A SUMMARY OF THE CM THEORY OF ELLIPTIC CURVES

JAYCE GETZ

1. Introduction: a few modular forms

We first fix some terminology from the classical theory of modular forms over $\Gamma := \mathrm{SL}_2(\mathbb{Z})$. For $k \geq 4$, let

$$E_k(z) := 1 - \frac{B_k}{2k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$$

be the Eisenstein series of weight k. Here B_k is the kth Bernoulli number,

$$\sigma_{k-1}(n) := \sum_{d|n} d^{k-1}$$

and $q := e^{2\pi i z}$. We further define the Δ-, or discriminant function, to be the unique normalized weight 12 cusp form:

$$\Delta(z) := \frac{E_4(z)^3 - E_6(z)^2}{1728} = q \prod_{n=1}^{\infty} (1 - q^n)^{24}.$$

Finally we define the most important modular form for our purposes, namely the weight zero modular function

$$j(z) := \frac{E_4(z)^3}{\Delta(z)} = q^{-1} + 744 + 196884q + 21493760q^2 + \cdots . \tag{1.1}$$

The purpose of this expository paper is to describe some part of the intimate connection between this analytic function, the theory of elliptic curves with complex multiplication, and the algebraic number theory of imaginary quadratic fields. In terms of prerequisites, we will assume some familiarity with the j-function and its connection with the analytic geometry of elliptic curves, some basic constructs from the algebraic geometry of elliptic curves, and a knowledge of the tools of class field theory. We follow the relevant sections of [11] and [12, §II] closely.

2. The endomorphism ring over $\mathbb{C}$

Recall that for an elliptic curve $E/\mathbb{C}$, there exists a lattice $L \subset \mathbb{C}$ such that

$$\begin{array}{rcl} \mathbb{C}/L & \xrightarrow{\sim} & E \\ z \notin L & \mapsto & (\wp(z, L), \wp'(z, L), 1) \\ z \in L & \mapsto & (0:1:0) \end{array} \tag{2.1}$$

is an analytic isomorphism. Here $\wp$ is the classical Weierstrass $\wp$-function. Conversely, given any lattice $L \subset \mathbb{C}$, one can show that there exists an elliptic curve E for which an analytic isomorphism of the form (2.1) holds. Under this correspondence between lattices

Date: May 27, 2004.

and elliptic curves, isomorphism classes of elliptic curves over $\mathbb{C}$ correspond to equivalence classes of lattices, where the equivalence is given by $L \sim L'$ if $L = cL'$ for some $c \in \mathbb{C}^*$. By way of terminology, the map $L' \to L$ given by multiplication by $c \in \mathbb{C}^*$ is called a *homothety*, and two lattices related in such a way are called *homothetic*. Note that we may choose a lattice L_τ with basis $\{\tau, 1\}$ with $\tau \in \mathbb{H}$ in each homothety class. Different bases of L_τ are given by applying elements of Γ to the basis $\{\tau, 1\}$; it follows that we may take $\tau \in \mathfrak{F}$. With this stipulation, the basis $\{\tau, 1\}$ is uniquely determined. We will denote by E_τ the corresponding elliptic curve under the map

$$\mathbb{C}/L_\tau \to E_\tau.$$

We call this map (which is induced by (2.1)) an *analytic representation* of E_τ.

We now wish to make this analytic representation more explicit; additionally, because it will be useful later, we work in a slightly more general context. Let E/K be an elliptic curve over a field K of characteristic not equal to 2 or 3. Up to isomorphism, we can assume that E is given in affine coordinates by

$$E : y^2 = 4x^3 - g_4 x - g_6 \tag{2.2}$$

(see, for example, [7, §III.2]). If we restrict to the case $K = \mathbb{C}$, with the normalizations given above, the map (2.1) just formalizes the parametrization

$$E : (\wp'(z, L))^2 = 4(\wp(z, L))^3 - g_4\wp(z, L) - g_6.$$

that exists for some lattice $L \subset \mathbb{C}$.

We now wish define the j-invariant of E_τ, and show how it relates to $j(\tau)$. First, the *discriminant* $\Delta(E)$ of the elliptic curve E/k is defined as

$$\Delta(E) = (2\pi)^{-12}(g_4^3 - 27g_6^2). \tag{2.3}$$

Remark. It is important to observe that the discriminant function $\Delta(E)$ is *not* equal to the discriminant of the cubic polynomial defining the curve. Since the discriminant of the polynomial defining an elliptic curve E is *not* an isomorphism invariant of E, there are a variety of essentially equivalent ways to define the discriminant; the reason for our particular definition will soon be apparent.

We define the *j-invariant of E* to be the quantity

$$j(E) := \frac{1728 g_4^3}{(2\pi)^{12}\Delta(E)}. \tag{2.4}$$

One can show by elementary means that over any field K of characteristic not equal to 2 or 3 that $j(E)$ is indeed an invariant of the isomorphism class of E, and, further, given any $j(E) \in K$, there exists a curve of j-invariant $j(E)$ (see [7, §III.2]).

Note the similarity of (2.4) and (1.1). This is no accident. Let $\mathbb{C}/L_\tau \to E_\tau$ be an analytic representation. It turns out that, with the normalizations given above, we have $g_2 = \frac{4}{3}\pi^4 E_4(\tau)$, $g_3 = \frac{8}{27}\pi^6 E_6(\tau)$. Hence, we have

$$\Delta(E) = \frac{(E_4(\tau)^3 - E_6(\tau)^2)}{1728} = \Delta(\tau)$$

and

$$j(E_\tau) = j(\tau). \tag{2.5}$$

Thus the coincidence of the "j" in j-function and j-invariant is really no coincidence. Indeed, noting the fact that as the j-invariant varies over K it parameterizes isomorphism classes of elliptic curves over K (at least if we continue to assume that the characteristic of K is not 2 or 3), and recalling that the j-function is a bijection between $\mathfrak{F}$ and $\mathbb{C}$, we have a bijective map

$$\mathfrak{F} \longleftrightarrow \{\text{isomorphism classes of } E/\mathbb{C}\}\,.$$

For proofs of the statements we just made on the equality of the various definitions of j and Δ, see [8, §I and p. 112]. For a basic introduction to the theory of elliptic curves, see [7].

Now that we have (2.1) and the isomorphism invariant $j(E)$ in hand, we completely understand isomorphism classes of elliptic curves over $\mathbb{C}$ considered as analytic objects; they are explicitly parameterized by $\wp(z, L_\tau)$ (considered as a function of $\tau \in \mathfrak{F}$). For example, define $E[N]$*, the* N*-division points of* E, to be the points of E of order dividing N. Viewing $E/\mathbb{C}$ as $\mathbb{C}/L_\tau$, it is evident that $E[N]$ is simply the group $\frac{1}{N}L_\tau/L_\tau$, that is,

$$E[N] \approx \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}.$$

The ring of endomorphisms of E, or $\operatorname{End}(E)$, can also be understood in a relatively straightforward manner using analytic representations. To begin, we have the following:

Lemma 1. *Let* L, M *be two lattices in* $\mathbb{C}$*, and let*

$$\lambda : \mathbb{C}/L \to \mathbb{C}/M$$

be a complex analytic homomorphism. Then there exists a complex number α *so that the following diagram commutes:*

$$\begin{tikzcd} \alpha: & \mathbb{C} \arrow[r] \arrow[d] & \mathbb{C} \arrow[d] \\ \lambda: & \mathbb{C}/L \arrow[r] & \mathbb{C}/M. \end{tikzcd}$$

Here the top map is multiplication by α *and the bottom is the homomorphism* λ*.*

Proof. In a neighborhood of zero, λ can be expressed by a power series

$$\lambda(z) = a_0 + a_1 z + a_2 z^2 + \cdots\,,$$

On the other hand, λ is a homomorphism, so $a_0 = 0$ and additionally we have

$$\lambda(z + z') \equiv \lambda(z) + \lambda(z') \pmod{M}.$$

If we choose a small enough neighborhood U of zero, we must have that this congruence is an equality in U; thus

$$\lambda(z) = a_1 z$$

for $z \in U$. But for any $z \in \mathbb{C}$, z/n is in U for sufficiently large integers n, and from this we conclude that, identifying z with its reduction modulo L,

$$\lambda(z) = \lambda\left(n\left(\frac{z}{n}\right)\right) = n\lambda\left(\frac{z}{n}\right) = na_1\left(\frac{z}{n}\right) = a_1 z.$$

□

Remark. Abusing notation, we will often denote the complex number α and the homomorphism λ by the same symbol λ. We will also usually only be considering the special case $L = M$ of Lemma 1.

So far we have been identifying an elliptic curve with an analytic parametrization, and hence its endomorphism ring with the endomorphism ring of a lattice. The following proposition, in conjunction with Lemma 1, shows that this endomorphism ring is unchanged if we instead think of elliptic curves as objects in a category with isogenies as morphisms:

Proposition 2. *Let E_1, E_2 be elliptic curves analytically parametrized by the lattices L_1, L_2, respectively. Then the natural inclusion*

$$\{\textit{isogenies } \phi : E_1 \longrightarrow E_2\} \longrightarrow \{\textit{holomorphic maps } \phi : \mathbb{C}/L_1 \to \mathbb{C}/L_2 \textit{ with } \phi(0) = 0\}$$

is a bijection.

Proof. First note that an isogeny is given locally by everywhere defined rational functions (i.e. it is a morphism). Hence the map induced on the corresponding complex tori will be holomorphic. Thus the association

$$\mathrm{Hom}(E_1, E_2) \longrightarrow \text{Holom. Map}(\mathbb{C}/L_1, \mathbb{C}/L_2)$$

is well defined, and it is clearly injective.

We now prove injectivity. It suffices to provide an isogeny corresponding to a map λ induced by multiplication by α as in Lemma 1. The induced map on Weierstrauss equations (c.f. (2.2)) is given by

$$\begin{array}{ccc} E_1 & \longrightarrow & E_2 \\ [\wp(z, L_1), \wp'(z, L_1), 1] & \longmapsto & [\wp(\alpha z, L_2), \wp(\alpha z, L_2), 1] \end{array}$$

so we must show that $\wp(\alpha z, L_2)$ and $\wp'(\alpha z, L_2)$ can be expressed as rational functions of $\wp(z, L_1)$ and $\wp'(z, L_2)$. But $\alpha L_1 \subset L_2$, so for any $\omega \in L_1$,

$$\wp(\alpha(z + \omega), L_2) = \wp(\alpha z + \alpha\omega, L_2) = \wp(\alpha z, L_2),$$

and similarly for $\wp'(\alpha z, L_2)$. Thus both $\wp(\alpha z, L_2)$ and $\wp'(\alpha z, L_2)$ are complex analytic elliptic functions with respect to the lattice L_1. By elementary complex analysis, this implies that they can be expressed as rational functions of $\wp(z, L_1)$ and $\wp'(z, L_2)$ (see, for example, [11, §VI.3.2]]). □

Returning to the characterization of the endomorphism ring in Lemma 1, is clear that any $\lambda \in \mathbb{Z}$ will induce an endomorphism of $\mathbb{C}/L_\tau$, which we can then identify with an element of $\mathrm{End}(E_\tau)$. We will call these endomorphisms the *trivial endomorphisms of* E_τ. We have the following:

Definition. *If $E/\mathbb{C}$ is an elliptic curve with nontrivial elements in its endomorphism ring* $\mathrm{End}(E/\mathbb{C})$*, then we say E* ***is a curve with complex multiplication****, or, briefly, E* ***has CM****.*

The complex numbers λ inducing a nontrivial endomorphism of a lattice L turn out to be algebraic numbers; more specifically, they are quadratic over $\mathbb{Q}$. Before we formalize and prove this as a proposition, we offer another definition:

Definition. *Suppose $\tau \in \mathbb{H}$ is the root of a quadratic equation with integer coefficients; that is, $\tau = \frac{-b+\sqrt{b^2-4ac}}{2a}$ with $a, b, c \in \mathbb{Z}$ and $\gcd(a, b, c) = 1$. We say that τ is a* ***Heegner point*** *and that $d_\tau = b^2 - 4ac$ is the* ***discriminant*** *of τ.*

Proposition 3. *Suppose $E/\mathbb{C}$ is an elliptic curve. Then*

(1) *Every nontrivial endomorphism of $E/\mathbb{C}$ is induced (in the sense of Theorem 1) either by a Heegner point $\lambda \in \mathbb{H}$ or by $-\lambda$ for a Heegner point $\lambda \in \mathbb{H}$.*
(2) *The curve $E/\mathbb{C}$ has CM if and only if $j(E) = j(\tau)$ for some Heegner point $\tau \in \mathfrak{F}$.*
(3) *The curve $E/\mathbb{C}$ has CM if and only if* $\mathrm{End}(E) \cong \mathcal{O}$*, where $\mathcal{O}$ is an order in an imaginary quadratic number field K.*

Proof. The endomorphism ring of E is unchanged if we replace it with another elliptic curve isomorphic to it, so we assume without loss of generality that $E = E_\tau$, $\tau \in \mathfrak{F}$. Thus we have an analytic representation

$$\mathbb{C}/L_\tau \to E_\tau.$$

As we proved in Lemma 1, a nontrivial automorphism of E_τ can now be realized as a $\lambda \in \mathbb{C}^* - \mathbb{Z}$ such that

$$\lambda L_\tau \subset L_\tau$$

or, equivalently, for some $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Q}) \cap M_{2\times 2}(\mathbb{Z})$,

$$\begin{aligned} \lambda\tau &= a\tau + b \\ \lambda &= c\tau + d. \end{aligned}$$

This implies that λ is a root of the quadratic equation

$$\begin{vmatrix} x-a & -b \\ -c & x-d \end{vmatrix} = 0.$$

Thus λ is a quadratic irrational algebraic integer. Now note that τ cannot be real; otherwise L_τ would not be a lattice, and $c \neq 0$, for then λ would be an integer. Thus $\mathbb{Q}(\tau) = \mathbb{Q}(\lambda)$, and, further, both λ and τ are imaginary quadratic numbers. This proves (1).

We've also proven the "only if" implication of (2), just by recalling that j is an isomorphism invariant. The other direction follows similarly: note that if $j(E) = j(\tau)$ with τ a Heegner point, then $E_\tau \approx E$, and E_τ is evidently CM.

Finally, for (3), note that if E is CM, as proven above, there is an isomorphic curve E_τ where τ is a Heegner point. Thus $\mathrm{End}(E) \approx \mathrm{End}(L_\tau)$, and, again as proven above, any complex number inducing a nontrivial endomorphism of L_τ is an element of $\mathcal{O}_{\mathbb{Q}(\tau)}$, the ring of integers of $\mathbb{Q}(\tau)$, but not an element of $\mathbb{Z}$. With this observation in mind it is easy to see that the evident map $\mathrm{End}(L_\tau) \to \mathcal{O}_{\mathbb{Q}(\tau)}$ is a homomorphism of rings with identity, and, further, the image of this homomorphism is not contained in $\mathbb{Z} \subset \mathcal{O}_{\mathbb{Q}(\tau)}$. Thus $\mathrm{End}(L_\tau) \approx \mathrm{End}(E_\tau)$ is isomorphic to an order in $\mathcal{O}_{\mathbb{Q}(\tau)}$. Conversely, note that if $\mathrm{End}(E) \approx \mathcal{O}$, with $\mathcal{O}$ an order in a quadratic imaginary field, then $\mathrm{End}(E)$ is not isomorphic to $\mathbb{Z}$, so E must be CM. □

By way of terminology, if $\tau \in \mathbb{H}$ is a Heegner point, then $j(\tau) \in \mathbb{C}$ is called a *singular modulus.* In view of parts (3) and (4) of the last proposition, one might guess that these singular moduli would be of interest in the study of the arithmetic of imaginary quadratic number fields. This is indeed the case, but before we can explain anything in any more detail we must explore the connection between the CM elliptic curves and quadratic imaginary fields. We begin this program in the next section. First, however, we describe a normalization on the space of differentials Ω_E of an elliptic curve E that will be of use to us later . We recall for the reader's convenience that for a curve written in Weierstrauss form as in (4.1), a translation-invariant differential is given by

$$\omega := \frac{dx}{2y + a_1x + a_3} \in \Omega_E$$

(for background on Ω_E, see [11, §III.5]). We have the following:

Proposition 4. *Let $E/\mathbb{C}$ be a CM elliptic curve with endomorphism ring R. Then there is an isomorphism*

$$[\cdot] : R \xrightarrow{\sim} \mathrm{End}(E)$$

such that for any invariant differential $\omega \in \Omega_E$ we have

$$[\alpha]^*\omega = \alpha\omega.$$

Proof. Note that an isomorphism of elliptic curves has the effect of multiplying the invariant differential by a constant (see, for example, [11, §II.1, Table 1.2]). Therefore, it suffices to choose a lattice L analytically parametrizing some elliptic curve E_L in the isomorphism class of E, and then prove the proposition for E_L.

Note that the endomorphism ring of E_L is (or is isomorphic to)

$$\{\alpha \in \mathbb{C} : \alpha L \subset L\} = R \subset \mathbb{C}$$

by Proposition 12. More precisely, each $\alpha \in \mathbb{R}$ gives an endomorphism $[\alpha] : E_L \to E_L$ determined by the commutativity of the following diagram:

$$\begin{tikzcd}
\mathbb{C}/L \arrow[r, "\phi_\alpha"] \arrow[d, "f"] & \mathbb{C}/L \arrow[d, "f"] \\
E_L \arrow[r, "{[\alpha]}"'] & E_L
\end{tikzcd}.$$

Here ϕ_α is the map induced by $z \longmapsto \alpha z$ (c.f. Proposition 1) and f is an analytic parametrization. We claim that this map $[\cdot] : R \xrightarrow{\sim} \mathrm{End}(E)$ satisfies $[\alpha]^*\omega = \alpha\omega$.

First note that any two nonzero invariant differentials on E_L are scalar multiples of eachother. This follows trivially from the fact that their quotient would be a translation invariant function, and hence would be constant. So if we take any invariant differential $\omega \in \Omega_E$ and pull back via the isomorphism $f : \mathbb{C}/L \to E_L$, we obtain a multiple of the invariant differential dz on $\mathbb{C}/L$, say

$$f^*\omega = cdz.$$

Now using the commutative diagram yields

$$[\alpha]^*\omega = (f^{-1})^* \circ \phi_\alpha^* \circ f^*(\omega) = (f^{-1})^* \circ \phi_\alpha^*(cdz) = (f^{-1})^*(c\alpha dz) = \alpha\omega.$$

□

Corollary 5. *Let $(E_1, [\cdot]_{E_1})$ and $(E_2, [\cdot]_{E_2})$ be normalized elliptic curves with CM, and that both endomorphism rings are isomorphic to an order R in a quadratic imaginary field. Morever let $\phi : E_1 \to E_2$ be an isogeny. Then, for all $\alpha \in R$,*

$$\phi \circ [\alpha]_{E_1} = [\alpha]_{E_2} \circ \phi.$$

Proof. Let $0 \neq \omega \in \Omega_{E_2}$ be an invariant differential. Then

$$\begin{aligned}
(\phi \circ [\alpha]_{E_1})^*\omega &= [\alpha]_{E_1}^*(\phi^*\omega) \\
&= \alpha\phi^*\omega \text{ since } \phi^*\omega \text{ is an invariant differential on } E_1 \\
&= \phi^*\alpha\omega \\
&= \phi^*([\alpha]_{E_2}^*\omega \\
&= ([\alpha]_{E_2} \circ \phi)^*\omega.
\end{aligned}$$

Since we are working over $\mathbb{C}$, the map

$$\begin{array}{rcl} \mathrm{Hom}(E_1, E_2) & \longrightarrow & \mathrm{Hom}(\Omega_{E_1}, \Omega_{E_2}) \\ \phi & \longmapsto & \phi^* \end{array}$$

is injective. This follows, for instance, from the fact that every element of $\mathrm{Hom}(E_1, E_2)$ is induced by multiplication by a complex number by Lemma 1 and Proposition 2 when we view E_1, E_2 as $\mathbb{C}/L_1$ and $\mathbb{C}/L_2$ for two lattices $L_1, L_2 \subset \mathbb{C}$. Then the Ω_{E_i} can be thought of as the dual of the tangent space of $\mathbb{C}/L_i$ at the origin, which can be identified with $\mathbb{C}$. It is then straightforward to see that multiplication by $\lambda \in \mathbb{C}$ as an isogeny from $\mathbb{C}/L_1$ to $\mathbb{C}/L_2$ induces multiplication by λ as an element of $\mathrm{Hom}(\Omega_{E_1}, \Omega_{E_2})$. For an alternate proof, see [11, §II.4.2c].

In any case, injectivity implies that $\phi \circ [\alpha]_{E_1} = [\alpha]_{E_2} \circ \phi$. □

3. Class and Galois groups associated to imaginary quadratic fields

We've seen in Proposition 3 that every CM elliptic curve has endomorphism ring isomorphic to an order in a quadratic number field. We now work in an opposite direction. Fix an imaginary quadratic number field K, and let $\mathcal{O}_K$ be its ring of integers. We wish to study the following sets:

$$\begin{aligned} \mathcal{ELL}(\mathcal{O}_K) : &= \frac{\{\text{elliptic curves } E/\mathbb{C} \text{ with } \mathrm{End}(E) \cong \mathcal{O}_K\}}{\text{isomorphism over } \mathbb{C}} \\ &\cong \frac{\{\text{lattices } L \text{ with } \mathrm{End}(L) \cong \mathcal{O}_K\}}{\text{homothety}}. \end{aligned} \tag{3.1}$$

We now show that these sets are nonempty for any imaginary quadratic number field K. Fix an embedding $K \hookrightarrow \mathbb{C}$. Given any nonzero fractional ideal $\mathfrak{a} \subset K$, we know from elementary algebraic number theory that the image of $\mathfrak{a}$ under our chosen embedding (which we will also denote by $\mathfrak{a}$) is a lattice in $\mathbb{C}$. Denote by $E_{\mathfrak{a}}$ the elliptic curve associated to this lattice. We have

$$\begin{aligned} \mathrm{End}(E_{\mathfrak{a}}) &\cong \{\alpha \in \mathbb{C} : \alpha\mathfrak{a} \subset \mathfrak{a}\} \\ &= \{\alpha \in K : \alpha\mathfrak{a} \subset \mathfrak{a}\} \text{ since } \mathfrak{a} \subset K, \\ &= \mathcal{O}_K \text{ since } \mathfrak{a} \text{ is a fractional ideal.} \end{aligned}$$

Thus given $\mathcal{O}_K$, we can find an elliptic curve E with $\mathrm{End}(E) \approx \mathcal{O}_K$. Further, since homothetic lattices give rise to isomorphic elliptic curves, if $c \in K$, then $E_{(c)\mathfrak{a}} \approx E_{\mathfrak{a}}$. In other words, multiplying a fractional ideal by a principal ideal in $\mathcal{O}_K$ does not change the elliptic curve that arises from that ideal. In particular, if we denote by $\mathcal{CL}(K)$ the ideal class group of K, that is,

$$\mathcal{CL}(K) := \frac{\{\text{nonzero fractional ideals of } K\}}{\{\text{nonzero principal ideals of } K\}}.$$

then we have a map

$$\begin{array}{rcl} \mathcal{CL}(K) & \longrightarrow & \mathcal{ELL}(\mathcal{O}_K) \\ \overline{\mathfrak{a}} & \longmapsto & E_{\mathfrak{a}} \end{array}$$

where $\overline{\mathfrak{a}}$ is the ideal class of $\mathfrak{a} \in \mathcal{CL}(k)$. More generally, if L is any lattice and $\mathfrak{a}$ any nonzero fractional ideal of K, then define the product

$$\mathfrak{a}L := \{\alpha_1\lambda_1 + \cdots + \alpha_r\lambda_r : \alpha_i \in \mathfrak{a}, \lambda_i \in L\}.$$

Now let L be a lattice with $E_L \in \mathcal{ELL}(\mathcal{O}_K)$ its associated elliptic curve. We define

$$\overline{\mathfrak{a}} * E_L := E_{\mathfrak{a}^{-1}L} \tag{3.2}$$

The content of the following proposition is that (3.2) induces an action:

Proposition 6. *Let L be a lattice with $E_L \in \mathcal{ELL}(\mathcal{O}_k)$, and let $\mathfrak{a}$ and $\mathfrak{b}$ be non-zero fractional ideals of K. We have*

1. *$\mathfrak{a}L$ is a lattice in $\mathbb{C}$,*
2. *The elliptic curve $E_{\mathfrak{a}L}$ satisfies $\mathrm{End}(E_{\mathfrak{a}L}) \cong R_K$, and*
3. *$E_{\mathfrak{a}L} \cong E_{\mathfrak{b}L}$ if and only if $\overline{a} = \overline{b}$ in $\mathcal{CL}(\mathcal{O}_K)$.*

Hence we have a well defined action

$$\begin{array}{rcl} \mathcal{CL}(k) & \longrightarrow & \mathcal{ELL}(\mathcal{O}_K) \\ \overline{\mathfrak{a}} & \longmapsto & \overline{\mathfrak{a}} * E_L := E_{\mathfrak{a}^{-1}L}. \end{array} \tag{3.3}$$

Further, this action is simply transitive.

Proof. (1) By assumption, $\mathrm{End}(E_L) = \mathcal{O}_K$, so $\mathcal{O}_K L = L$. Choose a nonzero integer $d \in \mathbb{Z}$ so that $d\mathfrak{a} \subset \mathcal{O}_K$. Then $\mathfrak{a}L \subset \frac{1}{d}L$, so $\mathfrak{a}L$ is a discrete subgroup of $\mathbb{C}$. Similarly, choosing a nonzero integer d so that $d\mathcal{O}_k \subset \mathfrak{a}$, we find that $dL \subset \mathfrak{a}L$, so $\mathfrak{a}L$ also spans $\mathbb{C}$.

(2) For any $\alpha \in \mathbb{C}$ and any fractional ideal $\mathfrak{a} \neq 0$, we have that

$$\alpha\mathfrak{a}L \subset \mathfrak{a}L \iff \mathfrak{a}^{-1}\alpha\mathfrak{a}L \subset \mathfrak{a}^{-1}\mathfrak{a}L \iff \alpha L \subset L.$$

Hence

$$\mathrm{End}(E_{\mathfrak{a}L}) = \{\alpha \in \mathbb{C} : \alpha\mathfrak{a}L \subset \mathfrak{a}L\} = \{\alpha \in \mathbb{C} : \alpha L \subset L\} = \mathrm{End}(E_L) = \mathcal{O}_K.$$

(3) Recall that, as we discussed in §2, the isomorphism class of E_L is determined by the homothety class of L and the homothety class of L is determined by the ismorphism class of E_L. Thus

$$E_{\mathfrak{a}L} \cong E_{\mathfrak{b}L} \iff \mathfrak{a}L = c\mathfrak{b}L,$$

or, rewriting,

$$E_{\mathfrak{a}L} \cong E_{\mathfrak{b}L} \iff L = c\mathfrak{a}^{-1}\mathfrak{b}L \iff L = c^{-1}\mathfrak{a}\mathfrak{b}^{-1}L.$$

Hence if $E_{\mathfrak{a}L} \cong E_{\mathfrak{b}L}$, then both $c\mathfrak{a}^{-1}\mathfrak{b}$ and $c^{-1}\mathfrak{a}\mathfrak{b}^{-1}$ take L to itself. This implies, in particular, that they are both equal to $\mathcal{O}_K$. Thus

$$\mathfrak{a} = c\mathfrak{b}$$

which implies $c \in K$ and $\overline{a} = \overline{b}$. This provides the "only if" direction; the other direction is obvious.

To prove that (3.3) induces an action given what we have just proven, observe

$$\overline{a} * (\overline{b} * E_L) = \mathfrak{a} * E_{\mathfrak{b}^{-1}L} = E_{\mathfrak{a}^{-1}(\mathfrak{b}^{-1}L)} = E_{(\mathfrak{a}\mathfrak{b})^{-1}L} = (\overline{\mathfrak{a}}\overline{\mathfrak{b}}) * E_L.$$

That this action is simple (i.e. faithful) follows immediately from (2). To finish the proof of the proposition, we must show that it is transitive. Let $E_{L_1}, E_{L_2} \in \mathcal{ELL}(\mathcal{O}_K)$. We must find a nonzero fractional ideal $\mathfrak{a}$ with the property that $\mathfrak{a}_1 = \frac{1}{\lambda_1}L_1$. Choose any nonzero element $\lambda_1 \in L_1$, and consider the lattice $\mathfrak{a}_1 = \frac{1}{\lambda_1}L_1$. As we noted in the proof of Proposition 3, L_1 is equivalent under the action of Γ to a lattice with basis $\{1, \tau\}$, $\tau \in K$. It follows that $\mathfrak{a}_1 \subset K$, and, by assumption, it is a finitely generated $\mathcal{O}_K$ module. Thus it is a fractional ideal of K.

Similarly, choosing a non-zero $\lambda_2 \in L_2$, we obtain a second fractional ideal $\mathfrak{a}_2 = \frac{1}{\lambda_2} L_2$ of K. We have

$$\frac{\lambda_2}{\lambda_1} \mathfrak{a}_2 \mathfrak{a}_1^{-1} L_1 = L_2.$$

Thus, letting $\mathfrak{a} = \mathfrak{a}_2^{-1}\mathfrak{a}_1$, then we have

$$\overline{\mathfrak{a}} * E_{L_1} = E_{\mathfrak{a}^{-1}L_1} = E_{\frac{\lambda_1}{\lambda_2}L_2} \cong E_{L_2},$$

for homothetic lattices analytically parametrize isomorphic elliptic curves. □

Now that we have an action defined, we look briefly at a particular algebraic object generalizing the groups $E[m]$. Let $\mathfrak{a} \in \mathcal{O}_K$ be an (integral) ideal, and E be an elliptic curve with endomorphism ring isomorphic to $\mathcal{O}_K$. Recalling our normalization in Proposition 4, we define

$$E[\mathfrak{a}] := \{P \in E : [\alpha]P = 0 \text{ for all } \alpha \in \mathfrak{a}\}.$$

We call $E\mathfrak{a}$ the *group of* $\mathfrak{a}$*-torsion points of* E. The following proposition will be of use to us in the proof of Proposition 26 below:

Proposition 7. *Let $E \in \mathcal{ELL}(\mathcal{O}_K)$, and let $\mathfrak{a}$ be an integral ideal of $\mathcal{O}_K$. The following are true:*

1. *The group $E[\mathfrak{a}]$ is the kernel of the natural map $E \longrightarrow \overline{\mathfrak{a}} * E$.*
2. *The group $E[\mathfrak{a}]$ is a free $\mathcal{O}_K/\mathfrak{a}$-module of rank* 1.
3. *Thus the map $E \longrightarrow \overline{a} * E$ has degree $N^K_{\mathbb{Q}}\mathfrak{a}$.*

Proof. Let L be a lattice analytically parametrizing E. We have

$$\begin{aligned} E[\mathfrak{a}] &\cong \{z \in \mathbb{C}/L : \alpha z = 0 \text{ for all } \alpha \in \mathfrak{a}\} \\ &= \{z \in \mathbb{C} : \alpha z \in L \text{ for all } \alpha \in \mathfrak{a}\}/L \\ &= \{z \in \mathbb{C} : z\mathfrak{a} \subset L\}/L \\ &= \mathfrak{a}^{-1}L/L \\ &= \ker\left(\mathbb{C}/L \longrightarrow \mathbb{C}/\mathfrak{a}^{-1}L\right) \text{ here the map is just } z \mapsto z \\ &= \ker\left(E \longrightarrow \overline{\mathfrak{a}} * E\right). \end{aligned}$$

This proves (1).

For (2), keep the same notation as above. Arguing as in the proof of Proposition 3, we may assume that L is spanned by 1 and τ, where $\tau \in K$. In other words, $L \subset K$ is a finitely generated $\mathcal{O}_K$ module, and hence is a factional ideal of K.

From (1), we know that $E[\mathfrak{a}] \cong \mathfrak{a}^{-1}L/L$ as $\mathcal{O}_K/\mathfrak{a}$-modules. Note that if $\mathfrak{q}$ is any integral ideal dividing $\mathfrak{a}$, then the fact that $\mathcal{O}_K L = L$ implies

$$(\mathfrak{a}^{-1}L/L) \otimes_{\mathcal{O}_K} (\mathcal{O}_K/\mathfrak{q}) \cong \mathfrak{a}^{-1}L/(L + \mathfrak{q}\mathfrak{a}^{-1}L) = \mathfrak{a}^{-1}L/\mathfrak{q}\mathfrak{a}^{-1}L.$$

Hence if we use the Chinese Remainder Theorem to write

$$\mathcal{O}_K/A \cong \prod_{\mathfrak{p} \text{ prime}} \mathcal{O}_K/\mathfrak{p}^{e(\mathfrak{p})}$$

then we have

$$E[\mathfrak{a}] \cong \prod_{\mathfrak{p} \text{ prime}} \mathfrak{a}^{-1}L/\mathfrak{p}^{e(\mathfrak{p})}\mathfrak{a}^{-1}L.$$

Thus, it suffices to prove that if $\mathfrak{b}$ is a fractional ideal of $\mathcal{O}_K$ (in particular if $\mathfrak{b} = \mathfrak{a}^{-1}L$) and if $\mathfrak{p}^e$ is a power of a prime ideal, then $\mathfrak{b}/\mathfrak{p}^e$ is a free $\mathcal{O}_k/\mathfrak{p}^e$ module of rank one.

We momentarily write

$$R' := \mathcal{O}_K/\mathfrak{p}^e, \mathfrak{p}' := \mathfrak{p}/\mathfrak{p}^e \text{ and } \mathfrak{b}' := \mathfrak{b}/\mathfrak{p}^e\mathfrak{b}.$$

Note that R' is a local ring with maximal ideal $\mathfrak{p}'$ (indeed, the only ideals in R' are $(0), \mathfrak{p}'^{e-1}, \cdots \mathfrak{p}', (1)$). Consider the quotient

$$\mathfrak{b}'/\mathfrak{p}'\mathfrak{b}' \cong \mathfrak{b}/\mathfrak{p}\mathfrak{b}$$

as a vector space over the field $R'/\mathfrak{p}' \cong \mathcal{O}_K/\mathfrak{p}$. We claim that it is a one-dimensional vector space.

First we observe that any two elements of $\mathfrak{b}$ are $\mathcal{O}_K$-linearly dependent, so the dimension of $\mathfrak{b}/\mathfrak{p}\mathfrak{b}$ over $\mathcal{O}_K/\mathfrak{p}$ is at most one. On the other hand, if the dimension were zero, we would have $\mathfrak{b} = \mathfrak{p}\mathfrak{b}$, which is absurd. Hence the dimension is 1. By Nakayama's lemma (see [1, Proposition 2.8], for example), applied to the local ring R' and the R'-module $\mathfrak{b}'$, it follows that $\mathfrak{b}'$ is a free R'-module of rank one. This completes the proof of (2).

Finally, (3) follows immediately from (1) and (2):

$$\begin{aligned} \deg(E \to \mathfrak{a} * E) &= \#E[\mathfrak{a}] \text{ from (1)} \\ &= N_{\mathbb{Q}}^{K}\mathfrak{a} \text{ from (2).} \end{aligned}$$

□

We now return to the action discussed in Proposition 6. Fix the notation

$$h_K = |\mathcal{CL}(K)|.$$

Then Proposition 6 tells us, in particular, that $|\mathcal{ELL}| = h_K$. We can extract a good deal of additional information from Proposition 6; indeed, it is the basis for the remainder of the results in this paper. We first use it to prove that the singular moduli introduced above are algebraic numbers. In order to do this, we must understand how to translate the action of $\mathcal{CL}(\mathcal{O}_K)$ on $\mathcal{ELL}(\mathcal{O}_K)$ into an action of $\mathrm{Gal}(\overline{K}/K)$ on $\{j(E) : E \in \mathcal{ELL}(\mathcal{O}_K)\}$. We now begin this process.

For $\sigma \in \mathrm{Aut}(\mathbb{C})$, let c^σ denote $\sigma(c)$ for all $c \in \mathbb{C}$, and let E^σ denote the elliptic curve formed by letting σ act on the coefficients of the defining affine equation of E. Further, if $\phi : E \to E$ is an endomorphism of E, then denote by $\phi^\sigma : E^\sigma \to E^\sigma$ the induced endomorphism (i.e. isogeny from E^σ to itself) of E^σ. With this notation fixed, we have the following:

Lemma 8. *Let $E/\mathbb{C}$ be an representative of a class of elliptic curves in $\mathcal{ELL}(\mathcal{O}_K)$ for $\mathcal{O}_K$ the ring of integers of an imaginary quadratic field K. Then $j(E) \in \overline{\mathbb{Q}}$.*

Proof. Let $\sigma : \mathbb{C} \to \mathbb{C}$ be a field automorphism of $\mathbb{C}$. First note that $\mathrm{End}(E^\sigma) \simeq \mathrm{End}(E)$, simply because if $\phi : E \to E$ is any endomorphism of E, then $\phi^\sigma : E^\sigma \to E^\sigma$ is an endomorphism of E^σ. Thus $\mathrm{End}(E^\sigma) \approx \mathrm{End}(E)$. In particular, as σ varies, E^σ varies over only finitely many $\mathbb{C}$-automorphism classes of elliptic curves with endomorphism ring isomorphic to $\mathcal{O}_K$ because the action (3.3) is simply transitive and the class group is finite.

Note that E^σ is obtained from E by letting σ act on the coefficients of the affine equation defining E. The invariant $j(E)$ is just a rational combination of those coefficients, so we have

$$j(E^\sigma) = j(E)^\sigma. \tag{3.4}$$

Since the isomorphism class of an elliptic curve is determined by its j-invariant and there are only finitely many $\mathbb{C}$-isomorphism classes in $\{E^\sigma\}_{\sigma\in\mathrm{Aut}(\mathbb{C})}$, it follows that $j(E)^\sigma$ takes on only finitely many values as σ ranges over $\mathrm{Aut}(\mathbb{C})$. Therefore $[\mathbb{Q}(j(E)):\mathbb{Q}]$ is finite, so $j(E)$ is an algebraic number. This completes the proof. □

The first application of Lemma 8 is the following proposition, which tells us that we may choose a curve defined over $\overline{\mathbb{Q}}$ as a model for a given isomorphism class of CM curves.

Proposition 9. *Let K be a quadratic imaginary field. Then*

$$\mathcal{ELL}(\mathcal{O}_K) \cong \frac{\{\textit{elliptic curves } E/\overline{\mathbb{Q}} \textit{ with } \mathrm{End}(E)\cong\mathcal{O}_K\}}{\textit{isomorphism over } \overline{\mathbb{Q}}}.$$

Proof. For any subfield $\mathbb{F}\subset\mathbb{C}$ denote by

$$\mathcal{ELL}_F(\mathcal{O}_K) := \frac{\{\text{elliptic curves } E/F \text{ with } \mathrm{End}(E)\cong\mathcal{O}_K\}}{\text{isomorphism over } \mathbb{F}}$$

for the purposes of this proof. Fixing an embedding $\overline{\mathbb{Q}}\hookrightarrow\mathbb{C}$, we have a natural map

$$\epsilon : \mathcal{ELL}_{\overline{\mathbb{Q}}}(\mathcal{O}_K) \longrightarrow \mathcal{ELL}_{\mathbb{C}}(\mathcal{O}_K).$$

We need to check that this map is a bijection. Let E/CC represent an element of $\mathcal{ELL}_{\mathbb{C}}(\mathcal{O}_K)$. Then $j(E)\in\overline{\mathbb{Q}}$ by Lemma 8, and hence by the discussion in §2 there exists an elliptic curve $E'/\mathbb{Q}(j(E))$ with $j(E)=j(E')$, that is, $E\cong E'$ over $\mathbb{C}$. Thus ϵ is surjective.

Now let $E_1/\overline{\mathbb{Q}}$ and $E_2/\overline{\mathbb{Q}}$ be elements of $\mathcal{ELL}_{\overline{\mathbb{Q}}}(\mathcal{O}_K)$. If they are isomorphic over $\mathbb{C}$ (i.e. $\epsilon(E_1)=\epsilon(E_2)$), then their j-invariants are the same and are additionally defined over $\overline{\mathbb{Q}}$. Hence they are isomorphic over $\overline{\mathbb{Q}}$ as well. This proves injectivity. □

We can say a good deal more about the algebraic nature of $j(E)$, but in order to prove anything, we must first understand more precisely how to relate the action of $\mathcal{CL}(K)$ on $\mathcal{ELL}(\mathcal{O}_K)$ to the action of $\mathrm{Gal}(\overline{K}/K)$ on the K. The first step in towards this understanding is the first part of the following Theorem, the second part will be useful in §5

Theorem 10. *The following are true.*

(1) *Let $E/\mathbb{C}$ be a CM elliptic curve with endomorphism ring $R\subset\mathbb{C}$. Then*

$$[\alpha]_E^\sigma = [\alpha^\sigma]_{E^\sigma} \textit{ for all } \alpha\in R \textit{ and all } \sigma\in\mathrm{Aut}(\mathbb{C})$$

where the isomorphism $[\cdot]_E : R\xrightarrow{\sim}\mathrm{End}(E)$ and $[\cdot]_{E^\sigma} : R\xrightarrow{\sim}\mathrm{End}(E^\sigma)$ are normalized as in Proposition 4.

(2) *Let E_1/L and E_2/L be elliptic curves defined over a field $L\subset\mathbb{C}$. Then there is a finite extension L'/L such that every isogeny from E_1 to E_2 is defined over L'.*

Proof. For (1), let $\omega\in\Omega_E$ be a non-zero invariant differential on E. Then the normalizations described in Proposition 4 imply that

$$[\alpha]_E^*\omega = \alpha\omega \text{ for all } \alpha\in R.$$

Further, ω^σ is an invariant differential on E^σ (here ω^σ is the differential formed by letting σ act on the complex coefficients defining ω). Thus, again from Proposition 4,

$$[\beta]_{E^\sigma}^*\omega^\sigma = \beta\omega^\sigma \text{ for all } \beta\in R.$$

Now for any $\alpha\in R$ and any $\sigma\in\mathrm{Aut}(\mathbb{C})$ we compute

$$([\alpha]_E^\sigma)^*(\omega^\sigma) = ([\alpha]_E^*\omega)^\sigma = (\alpha\omega)^\sigma = \alpha^\sigma\omega^\sigma = [\alpha^\sigma]_{E^\sigma}^*(\omega^\sigma).$$

In particular, $[\alpha]_{E^\sigma}$ and $[\alpha^\sigma]_{E^\sigma}$ have the same effect on the invariant differential ω^σ.

Note that

$$\begin{aligned} &\text{End}(E^\sigma) &\longrightarrow& \ \text{End}(\Omega_{E^\sigma}) &\quad (3.5)\\ &\psi &\longmapsto& \ \psi^* &\quad (3.6)\end{aligned}$$

is injective by Proposition 4. Thus we have $[\alpha]_E^\sigma = [\alpha^\sigma]_{E^\sigma}$.

Now we prove (2). Take affine equations for E_1 and E_2 with coefficients in L. Let $\phi \in \text{Hom}(E_1, E_2)$ be an isogeny. Then for any $\sigma \in \text{Aut}(\mathbb{C})$ such that σ fixes L, we have $\phi^\sigma \in \text{Hom}(E_1, E_2)$. Note that $\deg \phi^\sigma = \deg \phi$. From [11, Proposition 11, §III.4], any isogeny $\phi \in \text{Hom}(E_1, E_2)$ is determined by its kernel, at least up to automorphisms of E_1, E_2. The curves E_1 and E_2 only have finitely many subgroups of any given order, and their automorphism groups are finite (this is immediate from the analytic parametrization). Therefore the set

$$\{\phi^\sigma : \sigma \in \text{Aut}(\mathbb{C}), \sigma \text{ fixes } L\}$$

is finite, which implies that ϕ is defined over a finite extension of L. Finally, we observe that $\text{Hom}(E_1, E_2)$ is a finitely generated group (see Corollary 7.5, [11, §III.8]), so it suffices to take a field of definition for some finite set of generators. □

Leaving explicit considerations of the endomorphism ring for a moment, we define an action of $\text{Gal}(\overline{K}/K)$ on $\mathcal{ELL}(\mathcal{O}_K)$ in the following manner. Suppose we are given $\sigma \in \text{Gal}(\overline{K}/K)$. Because the action of $\mathcal{CL}(K)$ defined in (3.3) is transitive, there is a representative $\overline{\mathfrak{a}}$ of the unique class in $\mathcal{CL}(K)$, depending on σ, such that $\overline{\mathfrak{a}} * E = E^\sigma$. Thus we have a well defined map

$$F : \text{Gal}(\overline{K}/K) \longrightarrow \mathcal{CL}(K)$$

characterized by the property

$$E^\sigma = F(\sigma) * E \text{ for all } \sigma \in \text{Gal}(\overline{K}/K). \tag{3.7}$$

We can also characterize F in terms of j-invariants. Using the fact that the j-invariant is, well, an invariant of the isomorphism class of a curve (or, equivalently, a lattice), we have

$$j(L)^\sigma = j(F(\sigma)^{-1}L) \tag{3.8}$$

where L is a lattice with $\text{End}(L) \approx \mathcal{O}_K$, as usual. We will show in Proposition 11 that F defines a homomorphism, which isn't that surprising. What is more striking is that the definition of F is independent of the choice of the isomorphism class of E; this will be proven in Proposition 11 as well.

Proposition 11. *Let $K/\mathbb{Q}$ be a quadratic imaginary field. Then there exists a homomorphism*

$$F : \text{Gal}(\overline{K}/K) \longrightarrow \mathcal{CL}(K)$$

characterized by the condition

$$E^\sigma = F(\sigma) * E \textit{ for all } \sigma \in \text{Gal}(\overline{K}/K) \textit{ and } E \in \mathcal{ELL}(\mathcal{O}_K).$$

Proof. We noted in the proof of Lemma 8 that $\text{End}(E^\sigma) \cong \text{End}(E)$ for any $\sigma \in \text{Aut}(\mathbb{C})$. This, combined with the fact that the action of $\mathcal{CL}(K)$ on $\mathcal{ELL}(\mathcal{O}_K)$ is simply transitive, imply that for any $\sigma \in \text{Gal}(\overline{K}/K)$ and any $E \in \mathcal{ELL}(\mathcal{O}_K)$, there is a unique $\overline{a} \in \mathcal{CL}(K)$

with $E^\sigma = \overline{\mathfrak{a}} * E$. Thus for a fixed E as above, we obtain a well defined map F as in the statement of the theorem. To prove that F is a homomorphism, just note that

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

for $\sigma, \tau \in \mathrm{Gal}(\overline{K}/K)$ (note $\mathrm{Gal}(\overline{K}/K)$ acts on the left).

This part was easy; the more involved part is to show that F is independent of the choice of E. Let $E_1, E_2 \in \mathcal{ELL}(\mathcal{O}_K)$, $\sigma \in \mathrm{Gal}(\overline{K}/K)$, and write $E_1^\sigma = \overline{\mathfrak{a}}_1 * E_1$ and $E_2^\sigma = \overline{\mathfrak{a}}_2 * E_2$. We must show that $\overline{\mathfrak{a}}_1 = \overline{\mathfrak{a}}_2$. Since $\mathcal{CL}(K)$ acts transitively on $\mathcal{ELL}(\mathcal{O}_K)$, we can find a $\overline{\mathfrak{b}}$ with $E_2 = \overline{\mathfrak{b}} * E_1$. Then

$$(\overline{\mathfrak{b}} * E_1)^\sigma = E_2^\sigma = \overline{\mathfrak{a}}_2 * E_2 = \overline{\mathfrak{a}}_2 * (\overline{\mathfrak{b}} * E_1) = (\overline{\mathfrak{a}}_2\overline{\mathfrak{b}}\overline{\mathfrak{a}}_1^{-1}) * E_1^\sigma. \tag{3.9}$$

We will prove independently in Proposition 12 below that $(\overline{\mathfrak{b}} * E_1)^\sigma$ is equal to $\overline{\mathfrak{b}}^\sigma * E_1^\sigma$. Noting that $\overline{\mathfrak{b}}^\sigma = \overline{\mathfrak{b}}$ because $\mathfrak{b} \subset K$, we can then cancel $\mathfrak{b}$ from both sides of (3.9) to conclude that $E_1^\sigma = (\overline{\mathfrak{a}}_2\overline{\mathfrak{a}}_1^{-1}) * E_1^\sigma$, which implies by Proposition 6(3) that $\overline{\mathfrak{a}}_1 = \overline{\mathfrak{a}}_2$. This completes the proof of the Proposition, modulo proving Proposition 12, which will be done below. □

We now need to prove

Proposition 12. *Suppose K is a quadratic imaginary field. Let $E/\overline{\mathbb{Q}}$ be an elliptic curve representing an element of $\mathcal{ELL}(\mathcal{O}_K)$, let $\overline{\mathfrak{a}} \in \mathcal{CL}(\mathcal{O}_K)$, and let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Then*

$$(\overline{\mathfrak{a}} * E)^\sigma = \overline{\mathfrak{a}}^\sigma * E^\sigma.$$

This will suffice to prove Proposition 11, since every isomorphism class in $\mathcal{ELL}(\mathcal{O}_K)$ has a representative defined over $\overline{\mathbb{Q}}$ by Proposition 9. Notice that Proposition 12 describes the algebraic action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the analytic object $\mathfrak{a} * E$ (recall $\mathfrak{a} * E := \mathbb{C}/\mathfrak{a}^{-1}L$ for some lattice L analytically parametrizing E). Indeed, the main objective of the proof of Proposition 12 will be to find a suitable algebraic description of $\mathfrak{a} * E$.

Before we begin this proof, however, we must first prove the following lemma from commutative algebra:

Lemma 13. *Let R be a Dedekind domain, $\mathfrak{a}$ a fractional ideal of R, and M a torsion-free R-module. Then the natural map*

$$\begin{array}{rcl} \phi : \mathfrak{a}^{-1}M & \longrightarrow & \mathrm{Hom}_R(\mathfrak{a}, M) \\ x & \longmapsto & \phi_x := (\alpha \mapsto \alpha x) \end{array}$$

is an isomorphism.

Proof of Lemma 13. It is easy to see that the given map is well defined and a monomorphism (because R is a domain). Using the fact that M is a free R-module, we can reduce the proof to the special case of demonstating

$$\begin{array}{rcl} \phi : \mathfrak{a}^{-1} & \longrightarrow & \mathrm{Hom}_R(\mathfrak{a}, R) \\ x & \longmapsto & \phi_x := (\alpha \mapsto \alpha x) \end{array}$$

is surjective. Now given an element $f \in \mathrm{Hom}_R(\mathfrak{a}, R)$ and $a, b \in \mathfrak{a} \subset R$, we clearly have $af(b) = bf(a)$. Thus $f(b) = \frac{b}{a}f(a)$, so $f = \phi_{f(a)/a}$. Further, $\frac{f(a)}{a} \in \mathfrak{a}^{-1}$, because it has the property that for every $b \in \mathfrak{a}$, $b\frac{f(a)}{a} \in R$. □

Proof of Proposition 12. Choose a lattice L so that $E \cong E_L$, and fix a resolution (i.e. an exact sequence)

$$\mathcal{O}_K^m \longrightarrow \mathcal{O}_K^n \longrightarrow \mathfrak{a} \longrightarrow 0.$$

Here the first map is represented by a matrix $A \in M_{m\times N}(\mathcal{O}_K)$. The main idea behind this proof is that we ought to have

$$\mathbb{C}/\mathfrak{a}L \cong \overline{\mathfrak{a}} * E \cong \mathrm{Hom}(\mathfrak{a}, E).$$

Here and throughout this proof, Hom means $\mathcal{O}_K$-module homomorphisms. However, in order to provide this sequence of isomorphisms, we are going to interpret $\mathrm{Hom}(\mathfrak{a}, E)$ not just as an $\mathcal{O}_K$-module, but also as an algebraic variety.

Using our free resolution in conjunction with the short exact sequence

$$O \longrightarrow L \longrightarrow \mathbb{C} \longrightarrow E \longrightarrow 0 \tag{3.10}$$

we obtain the following commutative diagram:

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] \\
0 \arrow[r] & \mathrm{Hom}(\mathfrak{a}, L) \arrow[r] \arrow[d] & \mathrm{Hom}(\mathfrak{a}, \mathbb{C}) \arrow[r] \arrow[d] & \mathrm{Hom}(\mathfrak{a}, E) \arrow[d] \\
0 \arrow[r] & \mathrm{Hom}(\mathcal{O}_K^n, L) \arrow[r] \arrow[d, "A"] & \mathrm{Hom}(\mathcal{O}_K^n, \mathbb{C}) \arrow[r] \arrow[d, "A"] & \mathrm{Hom}(\mathcal{O}_K^n, E) \arrow[d, "A"] \\
0 \arrow[r] & \mathrm{Hom}(\mathcal{O}_K^m, L) \arrow[r] & \mathrm{Hom}(\mathcal{O}_K^m, \mathbb{C}) \arrow[r] & \mathrm{Hom}(\mathcal{O}_K^m, E)
\end{tikzcd}.$$

For any $\mathcal{O}_K$ module M, we have $\mathrm{Hom}(\mathcal{O}_K, M) \cong M^n$, and applying Lemma 13 with $M = L$ and then $M = \mathbb{C}$, we obtain

$$\mathrm{Hom}(\mathfrak{a}, L) = \mathfrak{a}^{-1}L \quad \mathrm{Hom}(\mathfrak{a}, \mathbb{C}) = \mathfrak{a}^{-1}\mathbb{C} = \mathbb{C}$$

Hence we can rewrite the diagram above as

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & \mathfrak{a}^{-1}L \arrow[r] \arrow[d] & \mathbb{C} \arrow[r] \arrow[d] & \mathrm{Hom}(\mathfrak{a}, E) \arrow[d] & \\
0 \arrow[r] & L^n \arrow[r] \arrow[d, "A^t"] & \mathbb{C}^n \arrow[r] \arrow[d, "A^t"] & E^n \arrow[r] \arrow[d, "A^t"] & 0 \\
0 \arrow[r] & L^m \arrow[r] & \mathbb{C}^m \arrow[r] & E^m \arrow[r] & 0
\end{tikzcd}. \tag{3.11}$$

Here A^t is the transpose of the matrix A, and exactness of the bottom two rows follows immediately from (3.10).

An application of the snake lemma to the bottom two rows of (3.11) then yields the exact sequence

$$0 \longrightarrow \mathfrak{a}^{-1}L \longrightarrow \mathbb{C} \longrightarrow \ker(A^t : E^n \to E^m) \longrightarrow L^n/A^tL^m. \tag{3.12}$$

Now, $A^t : E^n \to E^m$ is an algebraic map of algebraic group varieties, since $A^t \in M_{m\times n}(\mathcal{O}_K)$ and $\mathrm{End}(E) = \mathcal{O}_K$. Hence the inverse image of the point $(0, 0, \cdots, 0) \in E^m$ is an algebraic group subvariety of E^n. By Theorem 10, for any $\sigma \in \mathrm{Aut}(\mathbb{C})$, the corresponding map $(E^\sigma)^n \to (E^\sigma)^m$ is obtained by applying σ to the entries of A^t, treated as elements of $\mathcal{O}_K \subset \mathbb{C}$.

If we give every object in (3.12) the topology induced by thinking of the object as a complex Riemann surface, note that it is topologically exact as well. With respect to these topologies, L^n/A^tL^m is discrete and $\mathbb{C}/\mathfrak{a}^{-1}L$ is connected. Hence (3.12) yields

$$(\mathfrak{a} * E)(\mathbb{C}) = \mathbb{C}/A^{-1}L \cong \text{ identity component of } \ker(A^t : E^n \to E^m).$$

The whole point of this business was to give an algebraic characterization of $\mathfrak{a} * E$, which we now have. We can now use this description to finish the proof of the Proposition. For any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we apply this characterization first to E and then to E^σ to deduce that

$$\begin{aligned}(\mathfrak{a} * E)^\sigma &= (\text{identity component of } \ker(A^t : E^n \to E^m))^\sigma \\ &= \text{identity component of } \ker((A^\sigma)^t (E^\sigma)^n \to (E^\sigma)^m) \\ &= \mathfrak{a}^\sigma * E^\sigma.\end{aligned}$$

This concludes the proof of Proposition 12. □

Proposition 11 hints at an intimate connection between the arithmetic of elliptic curves in $\mathcal{ELL}(\mathcal{O}_K)$ and the class field theory of K. One of the most important consequences of this relationship is the following statement:

Theorem 14. *Let E be an elliptic curve representing a class in $\mathcal{ELL}(\mathcal{O}_K)$. Then $K(j(E))$ is the Hilbert class field of K, that is, the maximal unramified abelian extension of K.*

We will prove Theorem 14 in §6; it will require class field theory, which we will assume, and more information from the general algebraic theory of elliptic curves, which we will develop to some extent in the next two sections.

4. Elliptic curves in arbitrary characteristic

In this section we collect some well-known general results on elliptic curves, all of which are proven in various sections of [11]. We begin writing down an explicit, general form for the affine equation defining an elliptic curve. We say that an elliptic curve $(E/K, O)$ (O the origin) is in *Weierstrass form* if its affine equation is given by

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_0 \tag{4.1}$$

with $a_i \in K$ and $0 = [0, 1, 0]$ (see [11, §III.3]). One can show, either by explicit manipulations as in [7, §III.2] or the Riemann-Roch theorem as in [11, Proposition 3.1, §III.3], that every elliptic curve defined over a field K of arbitrary characteristic can be put in Weierstrass form via linear changes of variable. In order to write down the discriminant and j-invariant of an elliptic curve given in Weierstrass form in a palatable form, we define the standard quantities

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= 2a_4 + a_1a_3, \\ b_6 &= a_3^2 + 4a_6, \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \\ c_4 &= b_2^2 - 24b_4, \\ c_6 &= -b_2^3 + 36b_2b_4 - 216b_6. \end{aligned}$$

Then we have

$$\begin{aligned} \mathrm{disc}(E) &= -b^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \\ j &= c_4^3/\mathrm{disc}(E). \end{aligned}$$

With these quantities defined, we note that a curve E has $\mathrm{disc}(E) \neq 0$ if and only if E is nonsingular.

We note that with respect to (4.1), an invariant differential on E/K is given by

$$\omega := \frac{dx}{2y + a_1x + a_3} \in \Omega_E. \tag{4.2}$$

The primary uses (at least in our setting) of differentials are to provide a criterion for separability, and to linearize isogenies. In particular, we have the following two results:

Proposition 15. *Let $\phi : E_1 \to E_2$ be an isogeny. Then ϕ is separable if and only if the map*

$$\phi^* : \Omega_{E_2} \longrightarrow \Omega_{E_1}$$

is injective, or equivalently, nonzero (since both spaces have dimension 1, nonzero).

Proof. See [11, S II.4] for a statement in this language and [3, §16.5] for a proof. □

Theorem 16. *Let E, E' be elliptic curves, ω an invariant differential on E, and let*

$$\phi, \psi : E' \to E$$

be two isogenies. Then

$$(\phi + \psi)^*\omega = \phi^*\omega + \psi^*\omega.$$

Proof. See [11, Theorem 5.2, §III.5]. □

Denote by $[m] : E \to E$ the typical "multiplication-by-m" map. Using Theorem 16 and inducting, we have $[m]^*\omega = m\omega$ for any invariant differential $\omega \in \Omega_E$ and $m \in \mathbb{Z}$. This observation yields the following useful corollary:

Corollary 17. *Let E/K be an elliptic curve, $0 \neq m \in \mathbb{Z}$. Assume that char$(K) = 0$ or that m is prime to char(K). Then the multiplication-by-m map on E is a finite, separable endomorphism.*

Proof. Let ω be an invariant differential on E. Then from our observation above,

$$[m]^*\omega = m\omega \neq 0$$

so $[m] \neq 0$. That the map is finite now follows from the fact that an isogeny is a non-constant map of curves (defined over K). Proposition 15 ensures that it is separable. □

We now leave differentials behind for a moment, and consider divisors. As usual, we denote by $\mathrm{Div}(E)$ the group of divisors of E, $\mathrm{Pic}(E)$ the Picard group of E, and $\mathrm{Div}^0(E)$, $\mathrm{Pic}^0(E)$ the subgroups consisting of degree 0 divisors and classes of degree 0 divisors, respectively. If $K(E)$ denotes the function field of E over K, then we denote by

$$\mathrm{div} : K(E) \longrightarrow \mathrm{Div}(E)$$

the typical homomorphism. One can use the Riemann-Roch theorem to prove that the following sequence is well defined and exact:

$$1 \longrightarrow \overline{K}^* \longrightarrow \overline{K}(E) \overset{\mathrm{div}}{\longrightarrow} \mathrm{Div}^0(E) \longrightarrow \mathrm{Pic}^0(E) \longrightarrow 0. \tag{4.3}$$

For a proof, see [11, §II.3]. Notice, in particular, that this sequence implies that every *effective divisor* (i.e. divisor of the form $\mathrm{div}(f)$ for $f \in \overline{K}(E)$) is of degree zero.

Now let E_1, E_2 be two elliptic curves. From (4.3), we have isomorphisms

$$\begin{array}{rcl} \kappa_i : E_i & \xrightarrow{\sim} & \mathrm{Pic}^0(E_i) \\ P & \longmapsto & \text{class of } (P) - (O) \end{array} \tag{4.4}$$

(compare [11, Proposition 3.4, §III.3]). Thus, given any isogeny $\phi : E_1 \to E_2$, we can define a group homomorphism

$$\begin{tikzcd} E_2 \arrow[r, "\kappa_2"] & \mathrm{Pic}^0(E_2) \arrow[r, "\phi^*"] & \mathrm{Pic}^0(E_1) \arrow[r, "\kappa_1^{-1}"] & E_1. \end{tikzcd}$$

One of the consequences of the following theorem is that this homomorphism is also an isogeny:

Theorem 18. *Let $\phi : E_1 \to E_2$ be a nonconstant isogeny of degree m. Then the following are true.*

(1) *There exists a unique isogeny*

$$\widehat{\phi} : E_2 \longrightarrow E_1$$

satisfying

$$\widehat{\phi} \circ \phi = [m].$$

(2) *As a group isomorphism, $\hat{\phi}$ equals the compositition*

$$\begin{array}{ccccccc} E_2 & \longrightarrow & \mathrm{Div}^0(E_2) & \xrightarrow{\phi^*} & \mathrm{Div}^0(E_1) & \longrightarrow & E_1 \\ Q & \longmapsto & (Q) - (O) & & \sum n_P(P) & \longmapsto & \sum [n_P]P. \end{array}$$

Proof. See [11, Theorem 7.1, §III.6]. □

Definition. *Given a nonconstant isogeny $\phi : E_1 \to E_2$ of degree m, the isogeny $\widehat{\phi} : E_2 \to E_1$ associated to it by Theorem 18 is called the* ***dual isogeny of*** *ϕ. If $\phi = [0]$, we take the convention $\widehat{\phi} = [0]$.*

The following theorem lists some elementary properties of dual isogenies:

Theorem 19. *Let*

$$\phi : E_1 \longrightarrow E_2$$

be an isogeny. Then the follwowing are true.

(1) *Let $m = \deg \phi$. Then*

$$\widehat{\phi} \circ \phi = [m] \text{ on } E_1,$$
$$\phi \circ \widehat{\phi} = [m] \text{ on } E_2.$$

(2) *Let $\lambda : E_2 \to E_3$ be another isogeny. Then*

$$\widehat{\lambda \circ \phi} = \widehat{\lambda} \circ \widehat{\phi}.$$

(3) *Let $\psi : E_1 \to E_2$ be another isogeny. Then*

$$\widehat{\phi + \psi} = \widehat{\phi} + \widehat{\psi}.$$

(4) *For all $m \in \mathbb{Z}$,*

$$\widehat{[m]} = [m] \text{ and } \deg[m] = m^2.$$

(5)
$$\deg \widehat{\phi} = \deg \phi.$$

(6)
$$\widehat{\widehat{\phi}} = \phi.$$

When one hears the word "dual," the first natural question one asks is "with respect to what pairing?" One answer in our particular case is the Weil pairing. In order to define this pairing, we will make use of the following fact (which follows from the proof of (4.3)): a divisor $\sum n_i(P_i) \in \mathrm{Div}(E)$ on an elliptic curve E is effective (i.e. the divisor of a function) if and only if $\sum n_i = 0$ and $\sum [n_i]P_i = 0$.

Let E/K be an elliptic curve over a field of characteristic 0 or prime characteristic p, and $T \in E[m]$ for some $m \geq 2$ prime to p. Then there exists a function $f \in \overline{K}(E)$ (the function field of E over $\overline{K}$) such that
$$\mathrm{div}(f) = m(T) - m(O).$$
Letting $T' \in E$ with $[m]T' = T$ (which is possible given the assumption $p \not\div m$, there is similarly a function $g \in \overline{K}(E)$ satisfying
$$\mathrm{div}(g) = [m]^*(T) - m^*(O) = \sum_{R \in E[m]} (T' + R) - (R).$$
(note that $\#E[m] = m^2$ by Theorem 34 below, and $[m^2]T' = 0$). One verifies easily that $f \circ [m]$ and g^m have the same divisor. Thus, by multiplying f by an element of $\overline{K}^*$ if necessary, we may assume
$$f \circ [m] = g^m.$$
Now suppose $S \in E[M]$ ($S = T$ is allowed). Then, for any point $X \in E$,
$$g(X + S)^m = f([m]X + [m]S) = f([m]X) = g(X)^m.$$
Thus we can define a pairing
$$e_m : E[m] \times E[m] \longrightarrow \mu_m$$
where μ_m is the set of mth roots of unity, by setting
$$e_m(S, T) = g(X + S)/g(X) \tag{4.5}$$
for any point $X \in E$ such that $g(X + S)$ and $g(X)$ are both defined and nonzero. Notice that this is a well-defined pairing; though g is only defined up to an element of $\overline{K}^*$, $e_m(S, T)$ does not depend on this choice. The pairing in (4.5) is called the *Weil e_m-pairing*, and it enjoys the following properties:

Proposition 20. *The Weil e_m-pairing is:*

(1) *Bilinear:*
$$\begin{aligned} e_m(S_1 + S_2, T) &= e_m(S_1, T)e_m(S_2, T) \\ e_m(S, T_1 + T_2) &= e_m(S, T_1)e_m(S, T_2); \end{aligned}$$

(2) *Alternating:*
$$e_m(T, T) = 1; \text{ in particular, } e_m(S, T) = e_m(T, S)^{-1};$$

(3) *Non-degenerate:*
$$\text{If } e_m(S, T) = 1 \text{ for all } S \in E[m], \text{ then } T = O;$$

(4) *Galois invariant: For all $\sigma \in \mathrm{Gal}(\overline{K}/K)$,*

$$e_m(S,T)^\sigma = e_m(S^\sigma, T^\sigma);$$

(5) *Compatible: If $S \in E[mm']$ and $T \in E[m]$, then*

$$e_{mm'}(S,T) = e_m([m']S,T).$$

Proof. See [11, Proposition 8.1, §III.8]. □

Further, if ϕ is an isogeny, ϕ and $\widehat{\phi}$ are adjoints with respect to the e_m-pairing:

Proposition 21. *Let $S \in E_1[m], T \in E_2[m]$, and $\phi : E_1 \to E_2$ be an isogeny. Then*

$$e_m(S, \widehat{\phi}(T)) = e_m(\phi(S), T).$$

Proof. See [11, Proposition 8.2, §III.8]. □

Now, the compatibility property of the e_m-pairing suggests that it might behave well ℓ-adically. This is indeed the case, but in order to take advantage of this fact, we require a few definition. From this point onward, we take the convention that $\ell \in \mathbb{Z}$ is a prime *not* equal to the characteristic of the relevant field K, if $\mathrm{char}(K) > 0$.

Definition. *Let E be an elliptic curve and $\ell \in \mathbb{Z}$ a prime. The (ℓ-adic)* ***Tate module of*** *E is the group*

$$T_\ell(E) := \varprojlim_n E[\ell^n]$$

the inverse limit being taken with respect to the natural maps

$$[\ell] : E[\ell^{n+1}] \longrightarrow E[\ell^n].$$

Definition. *Let K be a number field, and, as before,*

$$\mu_{\ell^n} \subset \overline{K}^*$$

the group of ℓ^nth roots of unity. The ***Tate module of*** *K is the group*

$$T_\ell(\mu) := \varprojlim_n \mu_{\ell^n}$$

taken with respect to the "raising to the ℓth power" maps

$$(\cdot)^\ell : \mu_{\ell^{n+1}} \longrightarrow \mu_{\ell^n}.$$

With this notation in place, we can string the e_{ℓ^n} pairings together into a pairing $e_E : T_\ell(E) \times T_\ell(E) \to T_\ell(\mu)$:

Proposition 22. *There exists a bilinear, alternating, non-degenerate, Galois invariant pairing*

$$e_E : T_\ell(E) \times T_\ell(E) \longrightarrow T_\ell(\mu).$$

Further, if $\phi : E_1 \to E_2$ is an isogeny, then ϕ and its dual isogeny $\widehat{\phi}$ are adjoints with respect to this pairing.

Proof. The only thing that needs to be checked, given the inverse limits defining $T_\ell(E)$ and $T_\ell(\mu)$, is that for all $S, T \in E[\ell^{n+1}]$,

$$e_{\ell^{n+1}}(S,T)^\ell = e_{\ell^n}([\ell]S, [\ell]T).$$

By bilinearity,

$$e_{\ell^{n+1}}(S,T)^\ell = e_{\ell^{n+1}}(S, [\ell]T),$$

and then the desired result follows by compatibility. □

We will again call $e_E : T_\ell(E) \times T_\ell(E) \to T_\ell(\mu)$ the Weil pairing.

The reason we recalled all of this material will be evident in the next section; it will be extremely useful in the proof of Proposition 25.

5. Reduction of elliptic curves

The primary purpose of this section is to prove propositions 25 and 26. Proposition 25 is crucial both in the proof of Proposition 26 and in our discussion of supersingularity in §7. We fix the notations K for a global field (not necessarily complete), ν a finite place of K, $\mathcal{O}_\nu$ its ring of integers, and π a uniformizer for $\mathcal{O}_\nu$ (i.e. the maximal ideal of $\mathcal{O}_\nu$ is $\pi\mathcal{O}_\nu$.

We begin with the following definition:

Definition. *Let E/K be an elliptic curve. A Weierstrass equation for E as in (4.1) is called a* ***minimal (Weierstrass) equation for*** *E at ν if $nu(disc(E))$ is minimized subject to the constraint that $a_i \in \mathcal{O}_\nu$. The value of $\nu(disc(E))$ for the minimal Weierstrass equation is the* ***valuation of the minimal discriminant of*** *E* ***at*** *ν.*

We introduced minimal equations mostly for the purpose of studying the reduciton of E under the canonical map $\mathcal{O}_\nu \to \mathcal{O}_\nu/\pi\mathcal{O}_\nu$. We make the following

Definition. *Let E/K be an elliptic curve, and let $\widetilde{E}$ be the curve defined by reducing the coefficients of a minimal Weierstrass equation for E under the map $\mathcal{O}_\nu \to \mathcal{O}_\nu/\pi\mathcal{O}_\nu$. We say that E has* ***good (or stable) reduction*** *if $\widetilde{E}$ is nonsingular.*

One can check that a curve has good reduction at ν if and only if $\nu(\mathrm{disc}(E)) = 0$. For a proof of this fact, see [11, §VII.5]. For a discussion of minimal Weierstrass equations, see [11, §VII.1].

Now, given an arbitrary prime ideal $\mathfrak{P} \subset K$, we can form a valuation $\nu_{\mathfrak{P}}$ associated to it in the usual way. We say that an elliptic curve E has *good reduction at* $\mathfrak{P}$ if it has good reduction at $\nu_{\mathfrak{P}}$. We recall one propositition and deduce a corollary before we start actually proving things again.

Proposition 23. *Let E/K be an elliptic curve and $m \geq 1$ an integer relatively prime to $char(\mathcal{O}_\nu/\pi OO_\nu)$. Assume K is complete with respect to ν. Then if E has good reduction at ν, the reduction map*

$$E(K)[m] \to \widetilde{E}$$

is injective.

Proof. See [11, Proposition 3.1, §VII.3]. □

Corollary 24. *Let E/K be an elliptic curve and $m \geq 1$ an integer relatively prime to a prime ideal $\mathfrak{P} \subset K$. Then if E has good reduction at ν, the reduction map*

$$E(K)[m] \to \widetilde{E}$$

is injective.

Proof. Apply the Lefschetz principle to Proposition 23. See [11, §VI.6] for details. □

We now actually prove something:

Proposition 25. *Let L be a number field, $\mathfrak{P}$ a maximal ideal of L, E_1/L, E_2/L elliptic curves with good reduction at $\mathfrak{P}$, and $\widetilde{E}_1$, $\widetilde{E}_2$ their reductions modulo $\mathfrak{P}$. Then the natural reduction map*

$$\begin{array}{rcl} \mathrm{Hom}(E_1, E_2) & \longrightarrow & \mathrm{Hom}(\widetilde{E}_1, \widetilde{E}_2) \\ \phi & \longmapsto & \widetilde{\phi} \end{array}$$

is injective. Further, it is degree-preserving:

$$\deg(\phi) = \deg(\widetilde{\phi}).$$

Proof of Proposition 25. First notice that since the degree of a nonzero isogeny is nonzero, the second assertion immediately implies the first. Therefore, we only have to prove that $\deg(\phi) = \deg(\widetilde{\phi})$. Choose a rational prime ℓ relatively prime to $\mathfrak{P}$. We will use the Weil pairing e with respect to ℓ to calculate everything on the Tate modules. For any $x, y \in T_\ell(E_1)$, we have

$$e_{E_1}(x,y)^{\deg(\phi)} = e_{E_1}((\deg(\phi))x, y) = e_{E_1}(\widetilde{\phi}\phi x, y) = e_{E_2}(\phi x, \phi y), \tag{5.1}$$

and a similar calculation on $\widetilde{E_1}$ yields

$$e_{\widetilde{E}_1}(\widetilde{x}, \widetilde{y})^{\deg \widetilde{\phi}} = e_{\widetilde{E}_2}(\widetilde{\phi}\widetilde{x}, \widetilde{\phi}\widetilde{x}) \tag{5.2}$$

Here we use our assumption that ℓ is relatively prime to $\mathfrak{P}$ and E_1, E_2 have good reduction a $\mathfrak{P}$.

Now, notice that if E/L is any elliptic curve with good reduction at $\mathfrak{P}$, then by (24), the canonical reduction map provides an isomorphism $E[\ell^n] \cong \widetilde{E}[\ell^n]$ for all $n \in \mathbb{Z}_{>0}$. It follows that in this scenario $T_\ell(E) \cong T_\ell(\widetilde{E})$, and further

$$\widetilde{e_E(x,y)} = e_{\widetilde{E}}(\widetilde{x}, \widetilde{y}) \text{ for all } x, y \in T_\ell(E). \tag{5.3}$$

We now take $x, y \in T_\ell(E_1)$ and compute

$$\begin{array}{rcl} e_{\widetilde{E}_1}(\widetilde{x}, \widetilde{y})^{\deg(\phi)} & = & \widetilde{e_{E_1}(x,y)}^{\deg(\phi)} \text{ from (5.3)} \\ & = & \widetilde{e_{E_2}(\phi x, \phi y)} \text{ from (5.1)} \\ & = & e_{\widetilde{E}_2}(\widetilde{\phi x}, \widetilde{\phi y}) \text{ from (5.3)} \\ & = & e_{\widetilde{E}_2}(\widetilde{\phi}\widetilde{x}, \widetilde{\phi}\widetilde{y}) \\ & = & e_{\widetilde{E}_2}(\widetilde{x}, \widetilde{y})^{\deg \tilde{\phi}} \text{ from (5.2).} \end{array}$$

This equality holds for all $x, y \in T_\ell(E_1)$, and hence for all $\widetilde{x}, \widetilde{y} \in T_\ell(\widetilde{E}_1)$. Noting that the Weil pairing on $T_\ell(\widetilde{E}_1)$ is non-degenerate, this implies $\deg(\phi) = \deg(\widetilde{\phi})$. □

We now prove the following proposition, which will turn out to be the backbone of the proof of Theorem 14 in §6.

Proposition 26. *There is a finite set of rational primes $S \subset \mathbb{Z}$ such that if $p \notin S$ is a prime which splits in K, say as $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$, then*

$$F(\sigma_{\mathfrak{p}}) = \overline{\mathfrak{p}} \in \mathcal{CL}(K).$$

Proof of Proposition 26. We know that $\mathcal{ELL}(\mathcal{O}_K)$ is finite from Proposition 6 and that every isomorphism class in $\mathcal{ELL}(\mathcal{O}_K)$ is represented by a curve that can be defined over $\overline{\mathbb{Q}}$ by Proposition 9. Thus we can choose a finite extension field N/K and representatives $E_1, \cdots, E_n$ defined over N for the distinct $\overline{K}$ isomorphism classes in $\mathcal{ELL}(\mathcal{O}_K)$. Futher, by Theorem 10(2), we may replace N with a finite extension so that every isogeny between any two of the E_i's is defined over N. We define our finite set S to be the set of rational primes satisfying any one of the following three conditions:

(1) p ramifies in N,
(2) some E_i has bad reduction at some prime of N lying over p, or
(3) p divides either the numerator or the denominator of one of the numbers $N_{\mathbb{Q}}^{L}(j(E_i) - j(E_k))$ for some $i \neq k$.

Notice that condition (3) says that the set of representatives "remains distinct" upon reduction modulo $\mathfrak{P}$. That is, if $p \notin S$ and if $\mathfrak{P}$ is a prime of L dividing p, then $\widetilde{E}_i \not\cong \widetilde{E}_k \pmod{\mathfrak{P}}$, since their j-invariants are not the same modulo $\mathfrak{P}$. Now let $p \notin S$ be a prime which splits as $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$ in K, and $\mathfrak{P}$ be a prime of N lying over $\mathfrak{P}$. Moreover, let E/L a representative of an isomorphism class in $\mathcal{ELL}(\mathcal{O}_K)$ and L be a lattice analytically parametrizing E. Choose an integral ideal $\mathfrak{a} \subset \mathcal{O}_K$ relatively prime to p such that $\mathfrak{a}\mathfrak{P}$ is principal, say

$$\mathfrak{a}\mathfrak{p} = (\alpha).$$

As we proved in Proposition 12, the following diagram of analytic maps can also be viewed as a diagram of isogenies:

$$\begin{tikzcd}
\mathbb{C}/L \arrow[r, "z \mapsto z"] \arrow[d, "\wr"] & \mathbb{C}/\mathfrak{p}^{-1}L \arrow[r, "z \mapsto z"] \arrow[d, "\wr"] & \mathbb{C}/\mathfrak{a}^{-1}\mathfrak{p}^{-1}L \arrow[r, phantom, "="] \arrow[d, "\wr"] & \mathbb{C}/(\alpha^{-1})L \arrow[r, "z \mapsto \alpha z", "\sim"'] & \mathbb{C}/L \arrow[d, "\wr"] \\
E \arrow[r, "\phi"'] & \overline{\mathfrak{p}} * E \arrow[r, "\psi"'] & \overline{a} * \overline{p} * E \arrow[r, phantom, "="] & (\alpha) * E \arrow[r, "\sim", "\lambda"'] & E.
\end{tikzcd}$$

Now choose a Weierstrass equation for E/L which is minimal at $\mathfrak{P}$, and let

$$\omega = \frac{dx}{2y + a_1 + a_2}$$

be the associated invariant differential on E. The pull-back of ω to $\mathbb{C}/L$ is some multiple of dz (since dz spans the one-dimensional space of differentials on $\mathbb{C}/L$). Since the map along the top row of the diagram is just $z \mapsto \alpha z$, we see that dz in turn pulls back to $d(\alpha z) = \alpha dz$. Tracing around the diagram, we have

$$(\lambda \circ \psi \circ \phi)^* \omega = \alpha \omega.$$

As usual, we will use a tilde to denote reduction modulo $\mathfrak{P}$. Since the equation for E/L is minimal at $\mathfrak{P}$ and E/L has good reduction at $\mathfrak{P}$, we obtain an equation for $\widetilde{E}$ by simply reducing the coefficients of the minimal Weierstrass equation modulo $\mathfrak{P}$. Thus the reduced differential

$$\widetilde{\omega} = \frac{dx}{\widetilde{2y + a_1x + a_3}}$$

is a nonzero invariant differential on $\widetilde{E}$. Further, since $(\alpha) = \mathfrak{a}\mathfrak{p}$ and since $\mathfrak{P}$ divides $\mathfrak{p}$, we have

$$(\widetilde{\lambda} \circ \widetilde{\psi} \circ \widetilde{\phi})^*\widetilde{\omega} = (\lambda \circ \widetilde{\psi \circ \phi})^*\omega = \widetilde{\alpha}\widetilde{\omega} = \widetilde{0}.$$

Thus, by Proposition 15,

$$\widetilde{\lambda} \circ \widetilde{\psi} \circ \widetilde{\phi}$$

is inseparable. On the other hand, by Proposition 25, and Proposition 7(3), we have

$$\begin{aligned} \deg \widetilde{\phi} &= \deg \phi = N_{\mathbb{Q}}^{K}\mathfrak{p} = p \\ \deg \widetilde{\psi} &= \deg \psi = N_{\mathbb{Q}}^{K}\mathfrak{a} \\ \deg \widetilde{\lambda} &= \deg \lambda = 1. \end{aligned}$$

Since $N_{\mathbb{Q}}^{K}\mathfrak{a}$ is prime to p by assumption, both $\widetilde{\psi}$ and $\widetilde{\lambda}$ are separable, so we conclude that

$$\widetilde{\phi} : \widetilde{E} \longrightarrow \widetilde{\overline{\mathfrak{p}} * E}$$

must be inseparable. Now, by general facts on morphisms of curves (see [11, II.2.12]), any such map factors as a qth-power Frobenius map followed by a separable map, so the fact that $\widetilde{\phi}$ has degree p and is inseparable implies that $\widetilde{\phi}$ must essentially be the pth-power Frobenius map. More precisely, there is an isomorphism from $\widetilde{E}^(p)$ (the curve formed by raising the coefficients of $\widetilde{E}$ to the pth power) to $\widetilde{\overline{\mathfrak{p}} * E}$ so that the composition

$$\widetilde{E} \longrightarrow \widetilde{E}^{(p)} \widetilde{\longrightarrow} \widetilde{\overline{p} * E}$$

equals $\widetilde{\phi}$. Here the first map is the pth power Frobenius map.

In particular, we have

$$j(\widetilde{\widetilde{p} * E}) = j(\widetilde{E}^{(p)}) = j(\widetilde{E})^p,$$

so

$$j(\widetilde{\mathfrak{p}} * E) \equiv j(E)^p = j(E)^{N_{\mathbb{Q}}^{K}\mathfrak{p}} \equiv j(E)^{\sigma_{\mathfrak{p}}} = j(E^{\sigma_{\mathfrak{p}}}) = j(F(\sigma_{\mathfrak{p}}) * E) \pmod{\mathfrak{P}}.$$

By our choice of the set S, we know that

$$j(E_i) \equiv j(E_k) \pmod{\mathfrak{P}} \text{ if and only if } E_i \cong E_k.$$

Hence $\widetilde{\mathfrak{p}} * E \cong F(\sigma_{\mathfrak{p}}) * E$, and the simplicity of the action of $\mathcal{CL}(K)$ on $\mathcal{ELL}(\mathcal{O}_K)$ then gives the conclusion

$$F(\sigma_{\mathfrak{p}}) = \overline{\mathfrak{p}}.$$

□

We record for use in §7 the following result which we proved in the course of the proof of Proposition 26:

Lemma 27. *Let K be a quadratic imaginary field and E be an elliptic curve with CM, $\mathrm{End}(E) \cong \mathcal{O}_K$. Moreover suppose E is defined over a number field N. If $\mathfrak{p}$ is a prime of K that does not ramify in L, and such that E has good reduction at all primes $\mathfrak{P} \subset L$ lying above $\mathfrak{p}$, the natural map*

$$E \longrightarrow \overline{\mathfrak{p}} * E$$

has degree p, and its reduction

$$\widetilde{E} \longrightarrow \widetilde{\overline{\mathfrak{p}} * E}$$

is purely inseparable (here we reduce modulo one of the primes $\mathfrak{P}$ of N lying above $\mathfrak{p}$).

6. The Hilbert class field

We first fix some notation from class field theory. Let K is a totally imaginary number field (which is the only case we will consider), N/K is a normal extension, and $\mathfrak{P} \subset N$ is a prime ideal lying over a prime ideal $\mathfrak{p} \subset K$ that does not ramify in L. We have a restriction homomorphism

$$\{\sigma \in \mathrm{Gal}(N/K) : \mathfrak{P}^{\sigma} = \mathfrak{P}\} \longrightarrow \mathrm{Gal}\left((\mathcal{O}_N/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})\right).$$

This map is surjective, and the group on the right hand side is generated by the *Frobenius automorphism*

$$x \longmapsto x^{N_{\mathbb{Q}}^{K}\mathfrak{p}}.$$

Here $N_{\mathbb{Q}}^{K}$ is the typical norm from K to $\mathbb{Q}$. If we further assume that N/K is an abelain extension (and recall our previous assumption that $\mathfrak{p}$ does not ramify), then there is a unique element $\sigma_{\mathfrak{p}} \in \mathrm{Gal}(N/K)$ with the property that

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

Everything thus far in this section has been a collection of basic results from algebraic number theory; for proofs see [13, §I.13, §I.14], for example.

Let $\mathfrak{c}$ be an integral ideal of K that is divisible by all primes that ramify in L/K (N.B. it is well known that there are only finitely many such primes) and let $I(\mathfrak{c})$ be the group of all fractional ideals of K which are relatively prime to $\mathfrak{c}$. We fix the notation

$$\begin{array}{rcl} (\cdot, L/K) : I(\mathfrak{c}) & \longrightarrow & \mathrm{Gal}(L/K) \\ \displaystyle\prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}} & \longmapsto & \displaystyle\prod_{\mathfrak{p}} \sigma_{\mathfrak{p}}^{n_{\mathfrak{p}}}. \end{array}$$

for the *Artin map.* Notice that all but finitely many of the $n_{\mathfrak{p}}$ are zero; we are just factoring elements of $I(\mathfrak{c})$ in order to define the map.

To motivate the next few definitions, we recall the following weak form of Artin reciprocity, which we will not prove:

Proposition 28 (Artin Reciprocity)**.** *Let L/K be a finite abelian extension of number fields. Then there exists an integral ideal $\mathfrak{c} \subset \mathcal{O}_K$, divisible by precisely the primes of K that ramify in L, such that*

$$((\alpha), L/K) = 1 \textit{ for all } \alpha \in K^* \textit{ satisfying } \alpha \equiv 1 \pmod{\mathfrak{c}}$$

We define the *conductor* of L/K, denoted by $\mathfrak{c}_{L/K}$, to be the largest ideal for which Proposition 28 is true. We further define

$$P(\mathfrak{c}) = \{(\alpha) : \alpha \in K^*, \alpha \equiv 1 \pmod{\mathfrak{c}}\}$$

We require one final definition before we can state the classical formulation of "Class Field Theory."

Definition. *Let $\mathfrak{c}$ be an integral ideal of K. A* ***ray class field of*** K ***(modulo*** $\mathfrak{c}$***)*** *is a finite abelian extension $K_\mathfrak{c}/K$ with the property that for any finite abelian extension N/K,*

$$\mathfrak{c}_{L/K}|\mathfrak{c} \Longrightarrow L \subset K_\mathfrak{c}.$$

Theorem 29 (Class Field Theory)**.** *Let L/K be a finite abelian extension of number fields, and $\mathfrak{c}$ an integral ideal of K. Then the following are true.*

(1) *The Artin map*
$$(\cdot, L/K) : I(\mathfrak{c}_{L/K}) \longrightarrow \mathrm{Gal}(L/K)$$
is a surjective homomorphism.

(2) *The kernel of the Artin map is $(N_K^L I_L)P(\mathfrak{c}_{L/K})$, where I_L is the group of non-zero fractional ideals of L.*

(3) *There exists a unique ray class field $K_\mathfrak{c}$ of K (modulo $\mathfrak{c}$). The conductor of $K_\mathfrak{c}/K$ divides $\mathfrak{c}$.*

(4) *The ray class field $K_\mathfrak{c}$ is characterized by the property that it is an abelian extension of K and satisfies*
$$\{\textit{primes of } K \textit{ that split completely in } K\} = \{\textit{prime ideals in } P(\mathfrak{c})\}.$$

The primary ray class field we will be considering is the ray class field modulo the unit ideal $\mathfrak{c} = (1)$. This is the maximal abelian extension of K which is unramified at all primes. We call $K_{(1)}$ the *Hilbert class field of* K and denote it by H. Notice that

$$I(\mathfrak{c}_{H/K}) = I((1)) = \{\text{all non-zero fractional ideals of } K\}$$
$$P(\mathfrak{c}_{H/K} = P((1)) = \{\text{all non-zero principal ideals of } K\},$$

so the Artin map induces an isomorphism between the ideal class group of K and the Galois group of the Hilbert class field of K:

$$(\cdot, H/K) : \mathcal{CL}(K) \xrightarrow{\sim} \mathrm{Gal}(H/K).$$

The final fact from class field theory that we will require is the following version of the Cebotarev density theorem (a generalization of Dirichet's theorem on primes in arithmetic progressions):

Theorem 30. *Let K be a number field and $\mathfrak{c}$ an integral ideal of K. Then every ideal class in $I(\mathfrak{c})/P(\mathfrak{c})$ contains infinitely many degree 1 primes of K.*

We are finally ready to start proving some results. Using Proposition 26 from the last section, we prove the following theorem, which contains Theorem 14 as part (1).

Theorem 31. *Let E be a curve representing an isomorphism class in $\mathcal{ELL}(\mathcal{O}_K)$. Then the following are true.*

(1) *The Hilbert class field of K is $H := K(j(E))$.*

(2) *If we denote by $h_K := \#\mathcal{CL}(K) = \#\,\mathrm{Gal}(H/K)$ as before, then $[\mathbb{Q}(j(E)) : \mathbb{Q}] = [K(j(E)) : K] = h_K$.*

(3) *If $E_1, ..., E_{h_K}$ be a complete set of representatives for $\mathcal{ELL}(\mathcal{O}_K)$, then $\{j(E_1), ..., j(E_{h_K})\}$ is the set of $\mathrm{Gal}(\overline{K}/K)$ conjugates for $j(E)$.*

(4) *For any nonzero fractional ideal $\mathfrak{a}$ of K,*
$$j(E)^{(\mathfrak{a}, H/K)} = j(\overline{\mathfrak{a}} * E),$$

in particular, if $\mathfrak{p}$ *is a prime ideal of* K*, then*

$$j(E)^{\sigma_{\mathfrak{p}}} = j(\overline{\mathfrak{p}} * E).$$

Proof. Let L/K be the finite extension corresponding to the homomorphism $F : \mathrm{Gal}(\overline{K}/K) \to \mathcal{CL}(K)$, that is, L is the fixed field of $\ker F$. Then

$$\begin{aligned} \mathrm{Gal}(\overline{K}/L) &= \ker F \\ &= \{\sigma \in \mathrm{Gal}(\overline{K}/K) : F(\sigma) = 1\} \\ &= \{\sigma \in \mathrm{Gal}(\overline{K}/K) : F(\sigma) * E = E\}. \end{aligned}$$

This last equality follows from Proposition 6, which states that the action of $\mathcal{CL}(K)$ on $\mathcal{ELL}(\mathcal{O}_K)$ is simply transitive (here we're thinking of E as an isomorphism class of curves). Continuing, the last set above is equal to

$$\begin{aligned} (\mathrm{Gal}(\overline{K}/L)) &= \{\sigma \in \mathrm{Gal}(\overline{K}/K) : E^{\sigma} = E^{\sigma}\} \\ &= \{\sigma \in \mathrm{Gal}(\overline{K}/K) : j(E^{\sigma}) = j(E)\} \\ &= \{\sigma \in \mathrm{Gal}(\overline{K}/K) : j(E)^{\sigma} = j(E)\} \\ &= \mathrm{Gal}(\overline{K}/K(j(E))). \end{aligned}$$

Thus $K(j(E)) = L$. Because F maps $\mathrm{Gal}(L/K)$ injectively into $\mathcal{CL}(K)$ (by definition of L), we see that $L/K = K(j(E))/K$ is an abelian extension.

Let $\rfloor_{L/K}$ be the conductor of L/K, and consider the composition of the Artin map with F:

$$I(\mathfrak{c}_{L/K}) \xrightarrow{(\cdot, L/K)} \mathrm{Gal}(L/K) \xrightarrow{F} \mathcal{CL}(\mathcal{O}_K).$$

We claim that this map is just the projection $\mathfrak{a} \mapsto \overline{\mathfrak{a}}$, that is,

$$F((\mathfrak{a}, L/K)) = \overline{\mathfrak{a}} \text{ for all } \mathfrak{a} \in I(\mathfrak{c}_{L/K}).$$

To see this, let $\mathfrak{a} \in I(\mathfrak{c}_{L/K})$, and let S be the finite set of primes described in Proposition 26. From Theorem 30, there exists a degree 1 prime $\mathfrak{p} \in I(\mathfrak{c}_{L/K})$ in the same $P(\mathfrak{c}_{L/K})$-ideal class as $\mathfrak{a}$ and not lying over a prime in S. In other words, we have an $\alpha \in K^*$ such that

$$\alpha \equiv 1 \pmod{\mathfrak{c}_{L/K}} \text{ and } \mathfrak{a} = (\alpha)\mathfrak{p}.$$

We compute

$$\begin{aligned} F((\mathfrak{a}, L/K)) &= F((\alpha)\mathfrak{p}, L/K)) \\ &= F((\mathfrak{p}, L/K)) \text{ since } \alpha = 1 \pmod{\mathfrak{c}_{L/K}} \\ &= \overline{\mathfrak{p}} \text{ from Proposition 26} \\ &= \overline{\mathfrak{a}}, \end{aligned}$$

which establishes the claim.

Notice that this implies, in particular, that if $(\alpha) \in I(\mathfrak{c}_{L/K})$ is a principal ideal (not necessarily congruent to 1 (mod $\mathfrak{c}_{L/K}$)), then

$$F(((\alpha), L/K)) = 1. \tag{6.1}$$

The map $F : \mathrm{Gal}(L/K) \to \mathcal{CL}(\mathcal{O}_K)$ is injective (by definition of L), so (6.1) implies that

$$((\alpha), L/K) = 1$$

for all $(\alpha) \in I(\mathfrak{c}_{L/K})$. But the conductor of L/K, by definition, is the largest integral ideal $\mathfrak{c}$ with the property that

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

Thus $\mathfrak{c}_{L/K} = (1)$, which implies L/K is everywhere unramified. Therefore $L \subset H$, the Hilbert class field of K.

Now, clearly the natural canonical quotient map $I(\mathfrak{c}_{L/K}) = I(1) \to \mathcal{CL}(K)$ is surjective, so the claim we proved above implies that the monomorphism $F : \mathrm{Gal}(L/K) \to \mathcal{CL}(K)$ is also surjective, and hence an isomorphism. Therefore,

$$[L : K] = \#\,\mathrm{Gal}(L/K) = \#\mathcal{CL}(K) = \#\,\mathrm{Gal}(H/K) = [H : K],$$

which, along with the inclusion $L \subset H$, implies $H = L$. From above, $L = K(j(E))$, so this completes the proof of (1) and the second equality in (2).

To prove the first equality in (2), note that the proof of Proposition 8 implies that

$$[\mathbb{Q}(j(E)) : \mathbb{Q}] \leq h_K.$$

This inequality, combined with $[K(j(E)) : K] = h_K$ and $[K : \mathbb{Q}] = 2$, implies that $[\mathbb{Q}(j(E)) : \mathbb{Q}] = h_K$. This completes the proof of (2).

We now prove (3). From Proposition 6, we know that $\mathcal{CL}(K)$ acts transitively on the set of j-invariants

$$\mathcal{J} := \{j(E_1), \cdots, j(E_{h_k})\}$$

simply by identifying an ismorphism class in $\mathcal{ELL}(\mathcal{O}_K)$ with the j-invariant of that class. From (3.8), we see that the homomorphism $F : \mathrm{Gal}(\overline{K}/K) \to \mathcal{CL}(K)$ is obtained by identifying the natural action of $\mathrm{Gal}(\overline{K}/K)$ on $\mathcal{J}$ with the action of $\mathcal{CL}(K)$ on $\mathcal{J}$ described above, so $\mathrm{Gal}(\overline{K}/K)$ acts transitively on $\mathcal{J}$. This proves (3).

Finally, the claim proven above gives (4) for all ideals in $I(\mathfrak{c}_{L/K}) = I((1))$, which is the set of all nonzero fractional ideals of K. □

We now wish to restate part (3) of Theorem 31 using the language of Heegner points. Recall that an integer $d \neq 1$ is a *fundamental discriminant* if it is not divisible by the square of any odd prime and satisfies either $d \equiv 1 \pmod 4$ or $d \equiv 8, 12 \pmod{16}$. We prove the following lemma:

Lemma 32. *Let $d < 0$ be a fundamental discriminant, and $K = \mathbb{Q}(\sqrt{d})$. Then there are precisely h_K Heegner points of discriminant d in $\mathfrak{F}$.*

Proof. Notice that if $\tau = \frac{-b+\sqrt{b^2-4ac}}{2a} \in \mathfrak{F}$ with $a, b, c \in \mathbb{Z}$, $\gcd(a, b, c) = 1$, and $b^2 - 4ac = d$, then $ax^2 + bxy + cy^2$ is a primitive positive definite quadratic form of discriminant d. Since d is fundamental, the number of such forms is precisely $|\mathcal{CL}(K)| = h_K$. □

We now have the following corollary of Theorem 31(3):

Corollary 33. *Let $d < 0$ be a fundamental discriminant and $\tau_1, ..., \tau_{h_K}$ be the Heegner points of discriminant d in $\mathfrak{F}$. Then $j(\tau_i) \in \overline{\mathbb{Z}}$ for all i, and $j(\tau_1), ..., j(\tau_{h_K})$ is a complete set of Galois conjugates under the action of Gal$(\overline{K}/K)$.*

Proof. First note that the map

$$\begin{aligned} \mathfrak{F} \quad &\longleftrightarrow \quad \frac{\{\text{lattices } L \subset \mathbb{C}\}}{\text{homothety}} \\ z \quad &\longmapsto \quad [L_z] \end{aligned} \tag{6.2}$$

is a bijection. Suppose $\tau \in \mathfrak{F}$ is a Heegner point of discriminant d. Using (2.5), we have that $j(E_\tau) = j(\tau)$, which implies by part (2) of Proposition 3 that E_τ has endomorphism ring isomorphic to an order in an imaginary quadratic number field. This implies that the same is true of L_τ. By the proof of Proposition 3, we may take this imaginary quadratic number field to be K. In fact, $\mathrm{End}(L_\tau) \cong \mathcal{O}_K$, the full ring of integers. To see this, we observe that $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ if d is odd (resp., $\mathcal{O}_K = \mathbb{Z}[\frac{\sqrt{d}}{2}]$ if d is even), hence one need only check that $\frac{1+\sqrt{d}}{2} \cdot \tau \in L_\tau$ (resp., $\frac{\sqrt{d}}{2} \cdot \tau \in L_\tau$). We omit this calculation.

With this claim in hand, (6.2) yields an injection

$$\begin{aligned} \{\text{Heegner points in } \mathfrak{F} \text{ of discriminant } d\} &\hookrightarrow \frac{\{\text{lattices } L \subset \mathbb{C} \text{ with } \mathrm{End}(L) \cong \mathcal{O}_K\}}{\text{homothety}} \\ \tau &\longmapsto [L_\tau]. \end{aligned} \tag{6.3}$$

The set on the left hand side of (6.3) has cardinality h_K by Lemma 32 as does the set on the right hand side by (3.1) and the fact that the action (3.3) is simply transitive. Thus (6.3) is a bijection.

We now identify the set on the right of (6.3) with (3.1). Applying Theorem 31(3) then yields the corollary. □

7. Supersingularity

After we discussed analytic parametrization in §2, the first algebraic object we discussed for an elliptic curve $E/\mathbb{C}$ was its group of N-torsion points

$$E[N] \approx \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}.$$

This isomorphism was immediate after we realized that $E/\mathbb{C}$ is essentially just a lattice in the complex plane.

If we ask for the description of the $E[N]$ for E an elliptic curve over a field of finite characteristic, providing the answer is a little more subtle. Our goal for this final section is to provide a very brief glimpse of what phenomenon can occur. In particular, we have the following:

Theorem 34. *Let E be an elliptic curve and $m \in \mathbb{Z}$, $m \neq 0$. Then the following are true.*

1. *If $char(K) = 0$ or m is prime to $char(K)$, then*
$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$
2. *If $char(K) = p$, then either*
$$E[p^e] = \{O\} \text{ for all } e \in \mathbb{Z}_{>0}$$
or
$$E[p^e] \cong \mathbb{Z}/p^e\mathbb{Z} \text{ for all } e \in \mathbb{Z}_{>0}.$$

Proof. For (1), we apply Proposition 17 to conclude that $[m]$ is a finite, separable map. Hence, using Theorem 19, we conclude

$$\#E[m] = \deg[m] = m^2.$$

By the same argument, for every integer d dividing m we have

$$\#E[d] = d^2.$$

From the classification theorem for finite abelian groups, we see that we must have

$$E[m] \approx \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

We now prove (2) (compare [11, Corollary 6.4, §III.6]). In this case, $[p^e]$ is no longer a separable morphism. However, any morphism ψ between smooth curves over a field of prime characteristic p be written as a composition $\lambda \circ \rho$, where λ is separable and ρ is purely inseparable (indeed, ρ is the qth power Frobenius map for some pth power q). We thus define $\deg_s \psi = \deg \lambda$. For a general morphism between curves, we have

$$\#\psi^{-1}(P) = \deg_s \psi$$

for all but finitely many points P, but if ψ is an isogeny, this equality is true for all points P. Thus, in particular, if we denote by ϕ the p-th power Frobenius endomorphism, we have

$$\begin{aligned} \#E[p^e] &= \deg_s[p^e] \\ &= (\deg_s(\widehat{\phi} \circ \phi))^e \\ &= (\deg_s \widehat{\phi})^e. \end{aligned}$$

Now, the p-th Frobenius endomorphism has degree p; this combined with Theorem 19 yields

$$\deg \widehat{\phi} = \deg \phi = p.$$

Thus there are two possibilities. If $\widehat{\phi}$ is inseparable, then $\deg_s \widehat{\phi} = 1$, so

$$\#E[p^e] = 1$$

for all e. Otherwise $\widehat{\phi}$ is separable, so $\deg_s \widehat{\phi} = p$ and

$$\#E[p^e] = p^e$$

for all $e > 0$. This implies (since it is an equality for all positive integers e) that

$$E[p^e] = \mathbb{Z}/p^e\mathbb{Z}.$$

□

Thus, if we have a curve $E/\overline{\mathbb{F}}_p$, there are two possibilities for $E[p]$, either it is trivial, or isomorphic to $\mathbb{Z}/p\mathbb{Z}$. In the first case we say that E is *supersingular at p*. Although, given $E/\mathbb{Q}$, it is in general not easy to find primes p at which E is supersingular, a famous theorem of Elkies asserts that there are infinitly many such primes.

Recalling that $j(E)$ is an isomorphism invariant of E, and given the central role that the study of j-invariants plays in CM theory, it should come as no surprise that it enters the discussion here as well. We note first that if $E/\overline{\mathbb{Q}}$ has good reduction at a prime ideal $\mathfrak{P} \subset \mathcal{O}_K$ above $p \geq 5$, then $j(E)$ is p-integral. This follows trivially from the computation of the j-invariant in terms of the discriminant below (4.1), for example. Thus we can make the following:

Definition. *Let K be a number field, and suppose $E/\overline{\mathbb{Q}}$ is supersingular at a prime ideal $\mathfrak{P} \subset \mathcal{O}_K$ above a prime $p \geq 5$. Then the reduction of $j(E)$ in $\overline{\mathbb{F}}_p$ is said to be a* ***supersingular j-invariant*** *over $\overline{\mathbb{F}}_p$.*

Using the dictionary between Heegner points and CM elliptic curves we have developed, we can state the following theorem, which yields a nice method of deciding whether a CM curve is supersingular at a particular prime:

Theorem 35. *Let τ be a Heegner point of discriminant $d_\tau < -4$, (d_τ a fundamental discriminant), and E_τ be an elliptic curve with j-invariant $j(\tau)$. Fix a prime $p \geq 5$, and suppose that p is inert or ramified in $\mathbb{Q}(\sqrt{d_\tau})$. If E_τ has good reduction at $\mathfrak{p}$ for all primes $\mathfrak{p}$ above p in $\mathbb{Q}(j(\tau))$, then $j(\tau)$ reduces to a supersingular j-invariant in $\overline{\mathbb{F}}_p$.*

Remark. There is a converse statement, namely that if p splits completely in $\mathbb{Q}(\sqrt{d_\tau})$ and E_τ has good reduction at $\mathfrak{p}$ for all primes $\mathfrak{p}$ above p in $\mathbb{Q}(j(\tau))$, then E_τ is not supersingular at p. For a proof of this, see [9, §13.4.12].

We now prove Theorem 35:

Proof of Theorem 35. Let $K := \mathbb{Q}(\sqrt{d_\tau})$ and assume, without loss of generality, that E is defined over the finite extension N/K (by Theorem 31 we could take $N = H$, the Hilbert class field of K, for example). Further, let ω be the standard invariant differential for E (written down explicitly after (4.1) and $[\cdot]$ the corresponding normalized isomorphism $\mathcal{O}_K \cong E$ (we know that $\mathrm{End}(E) \cong \mathcal{O}_K$ by the assumption that d_τ is a fundamental discriminant).

Suppose first that p splits completely in K as $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$, $pp \neq \mathfrak{p}'$, and $\mathfrak{P} \subset N$ is a prime above $\mathfrak{p}$. Moreover, choose a positive integer M so that $\mathfrak{p}^m$ and $\mathfrak{p}'^n$ are both principal, say

$$\mathfrak{p}^m = \mu\mathcal{O}_K \text{ and } \mathfrak{p}'^m = \mu'\mathcal{O}_K.$$

Then we have $\mu\mu' = p^m$. Note $\mu \notin \mathfrak{p}$, so we have that $[mu]_E^*\omega = \mu\omega \not\equiv 0 \pmod{\mathfrak{P}}$ by our assumption that E has good reduction at $\mathfrak{P}$. Applying Proposition 15 then implies that $\widetilde{[\mu]} \in \mathrm{End}(\widetilde{E})$ is separable, so, using Proposition 25 and Proposition 7, we have

$$\deg \widetilde{[\mu]} = \deg[\mu] = N_{\mathbb{Q}}^K(\mu) = p^m.$$

On the other hand, because $\widetilde{[\mu]}$ is an isogeny we have

$$\# \ker(\widetilde{[\mu]} : \widetilde{E} \to \widetilde{E}) = \deg_s[\mu] = \deg[\mu] = p^m.$$

Since $p^m = \mu\mu'$, this implies the kernel of the map

$$\widetilde{[p^m]} : \widetilde{E} \longrightarrow \widetilde{E}$$

is nonzero; in other words, $\widetilde{E}$ has a point of order p. □

We end this paper with an explicit example to illustrate Theorem 35:

Example. Consider the elliptic curve $E : y^2 = x^3 + x$. Using the formula given after (4.1), we calculate that the discriminant of this curve is -4 and conclude that it has good reduction at any prime $p \geq 3$. We then calculate that the j-invariant is 1728. It is a standard fact from the theory of modular functions that j maps the arc from $e^{2\pi i/3} = -\frac{1}{2} + \frac{\sqrt{-3}}{2}$ to i along the unit disc $\{z : |z| = 1\}$ bijectively onto the interval $[0, 1728]$; in particular, $j(i) = 1728$. It follows that from Proposition 3 that E has CM with endomorphism ring an order in $K = \mathbb{Q}(i)$.

It is a fact from elementary number theory that a prime $p \geq 5$ splits in K if and only if $p \equiv 1 \pmod 4$. Therefore, by Theorem 35, we should expect that $E : y^2 = x^3 + x$ is supersingular when considered as a curve in $\mathbb{F}_p$ for primes $p \geq 5$ with $p \equiv 3 \pmod 4$. We prove this in an elementary manner by demonstrating that $|E/\mathbb{F}_p| = p + 1$. This implies $E/\mathbb{F}_p$ has no p-torsion, which is one of our definitions of supersingularity.

Let $\left(\frac{\cdot}{\cdot}\right)$ denote the typical Legendre symbol. We have

$$\left(\frac{x^3+x}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{x^2+1}{p}\right).$$

Because $p \equiv 3 \pmod 4$, $\left(\frac{-1}{p}\right) = -1$, so

$$\left(\frac{(-x)^3+(-x)}{p}\right) = \left(\frac{-x}{p}\right)\left(\frac{(-x)^2+1}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{x}{p}\right)\left(\frac{x^2+1}{p}\right) = -\left(\frac{x}{p}\right)\left(\frac{x^2+1}{p}\right).$$

By pairing x and $-x$ for $x \in \mathbb{F}_p^*$, we can conclude that exactly half the $p-1$ elements $x \in \mathbb{F}_p^*$ have the property that x^3+x is a quadratic residue. Each such x yields two solutions to the equation $y^2 = x^3+x$ over $\mathbb{F}_p^*$, corresponding to $\pm y$. Adding in the point $(x,y) = (0,0)$ and the point at infinity, we have $|E/\mathbb{F}_p| = p+1$.

References

[1] M. F. Atiyah and I. G. MacDonald, *Introduction to Commutative Algebra*, Addison-Wesley, Reading, MA, (1969).

[2] M. Deuring, *Teilbarkeitseigenschaften der singulären modulen der elliptischen funktionen und die diskriminante der klassengleichung*, Comm. Math. Helv. **19** (1945), 74-82.

[3] D. Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Springer Verlag, New York, (1995).

[4] F.Q. Gouvêa, *Arithmetic of p-adic modular forms*, Springer Lect. Notes in Math., **1304**, (1985).

[5] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer Verlag, New York, 1991.

[6] M. Kaneko and D. Zagier, *Supersingular j-invariants, hypergeometric series, and Atkin's orthogonal polynomials*, Computational Perspectives on Number Theory (Chicago, IL, 1995), AMS/IP **7** (1998), 97–126.

[7] A. Knapp, *Elliptic Curves*, Mathematical Notes, Princeton University Press, **40** Princeton, New Jersey, 1992.

[8] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Springer-Verlag, New York, 1993.

[9] S. Lang, *Elliptic Functions, 2nd edition*, Springer-Verlag, New York, 1987.

[10] K. Ono, *The Web of Modularity: Arithmetic of the Coefficients of Modular Forms and q-series*, AMS-CBMS Regional Conference Series in Mathematics, **102** (2004) Providence, RI.

[11] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.

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

[13] W. Stein, *A Brief Introduction to Classical and Adelic Algebraic Number Theory*, http://modular.fas.harvard.edu/edu/Spring2004/129/ant/.

4404 South Ave. W, Missoula, MT 59804
E-mail address: getz@fas.harvard.edu