct) primes above a given prime in $\mathbb{Z}$ are all Galois conjugate, and therefore equal by abelianity.

Let q be another odd prime, and note that p^* is a square mod q iff q splits in $\mathbb{Q}(\sqrt{p^*})$ which in turn holds iff the Artin symbol of q in $\mathbb{Q}(\sqrt{p^*})/\mathbb{Q}$ is trivial (this is where we use Artin reciprocity); this Artin symbol arises as the restriction of the corresponding Artin symbol in $\mathbb{Q}(\zeta_p)/\mathbb{Q}$.

The Artin symbol of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ at the prime q is $((q), \mathbb{Q}(\zeta_p)/\mathbb{Q}) = (\zeta_p \mapsto \zeta_p^q)$ in $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, since $N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(q) = q^{p-1} \equiv q \pmod{p}$. $((q), \mathbb{Q}(\sqrt{p^*})/\mathbb{Q})$ is the image of the previous Artin symbol under the restriction morphism; since both Galois groups are cyclic, this morphism is the unique nontrivial homomorphism from $(\mathbb{Z}/(p))^\times \to \mathbb{Z}/(2) = \{\pm 1\}$, e.g, the Legendre symbol. Therefore, we have shown that $\left(\frac{q}{p}\right) = 1$ iff $\left(\frac{p^*}{q}\right) = 1$, e.g, their product is always 1, so

$$\left(\frac{q}{p}\right)\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)\left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = 1$$

where the latter equality uses Euler's criterion.

Definition 11 (Hilbert Class Field) *The Hilbert Class Field of a number field $K/\mathbb{Q}$ is a finite abelian extension H/K with the property that for any other finite abelian extension L/K, $L \subseteq H$.*

The Hilbert class field is the maximal unramified abelian extension of a given number field K, and satisfies $\mathrm{Gal}(H/K) = \mathrm{Cl}(K)$ (where $=$ denotes a canonical isomorphism). That such a field uniquely exists is a difficult result in general which we will borrow, although we will directly construct the Hilbert class field for imaginary quadratic number fields and directly prove its usual nice properties in this case.

Theorem 12 (Results from Class Field Theory) *With L/K and $\mathfrak{c}_{L/K}$ as above, the Artin map $(-, L/K) : I(\mathfrak{c}_{L/K}) \to \mathrm{Gal}(L/K)$ is a surjective homomorphism, with kernel $(N_{L/K} I_L) P(\mathfrak{c}_{L/K})$ where I_L is the group of non-zero fractional ideals of L, $P(\mathfrak{c}_{L/K})$ the group of principal ideals which are $1 \pmod{\mathfrak{c}_{L/K}}$.*

Moreover, the Hilbert class field H of K uniquely exists, with conductor (1), and satisfying the property that all prime principal ideals in K split completely in H.

Note that $I(\mathfrak{c}_{H/K}) = I(1)$ consists of all non-zero fractional ideals of K, $P(\mathfrak{c}_{H/K})$ consists of all non-zero principal ideals of K, so the above results imply that $(-, H/K)$ induces an isomorphism between $\mathrm{Cl}(K)$ and $\mathrm{Gal}(H/K)$.

Finally, we will need the following version of Dirichlet's theorem on primes in arithmetic progressions:

Theorem 13 *Let K be a number field, $\mathfrak{c}$ an integral ideal. Every class in $I(\mathfrak{c})/P(\mathfrak{c})$ contains infinitely many degree 1 primes of K.*

III. RESULTS

We are now nearly ready to prove our main result:

Theorem 14 *Let $E/\mathbb{C}$ be an elliptic curve with complex multiplication by $\mathcal{O}_K$, where $K/\mathbb{Q}$ is an imaginary quadratic number field, then $K(j(E))$ is the Hilbert class field of K, and $\mathrm{Gal}(K(j(E)), K) = \mathrm{Cl}(K)$ (which we show without appeal to the general theory of Hilbert class fields).*

First note, however, that given $\mathcal{O}_K$, we can always produce an elliptic curve with complex multiplication by $\mathcal{O}_K$, for example, by taking E to be $E_{\mathcal{O}_K}$, the curve corresponding to the lattice, since $\mathrm{End}(E_{\mathcal{O}_K}) \cong \{\alpha \in \mathbb{C} : \alpha \mathcal{O}_K \subseteq \mathcal{O}_K\} = \mathcal{O}_K$ where the latter equality follows from the observation that if $\alpha \mathcal{O}_K \subseteq \mathcal{O}_K$, then $\alpha \in \mathcal{O}_K$ since $\mathcal{O}_K$ contains 1 (with the other inclusion obvious). Clearly, any lattice homothetic to $\mathcal{O}_K$ also corresponds to an elliptic curve with $\mathcal{O}_K$ complex multiplication; in fact, more can be said, and we will explore this below. Understanding which elliptic curves (equivalently lattices) have complex multiplication by $\mathcal{O}_K$ is useful. For the following discussion, let $\mathcal{ELL}(\mathcal{O})$ be the set of elliptic curves $E/\mathbb{C}$ up to isomorphism with $\mathrm{End}(E) = \mathcal{O}$.

Proposition 15 *$\mathrm{Cl}(\mathcal{O}_K)$ has a natural action on $\mathcal{ELL}(\mathcal{O}_K)$ which is simply transitive.*

Proof: To produce the action, we observe that, given $\mathfrak{a}, \mathfrak{b}$ nonzero fractional ideals of K, a lattice Λ with $E_\Lambda \in \mathcal{ELL}(\mathcal{O}_K)$, $\mathfrak{a}\Lambda$ is a lattice with $\mathrm{End}(\mathfrak{a}\Lambda) \cong \mathcal{O}_K$, and $E_{\mathfrak{a}\Lambda} = E_{\mathfrak{b}\Lambda}$ iff $\mathfrak{a} = \mathfrak{b}$ in $\mathrm{Cl}(K)$, e.g, up to principal ideals (homothety). To see that $\mathfrak{a}\Lambda$ is a lattice in $\mathbb{C}$, note that since $\mathrm{End}(E_\Lambda) = \mathcal{O}_K$, $\mathcal{O}_K \Lambda = \Lambda$. Since $\mathfrak{a}$ is a fractional ideal, there exists $d \in \mathbb{Z}$ such that $d\mathfrak{a} \subset \mathcal{O}_K$, so $\mathfrak{a}\Lambda \subseteq \frac{1}{d}\Lambda$, so $\mathfrak{a}\Lambda$. Similarly, finding d s.t $d\mathcal{O}_K \subset \mathfrak{a}$, this implies that $d\Lambda \subseteq \mathfrak{a}\Lambda$ from which it follows that $\mathfrak{a}\Lambda$ spans $\mathbb{C}$ and is therefore a lattice.

To see that $\mathfrak{a}\Lambda$ corresponds to an elliptic curve with complex multiplication by $\mathcal{O}_K$, note that for any $\alpha \in \mathbb{C}$, $\mathfrak{a}$ a nonzero fractional ideal, we have

$$\alpha\mathfrak{a}\Lambda \subseteq \mathfrak{a}\Lambda \iff \mathfrak{a}^{-1}\alpha\mathfrak{a}\Lambda \subseteq \mathfrak{a}^{-1}\mathfrak{a}\Lambda \iff \mathfrak{a}\Lambda \subseteq \Lambda$$

so $\mathrm{End}(E_{\alpha\Lambda}) = \{\alpha \in \mathbb{C} : \alpha\Lambda \subseteq \Lambda\} = \mathcal{O}_K$ by the above identifications, and by assumption.

Finally, to see that the action of ideals descends to the action of ideal classes, note that if $\mathfrak{a} = \mathfrak{b}$ in $\mathrm{Cl}(K)$, then $\mathfrak{a} = c\mathfrak{b}$ for some $c \in K$, so $\mathfrak{a}\Lambda$ and $\mathfrak{b}\Lambda$ are homothetic.

Then, we define the action $\mathrm{Cl}(K) \curvearrowright \mathcal{ELL}(\mathcal{O}_K)$ as

$$\mathfrak{a} \times E_\Lambda = E_{\mathfrak{a}^{-1}\Lambda}$$

where we multiply by $\mathfrak{a}^{-1}$ so that

$$\mathfrak{a} \times (\mathfrak{b} \times E_\Lambda) = \mathfrak{a} \times (E_{\mathfrak{b}^{-1}\Lambda}) = E_{(\mathfrak{a}\mathfrak{b})^{-1}\Lambda}$$

e.g so that the group action axioms are satisfied. This action is simply transitive, which will imply that $|\mathrm{Cl}(K)| = |\mathcal{ELL}(\mathcal{O}_K)|$. To see this, given E_{Λ_1} and E_{Λ_2}, we need to find (precisely one) $\mathfrak{a}$ such that $\mathfrak{a}E_{\Lambda_1} = E_{\Lambda_2}$. Pick λ_1, λ_2 nonzero in Λ_1 and Λ_2 respectively, and set $\mathfrak{a}_i = \frac{1}{\lambda_i}\Lambda_i$ which are clearly fractional ideals. Then

$$\frac{\lambda_2}{\lambda_1}\mathfrak{a}_2\mathfrak{a}_1^{-1}\Lambda_1 = \Lambda_2$$

so, setting $\mathfrak{a} = \frac{\lambda_1}{\lambda_2}\mathfrak{a}_2^{-1}\mathfrak{a}_1$, we have $\mathfrak{a}E_{\Lambda_1} = E_{\Lambda_2}$. To see that this $\mathfrak{a}$ is unique, we want to show that $\mathfrak{a}E_\Lambda = \mathfrak{b}E_\Lambda$ implies $\mathfrak{a} = \mathfrak{b}$, but this is part of what we have already shown above. ■

We will apply this result several times on the road to our main theorem.

Let $E/\mathbb{C}$ be an elliptic curve, $\sigma : \mathbb{C} \to \mathbb{C}$ any field automorphism. Then we may define E^σ as the elliptic curve obtained by allowing σ to act on the coefficients of a Weierstrass equation for E. This construction satisfies the nice property that

$\mathrm{End}(E^\sigma) = \mathrm{End}(E)$ (which is immediate by the fact that σ is an automorphism), which allows us to prove the following:

Proposition 16 *Let $E/\mathbb{C}$ be an elliptic curve with complex multiplication by $\mathcal{O}_K$ where K is an imaginary quadratic number field. Then $j(E) \in \overline{\mathbb{Q}}$.*

Proof: Let $\sigma \in \mathrm{Aut}(\mathbb{C})$. Since E^σ is obtained by the action of σ on the coefficients of an equation for E, and since the j-invariant is a rational function of those coefficients, we have that $j(E^\sigma) = \sigma(j(E))$. However, since E^σ is in $\mathcal{ELL}(\mathcal{O}_K)$, which is finite via the simply transitive action of $\mathrm{Cl}(K)$, $\sigma(j(E))$ takes on only finitely many values as σ ranges over $\mathrm{Aut}(\mathbb{C})$. Therefore, $[\mathbb{Q}(j(E)) : \mathbb{Q}]$ is finite, and $j(E)$ is algebraic. In fact, one can show that $j(E)$ is an algebraic integer, not just an algebraic number, but this is just beyond the scope of our discussion. ■

From the above arguments, we can easily see that there is a natural $\mathrm{Gal}(\overline{K}/K)$ action on $\mathcal{ELL}(\mathcal{O}_K)$ where $\sigma \cdot E = E^\sigma$. For any such σ, there exists a unique $\mathfrak{a} \in \mathrm{Cl}(K)$ such that $\mathfrak{a} \times E = E^\sigma$ (since the action of $\mathrm{Cl}(K)$ is simply transitive). This gives a well-defined map $F : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Cl}(K)$ characterized by $E^\sigma = F(\sigma) \times E$ for all σ; this map will be crucial in understanding the field $K(j(E))$.

Proposition 17 *F is a homomorphism.*

Proof: Given $\sigma, \tau \in \mathrm{Gal}(\overline{K}/K)$, for any elliptic curve $E/\mathbb{C}$ we have that

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

Since we only obtained $F(\sigma)$, $F(\tau)$ by fixing E, we now must show that this definition is independent of E; let $E_1, E_2 \in \mathcal{ELL}(\mathcal{O}_K)$, and write $E_1^\sigma = \mathfrak{a}_1 E_1$, $E_2^\sigma = \mathfrak{a}_2 E_2$. We want to show that $\mathfrak{a}_1 = \mathfrak{a}_2$; to that end, by the transitivity of $\mathrm{Cl}(K) \curvearrowright \mathcal{ELL}(\mathcal{O}_K)$, there exists $\mathfrak{b}$ such that $E_2 = \mathfrak{b} \times E_1$. Then

$$(\mathfrak{b} \times E_1)^\sigma = E_2^\sigma = \mathfrak{a}_2 \times E_2 = \mathfrak{a}_2 \times (\mathfrak{b} \times (\mathfrak{a}_1^{-1} \times E_1^\sigma)) = \mathfrak{a}_2 \mathfrak{b} \mathfrak{a}_1^{-1} \times E_1^\sigma$$

Then, assuming that $(b \times E_1)^\sigma = \mathfrak{b} \times E_1^\sigma$ (the proof of which we omit), we have that $E_1^\sigma = \mathfrak{a}_2 \mathfrak{a}_1^{-1} E_1^\sigma$; again by simple transitivity, this implies that $\mathfrak{a}_1 = \mathfrak{a}_2$ as desired. ■

That F is a homomorphism will be crucial in establishing a canonical isomorphism between $\mathrm{Gal}(H/K)$ and $\mathrm{Cl}(K)$. The last ingredient we need for our main theorem is the following technical lemma, the proof of which we will omit:

Lemma 18 *There is a finite set of primes $S \subset \mathbb{Z}$ such that for primes $p \notin S$ which split in K, say, as $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$, then $F(\sigma_\mathfrak{p}) = \mathfrak{p} \in \mathrm{Cl}(K)$ (e.g $F(\sigma_\mathfrak{p}) = \mathfrak{p}$ for some prime $\mathfrak{p}$ above p).*

We are, at last, ready to prove the main theorem:

Proof: The homomorphism $F : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Cl}(K)$ produces a field extension L/K where L is the fixed field of $\ker F$. Then $\mathrm{Gal}(\overline{K}/L) = \ker F$ consists of $\sigma \in \mathrm{Gal}(\overline{K}/K)$ s.t $F(\sigma) = 1$, e.g, $F(\sigma) \times E = E$ for any (or all) $E \in \mathcal{ELL}(\mathcal{O}_K)$ (by simple transitivity). Reformulating (by the definition of F), this is the set of all σ with $E^\sigma = E$. Since the j-invariant is a complete invariant for elliptic curves, this condition may be replaced with $j(E^\sigma) = j(E)$, and, finally, by a previous result, we know that $j(E^\sigma) = \sigma(j(E))$, so

$$\mathrm{Gal}(\overline{K}/L) = \{\sigma \in \mathrm{Gal}(\overline{K}/K : \sigma(j(E)) = j(E)\} = \mathrm{Gal}(\overline{K}/K(j(E)))$$

where the final equality is obvious.

Therefore, $L = K(j(E))$ by the Galois correspondence. Moreover, since F restricted to $\mathrm{Gal}(L/K)$ is an embedding into $\mathrm{Cl}(K)$, an abelian group, we may continue that L/K is an abelian extension. Let $\mathfrak{c}_{L/K}$ be the conductor of L/K, and consider the following chain:

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

We claim that this composition is the natural projection $I(\mathfrak{c}_{L/K}) \twoheadrightarrow \mathrm{Cl}(\mathcal{O}_K)$ sending an ideal to its class, e.g, $F((\mathfrak{a}, L/K)) = \mathfrak{a} \in \mathrm{Cl}(K)$ for all $\mathfrak{a} \in I(\mathfrak{c}_{L/K})$. Let S be the finite set of primes in the above proposition; by the analogue of Dirichlet's theorem we stated above, there exists a degree 1 prime $\mathfrak{p} \in I(\mathfrak{c}_{L/K})$ in the same class as $\mathfrak{a}$ and not lying over a prime in S, e.g, $\mathfrak{a} \equiv 1 \pmod{\mathfrak{c}_{L/K}}$ and $\mathfrak{a} = (\alpha)\mathfrak{p}$ for some $\alpha \in K^*$. Therefore,

$$F((\mathfrak{a}, L/K)) = F(((\alpha)\mathfrak{p}, L/K)) = F((\mathfrak{p}, L/K)) = \mathfrak{p} = \mathfrak{a}$$

where the second equality is just the fact that $\alpha \equiv 1 \pmod{\mathfrak{c}_{L/K}}$ and the third equality is from the above proposition.

Note that this argument implies that $F(((\alpha), L/K)) = 1$ for all $(\alpha) \in I(\mathfrak{c}_{L/K})$; since $F : \mathrm{Gal}(L/K) \to \mathrm{Cl}(K)$ is injective (via the definition of L in terms of $\ker F$), we may conclude that $((\alpha), L/K) = 1$ for all $(\alpha) \in I(\mathfrak{c}_{L/K})$. Since the conductor is defined as the largest integral ideal $\mathfrak{c}$ with the property that

$$\alpha \equiv 1 \pmod{\mathfrak{c}} \implies ((\alpha), L/K) = 1$$

it follows that $\mathfrak{c}_{L/K} = (1)$. Since, by Artin reciprocity, all the primes of K which ramify in L divide $\mathfrak{c}_{L/K}$, we may conclude that L is unramified everywhere. Thus $L \subseteq H$ where H is the Hilbert class field of K. We will show that $L = H$: since the map $I(\mathfrak{c}_{L/K}) = I((1)) \to \mathrm{Cl}(K)$ is vacuously surjective, that $F((\mathfrak{a}, L/K)) = \mathfrak{a}$ implies that $F : \mathrm{Gal}(L/K) \to \mathrm{Cl}(K)$ is also surjective, and therefore an isomorphism, so

$$[L : K] = |\mathrm{Gal}(L/K)| = |\mathrm{Cl}(K)| = |\mathrm{Gal}(H/K)| = [H : K]$$

which implies that $L = H$, that is, $K(j(E))$ is the Hilbert class field of K. ■

In terms of using this theorem to calculate class numbers, we can say more:

Proposition 19 $[\mathbb{Q}(j(E)) : \mathbb{Q}] = h_K$

Proof: Note that $[\mathbb{Q}(j(E)) : \mathbb{Q}] \leq h_K$ by the argument used to show that $j(E)$ is an algebraic number; the values of E^σ are contained in $\mathcal{ELL}(\mathcal{O}_K)$ which is in bijection with $\mathcal{O}_K$, and these values correspond to the values of $\sigma(j(E))$. Since $[K(j(E)) : K] = h_K$ by the above, and $[K : \mathbb{Q}] = 2$, so $[K(j(E)) : \mathbb{Q}] = 2h_K$; forming this extension differently, we could first take $\mathbb{Q}(j(E))/\mathbb{Q}$ and then adjoin the square root giving K. If $[\mathbb{Q}(j(E)) : \mathbb{Q}] < h_K$, then $[K(j(E)); \mathbb{Q}] < 2h_K$, from which the result follows. ■

Example 20 Consider the elliptic curve E given by the equation

$$y^2 = 4x^3 - ax$$

which all determine the same curve (up to isomorphism) since $j(E) = 1728$. These curves have complex multiplication by $\mathbb{Z}[i]$, since they $\mathbb{Z}/(4)$ automorphisms, generated by $(x, y) \mapsto (-x, iy)$. However, since $j(E) \in \mathbb{Q}$ (in fact $\mathbb{Z}$), we can see that $\mathbb{Q}(i)$ has class number one, and is its own Hilbert class field.

Example 21 (Numerics Taken from [2]) Let $K = \mathbb{Q}(\sqrt{-15})$, $\mathcal{O}_K = \mathbb{Z}[\alpha]$ where $\alpha = \frac{1+\sqrt{-15}}{2}$. One can show that K has class number 2, generated by $(2, \alpha)$, therefore $|\mathcal{ELL}(\mathcal{O}_K)| = 2$, and the two isomorphism classes are conjugate to one another, in the sense that if $j(E_{\mathcal{O}_K}) = A + B\sqrt{5}$, $j(E_{(2,\alpha)}) = A - B\sqrt{5}$ (where we know that the j-invariant lands in $\mathbb{Q}(\sqrt{5})$ by the fact that $H = K(\sqrt{5}, \sqrt{-3})$ and j must land in $\mathbb{R}$ here). Using the q-expansion of the j-invariant, we may calculate

$$j(E_{\mathcal{O}_K}) = j(e^{2\pi i\alpha}) \approx -191657.832863$$

and

$$j(E_{(2,\alpha)}) = j(e^{-\sqrt{15}i\pi/2}) \approx 632.83286254$$

With these two values, we can calculate A and B as above, and find that

$$j(E_{\mathcal{O}_K}) = -52515 - 85995\alpha \in \mathcal{O}_K$$

REFERENCES

[1] Joseph Silverman. *The Arithmetic Of Elliptic Curves.* Springer-Verlag, New York, 2016.

[2] Joseph Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves.* Springer-Verlag, New York, 1994.

[3] James S. Milne. *Modular Functions and Modular Forms (v1.31).* 2017. `www.jmilne.org/math/CourseNotes/mf.html`