Elliptic Curves with Complex Multiplication

Tom O'Brien

September 10, 2009

Contents

1 Introduction

2 The endomorphism ring of an elliptic curve

Unless stated otherwise, all elliptic curves are defined over a field k of characteristic zero.

2.1 Isogenies

Let E_1 and E_2 be elliptic curves. An *isogeny* from E_1 to E_2 is a morphism (of projective varieties) $\phi\colon E_1 \to E_2$ which satisfies

$$\phi(\mathcal{O}) = \mathcal{O},$$

where $\mathcal{O}$ is the neutral element of E. Any isogeny is automatically a group homomorphism ([Sil86] III, §4, Thm 4.8), and we denote by $Hom(E_1, E_2)$ the group of all isogenies $\phi : E_1 \to E_2$. Any non-zero isogeny is surjective ([Sha94] I, §5.3, Thm 4). Therefore, an isogeny $\phi\colon E_1 \to E_2$ induces an injective homomorphism of function fields $\phi^*\colon \bar{k}(E_2) \to \bar{k}(E_1)$ given by

$$\phi^*(f) = f \circ \phi.$$

The extension $\bar{k}(E_1)/\phi^*\left(\bar{k}(E_2)\right)$ is finite ([Har77] II, Prop 6.8), and we thus define the *degree* of ϕ to be the degree of the field extension. We define the degree of the zero isogeny to be zero. If $\phi_1\colon E_1 \to E_2$ and $\phi_2\colon E_2 \to E_3$ are isogenies of elliptic curves, then $\phi_2 \circ \phi_1$ is an isogeny, and

$$deg(\phi_2 \circ \phi_1) = deg(\phi_2)\, deg(\phi_1), \tag{1}$$

by the tower law for field extensions. We say ϕ is *separable*, *inseparable* or *purely inseparable* according to the extension. In particular, when k is of characteristic zero every isogeny ϕ is separable.

Proposition 2.1.1. *Let E_1 and E_2 be elliptic curves over a field k such that there exists an isogeny $\phi : E_1 \to E_2$. Then $\#\ker\phi$ is finite, and*

$$deg(\phi) = \#\ker\phi.$$

Proof. See ([Sil86] III, Thm. 4.10). □

An *endomorphism* of an elliptic curve E is an isogeny from E to itself. The set of all endomorphisms of E forms a ring $End(E)$ under pointwise addition and composition of morphisms, and is known as the *endomorphism ring* of E.

2.2 Some properties of $End(E)$

We will show that the endomorphism ring of an elliptic curve has a very particular structure. The following example allows us to determine some basic properties.

Example 2.2.1. Let E be an elliptic curve given by the equation

$$y^2 = x^3 + Ax + B.$$

For every rational integer m the *multiplication-by-m* map $[m] : E \to E$ defined by

$$[m]\,P = \begin{cases} \mathcal{O} & m = 0, \\ P + \ldots + P & m > 0, \\ -\left(P + \ldots + P\right) & m < 0, \end{cases}$$

is an endomorphism of E. Its kernel $E[m]$ is the subgroup of E consisting of all points (not just those with co-ordinates in k) whose order divides m. From the definition (and the tower law for field extensions) it follows that $[m] \circ [n] = [mn]$.

The multiplication-by-m maps allow us to study $End(E)$, considered as a $\mathbb{Z}$-module.

Lemma 2.2.1. *For any non-zero integer m, the multiplication-by-m endomorphism is non-constant. In particular, $deg([m]) \geq 1$.*

Proof. See ([Sil86] III Prop 4.2). □

Proposition 2.2.1. *Let E be an elliptic curve over a field k. Then the endomorphism ring $End(E)$ is torsion-free as a $\mathbb{Z}$-module.*

Proof. Let ϕ be an endomorphism of E, and suppose $[m] \circ \phi = [0]$. Then

$$deg([m]) \cdot deg(\phi) = 0,$$

so either $[m] = [0]$, or $deg([m]) \geq 1$ by Lemma 2.2.1 $[m] \neq [0]$, in which case $deg(\phi) = 0$ whence $\phi = [0]$. □

Corollary 2.2.1. *The endomorphism ring $End(E)$ of an elliptic curve E is of characteristic zero, with no zero divisors.*

Proof. Proposition 2.2.1 above shows that $End(E)$ is of characteristic zero, and if ϕ_1 and ϕ_2 are endomorphisms of E such that

$$\phi_1 \circ \phi_2 = [0],$$

then

$$deg(\phi_1) \cdot deg(\phi_2) = 0,$$

whence either $\phi_1 = [0]$ or $\phi_2 = [0]$. □

An elliptic curve whose endomorphism ring is strictly larger than $\mathbb{Z}$ is said to have *complex multiplication*. We will see shortly (Proposition 2.3.1) that $deg([m]) = m^2$. Given that this is true, it is clear that an elliptic curve E has complex multiplication if and only if it possesses an endomorphism ϕ whose degree is a non-square.

Example 2.2.2. Consider the elliptic curve E given by the equation

$$y^2 = x^3 + x.$$

The map $[i] : E \to E$ given by

$$[i]\,(x, y) = (-x, iy)$$

is an endomorphism of E. Note that $[i]^2 = [-1]$, so that $[i] \neq [m]$ for any rational integer m. Thus E has complex multiplication.

Example 2.2.3. Let k be a field of characteristic $q = p^r$, and let E be an elliptic curve over k. We define $E^{(q)}$ to be the curve obtained by raising the coefficients of the Weierstrass equation of E to the q-th power. The *Frobenius morphism* $\phi_q : E \to E^{(q)}$ is given by

$$\phi_q(x, y) = (x^q, y^q).$$

Now, if $k = \mathbb{F}_q$ is a finite field, then k^* is cyclic of order $q - 1$ so that $E^{(q)} = E$, and ϕ_q is actually an endomorphism of E. It is known ([Sil86] II Prop 2.1) that $deg(\phi_q) = q$, so that when q is a non-square (i.e. r is odd), then every elliptic curve defined over k has complex multiplication.

Proposition 2.2.2. *Let E_1 and E_2 be isomorphic elliptic curves. Then $End(E_1)$ is isomorphic to $End(E_2)$.*

Proof. Let $f\colon E_1 \to E_2$ denote the isomorphism, and let ϕ be an endomorphism of E_1. We determine an isomorphism $F\colon End(E_1) \to End(E_2)$ by the following commutative diagram:

$$\begin{array}{ccc} E_1 & \xrightarrow{\phi} & E_1 \\ \Big\downarrow{\scriptstyle f} & & \Big\downarrow{\scriptstyle f} \\ E_2 & \longrightarrow & E_2 \end{array}$$

i.e. $F(\phi) = f \circ \phi \circ f^{-1}$. □

We will see shortly that the endomorphism ring of any elliptic curve with complex multiplication (in characteristic zero) has the structure of an order in an imaginary quadratic field. In the next two sections we develop the technical tools required to prove this result.

2.3 Dual isogenies

Let E_1 and E_2 be elliptic curves. For every non-zero isogeny $\phi\colon E_1 \to E_2$ there exists a unique isogeny $\hat{\phi}\colon E_2 \to E_1$ which satisfies

$$\hat{\phi} \circ \phi = [m]\,, \tag{2}$$

where m is the degree of ϕ (when $\phi = [0]$ we define $\hat{\phi}$ to be $[0]$). We say $\hat{\phi}$ is the *dual isogeny* to ϕ. Note that, for any elliptic curve E, we have $\widehat{[1]} = [1]$. This follows from the definition of the dual isogeny and the ring structure of $End(E)$.

The dual isogeny will be a useful tool in studying the multiplication-by-m maps. Some basic properties are given in the following lemma:

Lemma 2.3.1. *Let $\phi\colon E_1 \to E_2$ be an isogeny of degree d. Then*

(i) $\bar{\phi} \circ \phi = [d]$ *on* E_1, *and* $\phi \circ \bar{\phi} = [d]$ *on* E_2,

(ii) if $\theta\colon E_2 \to E_3$ is another isogeny, then

$$\widehat{\theta \circ \phi} = \hat{\phi} \circ \hat{\theta},$$

(iii) if $\psi\colon E_1 \to E_2$ is another isogeny, then

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

Proof. See ([Sil86] III §6, Thm 6.2). □

Proposition 2.3.1. *Let E be an elliptic curve over a field k, and let m be a non-zero integer. Then*

(i) $\widehat{[m]} = [m]$,

(ii) $deg([m]) = m^2$.

Proof. To prove (i) we proceed by induction. It is obvious that $\widehat{[0]} = [0]$ and $\widehat{[1]} = [1]$. Now let m be an arbitrary integer (for simplicity, suppose m is positive; the proof is hardly changed otherwise). Then

$$\begin{aligned}
\widehat{[m]} &= [\widehat{(m-1)} + 1] \\
&= \widehat{[m-1]} + \widehat{[1]} \quad \text{(by Lemma 2.3.1 (i))} \\
&= [m-1] + [1] \quad \text{(by the inductive hypothesis)} \\
&= [m],
\end{aligned}$$

thus completing the proof of (i).

Now let $d = deg([m])$. Then, by Lemma 2.3.1 (i) we have

$$[d] = [m] \circ \widehat{([m])} = [m] \circ [m] = [m^2],$$

and since $End(E)$ is torsion-free we must have $d = m^2$ as required. □

Corollary 2.3.1. *Let E and m be as above. Then*

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

Proof. We proceed by induction. For $m = 1$ and $m = 2$ the result is clear. So suppose $m > 2$. By Proposition 2.1.1 we have

$$\#E[d] = deg([d]) = d^2,$$

for every integer d dividing m. Now recall that a finite abelian group G of order g is isomorphic to the direct product of its p-primary components G_p, where

$$G_p = \{s \in G : s \text{ has } p\text{-power order}\},$$

for each prime p dividing g. If $G = E[m]$ then its p-primary components are precisely the subgroups $E[p_i^{e_i}]$, where $m = p_1^{e_1} \dots p_r^{e_r}$ is the prime factorisation of m. In particular, each of the $E[p_i^{e_i}]$ is (by the inductive hypothesis) isomorphic to $\mathbb{Z}/p_i^{e_i}\mathbb{Z} \times \mathbb{Z}/p_i^{e_i}\mathbb{Z}$. This completes the proof. □

2.4 The Tate module

Let E be an elliptic curve over a field k of characteristic zero, and let ℓ be a rational prime. For every positive integer n the multiplication-by-ℓ map takes $E[\ell^{n+1}]$ into $E[\ell^n]$. We thus define the *ℓ-adic Tate module of E* to be the projective limit

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

As a $\mathbb{Z}$-module $E[\ell^n]$ is clearly annihilated by ℓ^n, and hence by the ideal $\ell^n\mathbb{Z}$, so that each of the $E[\ell^n]$ has the structure of a $\mathbb{Z}/\ell^n\mathbb{Z}$-module. Then $T_\ell(E)$, being a projective limit of $\mathbb{Z}/\ell^n\mathbb{Z}$-modules, has the structure of a $\mathbb{Z}_\ell$-module. Furthermore, since $E[\ell^n] \cong \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z}$ by Corollary 2.3.1, it follows immediately from the definition that

$$T_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell. \tag{3}$$

Let ϕ be an endomorphism of E. Note that if P is a point in $E[m]$ then

$$\begin{aligned} [m] \circ \phi(P) &= \phi(P) + \ldots + \phi(P) \\ &= \phi([m]P) \quad (\text{since } \phi \text{ is a homomorphism}) \\ &= \phi(\mathcal{O}) \quad (\text{since } P \in E[m]) \\ &= \mathcal{O} \quad (\text{by definition of } \phi) \end{aligned}$$

so that $\phi(E[m]) \subset E[m]$ for all m. In particular, taking $m = \ell^n$ for varying n shows that every endomorphism ϕ of E induces an endomorphism ϕ_ℓ of $T_\ell(E)$, i.e. there is a homomorphism $End(E) \to T_\ell(E)$ given by

$$\phi \to \phi_\ell, \tag{4}$$

and extending (4) to $End(E) \otimes \mathbb{Z}_\ell$ gives the following result.

Lemma 2.4.1. *The homomorphism $End(E) \otimes \mathbb{Z}_\ell \to End(T_\ell(E))$ induced by (4) is injective.*

Proof. See ([Sil86] III Thm. 7.7). □

It follows that $End(E) \otimes \mathbb{Z}_\ell$ has $\mathbb{Z}_\ell$-rank at most 4, since $End(T_\ell(E)) \cong M_2(\mathbb{Z}_\ell)$ by (3).

Proposition 2.4.1. *The endomorphism ring $End(E)$ of an elliptic curve E is a characteristic zero integral domain of at most rank 4 over $\mathbb{Z}$.*

Proof. Only the last statement needs proving. We have

$$rank_{\mathbb{Z}}(End(E)) = rank_{\mathbb{Z}_\ell}(End(E) \otimes \mathbb{Z}_\ell),$$

since if (x_i) is a set of basis elements of $End(E)$ over $\mathbb{Z}$ then $(x_i \otimes 1)$ is a $\mathbb{Z}_\ell$-basis for $End(E) \otimes \mathbb{Z}_\ell$. So $rank_{\mathbb{Z}}(End(E)) \leq 4$ as required. □

2.5 The action of $Gal(\bar{k}/k)$ on $E[m]$

Let E be an elliptic curve defined over some field k. Let $P = (x, y)$ be a point on E and let σ be an element of $Gal(\bar{k}/k)$. We define P^σ to be the point $P^\sigma = (x^\sigma, y^\sigma)$. If P is in $E[m]$ for some m, then

$$[m](P^\sigma) = (f_1(P^\sigma), f_2(P^\sigma))$$

where f_1 and f_2 are the rational functions which define $[m]$. But each f_i can be viewed as a quotient of polynomials in $k[x, y]/(y^2 - (x^3 + Ax + B)$. Then, since A and B are in k, and σ fixes k, we have $f_i^\sigma = f_i$. Hence,

$$[m](P^\sigma) = (f_1^\sigma(P^\sigma), f_2^\sigma(P^\sigma)) = ([m]P)^\sigma = \mathcal{O}^\sigma = \mathcal{O}$$

Lemma 2.5.1. *Let E be an elliptic curve over k. There is a well-defined action of $Gal(\bar{k}/k)$ on $E[m]$, given by*

$$P^\sigma = P, \quad P \in E[m], \sigma \in Gal(\bar{k}/k).$$

Proof. This is clear by the above remarks. □

A consequence of Lemma 2.5.1 is that we have a representation

$$\rho : Gal(\bar{k}/k) \to Aut(E[m]),$$

given by

$$\rho(\sigma)(P) = P^\sigma. \tag{5}$$

Note also, that by Corollary 2.3.1, we have that $Aut(E[m]) \cong GL_2(\mathbb{Z}/m\mathbb{Z})$.

2.6 The structure of $End(E)$ in characteristic zero

We are now in a position to describe the general structure of the endomorphism ring of an elliptic curve.

Theorem 2.6.1. *Let E be an elliptic curve over a field k of characteristic zero. Then either $End(E) \cong \mathbb{Z}$ or $End(E)$ is isomorphic to an order in a quadratic imaginary field.*

Proof. Let $K = End(E) \otimes \mathbb{Q}$. For each $\alpha \in \mathbb{Q}, \phi \in End(E)$ we define an extended dual $\widehat{\alpha \cdot \phi}$ by

$$\widehat{\alpha \cdot \phi} = \alpha \cdot \widehat{\phi},$$

where $\widehat{\phi}$ is the dual isogeny to ϕ. We define functions $N : K \to \mathbb{Q}$ and $T : K \to \mathbb{Q}$ by

$$N\Phi = \Phi \cdot \widehat{\Phi} \quad \text{and} \quad T\Phi = \Phi + \widehat{\Phi}.$$

Note that, by Proposition 2.3.1, the value of $N\Phi$ is the product of a positive rational number and a positive integer, so that $N\Phi$ is a positive rational number. Furthermore, we have

$$N(\Phi - 1) = (\Phi - 1) \cdot \widehat{(\Phi - 1)} = N\Phi - T\Phi + 1,$$

so that

$$T\Phi = 1 + N\Phi - N(\Phi - 1)$$

is indeed rational. It is clear from the definitions that T is $\mathbb{Q}$-linear, and that $T\alpha = 2\alpha$ for α in $\mathbb{Q}$ (here of course we identify $\alpha \in \mathbb{Q}$ with $\alpha \cdot [1] \in K$). Now, if $K = \mathbb{Q}$ we are done. Otherwise, choose some Φ in $K - \mathbb{Q}$. We may assume, without loss of generality, that $T\Phi = 0$, for we are free to replace Φ with $\Phi - \frac{1}{2}T\Phi \in K - \mathbb{Q}$ (since $\frac{1}{2}T\Phi \in \mathbb{Q}$), and

$$\begin{aligned} T(\Phi - \frac{1}{2}T\Phi) &= T\Phi - \frac{1}{2}T(T\Phi) \\ &= T\Phi - \frac{1}{2}(2T\Phi) \\ &= 0. \end{aligned}$$

Then, we have

$$\begin{aligned} 0 &= (\Phi - \Phi)(\Phi - \widehat{\Phi}) \\ &= \Phi^2 - (T\Phi)\Phi + N\Phi \\ &= \Phi^2 + N\Phi, \end{aligned}$$

so that Φ^2 is a negative rational number. Hence, $\mathbb{Q}(\Phi)$ is a quadratic imaginary field. Now, by Proposition 2.4.1, it is possible that K is a 4-dimensional $\mathbb{Q}$-vector space. However, this can only happen when k is of prime characteristic (in this case K could be a quaternion algebra). See ([Sil86] VI Thm. 6.16) for a complex analytic proof of this. Since we assume that k is of characteristic zero, we must have $K = \mathbb{Q}(\Phi)$, which completes the proof. □

In Example 2.2.2 we saw that the endomorphism ring of the elliptic curve E with equation $y^2 = x^3 + x$ contains the ring $\mathbb{Z}[i]$ of Gaussian integers. It follows by Theorem 2.6.1 that the endomorphism ring of E is precisely $\mathbb{Z}[i]$.

3 Elliptic curves over $\mathbb{C}$

Our ultimate aim is to develop the theory of complex multiplication for elliptic curves defined over $\bar{\mathbb{Q}}$. In Section 5.2 we prove that any elliptic curve defined over $\mathbb{C}$ with complex multiplication is isomorphic to an elliptic curve defined over $\bar{\mathbb{Q}}$. We turn our attention thus to the complex theory; the main benefit of which (from our point of view) is that an isogeny of complex elliptic curves has a very simple geometric interpretation.

3.1 A brief review of elliptic curves over $\mathbb{C}$

The material relating to the lattices and functions considered in this section can be found in ([Ser73] VII).

Recall that a *lattice* in $\mathbb{C}$ is a subgroup Λ of $\mathbb{C}$ of $\mathbb{Z}$-rank 2, with a $\mathbb{Z}$-basis (ω_1, ω_2) which spans $\mathbb{C}$ over $\mathbb{R}$. The following lemma will not be used until later, but is convenient to prove here.

Lemma 3.1.1. *A subgroup Λ of $\mathbb{C}$ is a lattice if and only if it is a discrete subgroup of $\mathbb{C}$, which spans $\mathbb{C}$ over $\mathbb{R}$.*

Proof. It is clear that a lattice is a discrete subgroup of $\mathbb{C}$. Conversely, let Λ be a discrete subgroup of $\mathbb{C}$. Let ω_1 be a non-zero point in Λ with $|\omega_1|$ minimal, and choose ω_2 in $\Lambda - \mathbb{Z}\omega_1$ with $|\omega_2|$ minimal (such an element exists since Λ spans $\mathbb{C}$ over $\mathbb{R}$). The ratio $\frac{\omega_2}{\omega_1}$ is non-real, since otherwise there would exist an integer n such that

$$n < \frac{\omega_1}{\omega_2} < n + 1,$$

so that $\omega_2 - n\omega_1$ is a point in Λ which satisfies

$$|\omega_2 - n\omega_1| < |\omega_1|,$$

contradicting the minimality of $|\omega_1|$. Then $\mathbb{C} = \mathbb{R}\omega_1 + \mathbb{R}\omega_2$, so that any element ω in Λ can be written in the form

$$\omega = a\omega_1 + b\omega_2, \quad a, b \in \mathbb{R}.$$

Given such an element ω, let m and n be integers such that

$$|a - m| \leq \frac{1}{2} \quad \text{and} \quad |b - n| \leq \frac{1}{2},$$

and consider the element

$$\omega' = \omega - m\omega_1 - n\omega_2 = (a - n)\omega_1 + (b - n)\omega_2 \in \Lambda.$$

Then we have the following inequality:

$$|\omega'| \leq \frac{1}{2}|\omega_1| + \frac{1}{2}|\omega_2| \leq |\omega_2|.$$

Since $\frac{\omega_2}{\omega_1}$ is non-real, one easily deduces that the first inequalty is strict, whence ω' belongs to $\Lambda - \mathbb{Z}\omega_1$, so that ω is in Λ, thus completing the proof. $\square$

Let Λ be a lattice in $\mathbb{C}$. Recall the Weierstrass $\wp$-function:

$$\wp(z,\Lambda)^1 = \frac{1}{z^2} + \sum_{\omega\in\Lambda-0} \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2},$$

and its derivative

$$\wp'(z,\Lambda) = -2\sum_{\omega\in\Lambda} \frac{1}{(z-\omega)^3}.$$

The $\wp$-function is doubly-periodic, and thus descends to a well-defined function on the torus $\mathbb{C}/\Lambda$. Recall also the Eisenstein series for Λ of weight $2k$:

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

There is a relation of algebraic dependence between $\wp$ and its derivative, given by:

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3,$$

where $g_2 = 60G_4(\Lambda)$ and $g_3 = 140G_6(\Lambda)$. So if E_Λ is the curve in $\mathbb{P}^2_{\mathbb{C}}$ defined by the equation

$$y^2 = 4x^3 - g_2x - g_3, \tag{6}$$

then there is a holomorphic bijection of Riemann surfaces $\mathbb{C}/\Lambda \to E_\Lambda$ given by

$$z+\Lambda \to \begin{cases} [\wp(z) : \wp'(z) : 1] & z \neq 0, \\ [0:1:0] & z = 0. \end{cases}$$

The curve defined in (6) is non-singular provided the discriminant

$$\Delta(E_\Lambda) = g_2^3 - 27g_3^2$$

is non-zero.

3.2 Endomorphisms

One advantage of working over the complex numbers is that the endomorphism ring of an elliptic curve can be interpreted in a simple way in terms of the lattice which defines the curve.

Let Λ_1 and Λ_2 be lattices in $\mathbb{C}$. Suppose $\alpha \in \mathbb{C}$ is such that $\alpha\Lambda_1 \subset \Lambda_2$. Then α defines a map $\phi_\alpha \colon \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ given by

$$\phi_\alpha(z+\Lambda_1) = \alpha z + \Lambda_2. \tag{7}$$

This map is well defined; if $\omega \in \Lambda_1$, then

$$\alpha(z+\omega) = \alpha z + \alpha\omega \equiv \alpha z \pmod{\Lambda_2}.$$

The maps ϕ_α are clearly holomorphic group homomorphisms.

[1] We will usually supress the Λ and simply write $\wp(z)$

Proposition 3.2.1. *Let Λ_1 and Λ_2 be lattices in $\mathbb{C}$ and let E_{Λ_1} and E_{Λ_2} be the corresponding elliptic curves given by* (6)*. Then $Hom(E_{\Lambda_1}, E_{\Lambda_2})$ is isomorphic to $\{\alpha \in \mathbb{C} \colon \alpha\Lambda_1 \subset \Lambda_2\}$.*

Proof. We give a sketch of the proof, describing the maps involved. See ([Sil86] VI, Thm 4.1) for the full proof.

Let $Holom(\Lambda_1, \Lambda_2)$ denote the set of holomorphic maps $\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ with $\phi(0) = 0$. The idea is to show that there are bijections between the following two pairs of sets:

(i) $\{\alpha \in \mathbb{C} : \alpha\Lambda_1 \subset \Lambda_2\} \to Holom(\Lambda_1, \Lambda_2)$,

(ii) $\{\text{isogenies } E_{\Lambda_1} \to E_{\Lambda_2}\} \to Holom(\Lambda_1, \Lambda_2)$,

where the map in (i) is given by $\alpha \to \phi_a$ (where ϕ_α is given by (7)), and the map in (ii) is natural inclusion.

We have already seen that ϕ_α is in $Holom(\Lambda_1, \Lambda_2)$, so the mapping in (i) is well defined. The discreteness of Λ_2 shows that the mapping is injective. Conversely, any ϕ in $Holom(\Lambda_1, \Lambda_2)$ lifts to a holomorphic map $\Phi : \mathbb{C} \to \mathbb{C}$ with $\Phi(0) = 0$ such that the following diagram commutes:

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{\Phi} & \mathbb{C} \\ \downarrow & & \downarrow \\ \mathbb{C}/\Lambda_1 & \xrightarrow{\phi} & \mathbb{C}/\Lambda_2 \end{array} .$$

It turns out that $\Phi(\Lambda_1) \subset \Lambda_2$ and that the derivative Φ' of Φ is a holomorphic elliptic function and is thus constant. Thus $\Phi(z) = \alpha z + \beta$, and $\Phi(0) = 0$ shows that $\beta = 0$. Therefore $\phi(z) = \alpha z$ for some non-zero α such that $\alpha\Lambda_1 \subset \Lambda_2$, so $\phi = \phi_\alpha$, showing the mapping in (i) is surjective.

Now consider the mapping in (ii). Since an isogeny $\phi : E_{\Lambda_1} \to E_{\Lambda_2}$ is everywhere locally defined, it defines unique a holomorphic map of Riemann surfaces $\mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$. Conversely any holomorphic map $\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ is given by ϕ_α for some non-zero α satisfying $\alpha\Lambda_1 \subset \Lambda_2$, and so defines a map $E_{\Lambda_1} \to E_{\Lambda_2}$ by

$$(\wp(z, \Lambda_1), \wp'(z, \Lambda_1)) \to (\wp(\alpha z, \Lambda_2), \wp'(\alpha z, \Lambda_2)).$$

Since $\alpha\Lambda_1 \subset \Lambda_2$ it follows that both $\wp(\alpha z, \Lambda_2)$ and its derivative are both elliptic functions of Λ_1, and every such function can be expressed as a rational function in $\wp(z, \Lambda_1)$ and $\wp'(z, \Lambda_1)$, which shows that ϕ is an isogeny. □

Recall that we say two lattices Λ_1 and Λ_2 are *homothetic* if there exists a non-zero α in $\mathbb{C}$ such that $\Lambda_2 = \alpha\Lambda_1$.

Corollary 3.2.1. *Let Λ_1 and Λ_2 be as above. Then the curves E_{Λ_1} and E_{Λ_2} are isomorphic if and only if Λ_1 is homothetic to Λ_2.*

Proof. If $E_1 \cong E_2$ then there exist isogenies $\phi_1 : E_1 \to E_2$ and $\phi_2 : E_2 \to E_1$ which satisfy

$$\phi_2 \circ \phi_1 = id_{E_1} \quad \text{and} \quad \phi_1 \circ \phi_2 = id_{E_2}.$$

Let α and β be non-zero elements of $\mathbb{C}$ such that $\alpha\Lambda_1 \subset \Lambda_2$ and $\beta\Lambda_2 \subset \lambda_1$, and ϕ_1 and ϕ_2 correspond (as in the proof of Proposition 3.2.1) to the holomorphic functions ϕ_α and ϕ_β respectively. Since ϕ_1 and ϕ_2 compose to the identity we must have $\beta = \alpha^{-1}$, so that

$$\alpha\Lambda_1 \subset \Lambda_2 \subset \alpha\Lambda_1.$$

So $\Lambda_2 = \alpha\Lambda_1$ as required. Conversely, if Λ_1 and Λ_2 are homothetic then $\Lambda_2 = \alpha\Lambda_1$ for some non-zero α. Then the map $\phi_\alpha : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\alpha\Lambda_1$ is clearly a bijection with a holomorphic inverse, so E_{Λ_1} and E_{Λ_2} are isomorphic by the commutativity of the following diagram:

$$\begin{array}{ccc} \mathbb{C}/\Lambda_1 & \xrightarrow{\Phi} & \mathbb{C}/\alpha\Lambda_1 \\ \downarrow & & \downarrow \\ E_{\Lambda_1} & \xrightarrow{\phi} & E_{\Lambda_2} \end{array},$$

thus completing the proof. □

The next result is known as the *Uniformisation theorem.* It is useful in that it parametrises every elliptic curve over $\mathbb{C}$

Theorem 3.2.1. *Let A and B be complex numbers which satisfy*

$$A^3 - 27B^2 \neq 0.$$

Then there exists a unique lattice $\Lambda \subset \mathbb{C}$ such that

$$g_2(\Lambda) = A \quad \textit{and} \quad g_3(\Lambda) = B.$$

Proof. See ([Shi94] Section 4.2). □

An obvious consequence of the Uniformisation is the following corollary:

Corollary 3.2.2. *Let E be an elliptic curve over $\mathbb{C}$. Then there exists a lattice Λ in $\mathbb{C}$ such that $E \cong E_\Lambda$, where E_Λ is given by* (6).

Proof. Suppose E is given by the equation

$$y^2 = 4x^3 + Ax + B.$$

Then, since E is non-singular, its discriminant $A^3 - 27B^2$ is non-zero. Now by Uniformisation there exists a lattice Λ such that

$$g_2(\Lambda) = A \quad \text{and} \quad g_3(\Lambda) = B,$$

so that the j-invariant $j(E_\Lambda)$ of the elliptic curve E_Λ is given by

$$\begin{aligned} j(E_\Lambda) &= 1728 \cdot \frac{g_2^3(\Lambda)}{\Delta(E_\Lambda)} \\ &= 1728 \cdot \frac{A^3}{A^3 - 27B^2} \\ &= j(E), \end{aligned}$$

so $E \cong E_\Lambda$ as required. □

When E is an elliptic curve over $\mathbb{C}$, Proposition 3.2.1 together with Uniformisation imply that

$$End(E) \cong \{a \in \mathbb{C} : \alpha\Lambda \subset \Lambda\} \tag{8}$$

for some unique lattice Λ in $\mathbb{C}$.

4 Complex multiplication - basic results

In characteristic zero, the endomorphism ring an elliptic curve E with complex multiplication is isomorphic to an order in the ring of integers of some quadratic imaginary number field k (Theorem 2.6.1). For simplicity, we will only consider the case where $End(E)$ is isomorphic to the full ring of integers $\mathfrak{o}_k$ in some quadratic imaginary field k, and we shall say that E *has complex multiplication by* $\mathfrak{o}_k$. We denote by $Ell(\mathfrak{o}_k)$ the set of isomorphism classes of elliptic curves with complex multiplication by $\mathfrak{o}_k$. Note that, if E has complex multiplication by $\mathfrak{o}_k$ then there are exactly two ways in which $End(E)$ can be embedded in $\mathbb{C}$. We will always use the identification determined by the following commutative diagram (replacing E by E_Λ for some lattice Λ, which is possible by Uniformisation):

$$\begin{array}{ccc} \mathbb{C}/\Lambda & \xrightarrow{\phi_\alpha} & \mathbb{C}/\Lambda \\ \downarrow f & & \downarrow f \\ E_\Lambda & \xrightarrow{[\alpha]} & E_\Lambda \end{array} \tag{9}$$

where f is the isomorphism described in (6), and ϕ_α and $[\alpha]$ are the maps determined in Proposition 3.2.1 and (8) respectively.

For example, let $\Lambda = \mathbb{Z}[i]$. Then

$$\wp(iz) = \frac{1}{(iz)^2} + \sum_{\omega \in \Lambda - 0} \frac{1}{(iz-\omega)^2} - \frac{1}{\omega^2},$$

and since $i\Lambda = \Lambda$ we may replace ω with $i\omega$ in the above summation, so that

$$\wp(iz) = -\wp(z).$$

Similarly, the same method shows that

$$\wp'(iz) = i\wp(z).$$

Now consider the elliptic curve E_Λ. Then (9) says that the endomorphism $[i]$ is determined by

$$[i](x, y) = (-x, y).$$

Furthermore, using again the fact that $i\Lambda = \Lambda$ we have

$$g_3(\Lambda) = g_3(i\Lambda) = 140 \sum_{\omega \in \Lambda} \frac{1}{(i\omega)^6} = -g_3(\Lambda),$$

so that $g_3(\Lambda) = 0$ and E_Λ is given by the equation

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

Therefore, E_Λ is isomorphic to the elliptic curve E given by

$$y^2 = x^3 + x,$$

since $j(E_\Lambda) = 1728 = j(E)$. This justifies the description of the endomorphism described in Example 2.2.2.

4.1 Fractional ideals

We recall some basic results from algebraic number theory which we shall need in the sequel.

Let k be a number field, with ring of integers $\mathfrak{o}_k$. A *fractional ideal* of k is a non-zero $\mathfrak{o}_k$-module $\mathfrak{a}$ of k which satisfies one of the following two equivalent conditions:

(i) $\mathfrak{a}$ is finitely generated,

(ii) there exists a non-zero element a in $\mathfrak{o}_k$ such that $a\mathfrak{a} \subset \mathfrak{o}_k$.

Every ideal of $\mathfrak{o}_k$ is obviously a fractional ideal of k, and we refer to such an ideal as an *integral ideal*. The quotient $\mathfrak{o}_k/\mathfrak{a}$ is finite, and we define the *norm* $N\mathfrak{a}$ *of* $\mathfrak{a}$ by

$$N\mathfrak{a} = \#(\mathfrak{o}_k/\mathfrak{a}).$$

In particular, if k is quadratic, then $k = \mathbb{Q}(\sqrt{d})$ for some square-free integer d and every element α of k is of the form

$$\alpha = a + b\sqrt{d}$$

where a and b are in $\mathbb{Q}$. When α is an integer in k (i.e. $\alpha \in \mathfrak{o}_k$), then $a^2 - db^2$ is a rational integer, and the principle ideal (α) of $\mathfrak{o}_k$ satisfies

$$N(\alpha) = |a^2 - db^2|.$$

A fractional ideal is *principal* if it is of the form $c\mathfrak{o}_k$ for some c in k. If $\mathfrak{a}$ is a fractional ideal of k, then we define $\mathfrak{a}^{-1}$ to be the set

$$\mathfrak{a}^{-1} = \{x \in k \colon x\mathfrak{a} \subset \mathfrak{o}_k\}.$$

While not obvious from the definition, the set $\mathfrak{a}^{-1}$ is a fractional ideal, and the product $\mathfrak{a} \cdot \mathfrak{a}^{-1}$ is equal to $\mathfrak{o}_k$. The fractional ideals of k form an abelian group with identity element $\mathfrak{o}_k$. The quotient of this group by the principle fractional ideals is known as the *class group* of k, and is denoted by $Cl(k)$. It is finite, and its order h_k is known as the *class number* of k. Each ideal class in $Cl(k)$ can be represented by an integral ideal.

In the case where k is a quadratic imaginary field, the following result will allow us to construct elliptic curves with complex multiplication by $\mathfrak{o}_k$.

Lemma 4.1.1. *Let k be a quadratic imaginary number field. Every fractional ideal $\mathfrak{a}$ of k is a lattice in $\mathbb{C}$.*

Proof. Let $\mathfrak{a}$ be a fractional ideal of k. Using the inclusion $\mathbb{Z} \subset \mathfrak{o}_k$ it follows that $\mathfrak{a}$ is a free $\mathbb{Z}$-module of rank 2. Furthermore, it is clear that $\mathfrak{a}$ is not contained in $\mathbb{R}$. Thus $\mathfrak{a}$ is a lattice, as required. □

4.2 Constructing elliptic curves with complex multiplication by $\mathfrak{o}_k$

Thus far we have not found a satisfactory way of constructing elliptic curves (over $\mathbb{C}$) with complex multiplication. We shall remedy this situation now. More precisely, to every fractional ideal $\mathfrak{a}$ of k, for some quadratic imaginary field k, we will associate an elliptic curve which has complex multiplication by $\mathfrak{o}_k$. We shall see later (Theorem 4.2.2) that every elliptic curve with complex multiplication by $\mathfrak{o}_k$ is isomorphic to one which is obtained from a fractional ideal of k.

Theorem 4.2.1. *Let k be a quadratic imaginary field, $\mathfrak{o}_k$ its ring of integers, and let $\mathfrak{a}$ be a fractional ideal of k. Then the elliptic curve $E_{\mathfrak{a}}$ has complex multiplication by $\mathfrak{o}_k$.*

Proof. Consider the endomorphism ring of the elliptic curve $E_{\mathfrak{a}}$:

$$End(E_{\mathfrak{a}}) \cong \{\alpha \in \mathbb{C} \colon \alpha\mathfrak{a} \subset \mathfrak{a}\}$$

Now, since $\mathfrak{a} \subset k$, any such α must be an element of k. But $\mathfrak{a}$ is a finitely generated $\mathfrak{o}_k$-submodule of k, so in fact α must be an element in $\mathfrak{o}_k$. Conversely, any element α in $\mathfrak{o}_k$ trivially satisfies $\alpha\mathfrak{a} \subset \mathfrak{a}$. Thus $End(E_{\mathfrak{a}}) \cong \mathfrak{o}_k$. □

Recall that homothetic lattices give rise to isomorphic elliptic curves by Corollary 3.2.1. In particular, replacing a fractional ideal $\mathfrak{a}$ of k with $c\mathfrak{a}$ for some non-zero element c in k will give an elliptic curve $E_{c\mathfrak{a}}$ which has complex multiplication by $\mathfrak{o}_k$ and is isomorphic to $E_{\mathfrak{a}}$. This suggest that the class group $Cl(k)$ of k may play a role in the theory.

Let Λ be a lattice in $\mathbb{C}$. For a fractional ideal $\mathfrak{a}$ of k we define the product $\mathfrak{a}\Lambda$ to be the subset of $\mathbb{C}$ consisting of finite sums of products of elements of $\mathfrak{a}$ and Λ:

$$\mathfrak{a}\Lambda = \{\sum x_i\omega_i \colon x_i \in \mathfrak{a}, \omega_i \in \Lambda\}.$$

Lemma 4.2.1. *Suppose Λ is such that the elliptic curve E_Λ has complex multiplication by $\mathfrak{o}_k$. Then $\mathfrak{o}_k\Lambda = \Lambda$, and $\mathfrak{a}\Lambda$ is a lattice in $\mathbb{C}$ for every fractional ideal $\mathfrak{a}$ of k.*

Proof. The first part is clear, since $End(E_\Lambda) \cong \{\alpha \in \mathbb{C} \colon \alpha\Lambda \subset \Lambda\}$. Now let $\mathfrak{a}$ be a fractional ideal of k. Since k is a quadratic field, we have $k = \mathbb{Q}(\sqrt{d})$ for some square free integer d, and

$$\mathfrak{o}_k = \begin{cases} \mathbb{Z}[\sqrt{d}] & d \equiv 2 \text{ or } 3 \pmod 4, \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & d \equiv 1 \pmod 4. \end{cases}$$

Let a be an element of $\mathfrak{o}_k$ such that $a\mathfrak{a} \subset \mathfrak{o}_k$. We may assume a is a rational integer; if $d \equiv 2$ or $3 \pmod 4$ then $a = x + y\sqrt{d}$ for some rational integers x and y, and if a is not rational we may replace it with $(x - y\sqrt{d}) \cdot a$ which is a rational integer taking $\mathfrak{a}$ into $\mathfrak{o}_k$. Similarly if $d \equiv 1 \pmod 4$ then $a = \frac{x+y\sqrt{d}}{2}$,

and replacing a with $4 \cdot (\frac{x-y\sqrt{d}}{2}) \cdot a$ gives the desired result. Since $a\mathfrak{a} \subset \mathfrak{o}_k$ the first part of the lemma shows

$$\mathfrak{a}\Lambda \subset \frac{1}{a}\Lambda,$$

so $\mathfrak{a}\Lambda$ is a discrete subgroup of $\mathbb{C}$ and is hence a lattice by Lemma 3.1.1. $\square$

Suppose Λ is a lattice such that E_Λ has complex multiplication by $\mathfrak{o}_k$. Lemma 4.2.1 allows us to construct the elliptic curve $E_{\mathfrak{a}\Lambda}$, for some fractional ideal $\mathfrak{a}$ of k. The endomorphism ring of $E_{\mathfrak{a}\Lambda}$ is isomorphic to

$$\{\alpha \in \mathbb{C} : \alpha\mathfrak{a}\Lambda \subset \mathfrak{a}\Lambda\}.$$

However, since $\mathfrak{a} \cdot \mathfrak{a}^{-1} = \mathfrak{o}_k$ we have

$$\alpha\mathfrak{a}\Lambda \subset \mathfrak{a}\Lambda \Leftrightarrow \alpha\Lambda \subset \Lambda,$$

so $E_{\mathfrak{a}\Lambda}$ has complex multiplication by $\mathfrak{o}_k$.

It is now easy to see that there is a well-defined action of the class group $Cl(k)$ on $Ell(\mathfrak{o}_k)$. For an ideal class $\mathfrak{a}$ in $Cl(k)$ and an elliptic curve E_Λ in $Ell(\mathfrak{o}_k)$ we define the action as follows:

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

That the action is well-defined follows from the remarks after Theorem 4.2.1. Furthermore, we have

$$E_\Lambda^{\mathfrak{o}_k} = E_{\mathfrak{o}^{-1}\Lambda} = E_{\mathfrak{o}\Lambda} = E_\Lambda,$$

and

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

where $\mathfrak{a}$ and $\mathfrak{b}$ represent any non-trivial ideal classes in $Cl(k)$.

Remark 4.2.1. We choose $\mathfrak{a}^{-1}$ in the definition of the action out of respect for convention. The use of the inverse makes things easier in the deeper theory of complex multiplication (which we will not quite reach).

Lemma 4.2.2. *Let Λ be a lattice such that E_Λ has complex multiplication by $\mathfrak{o}_k$. Let (ω_1, ω_2) be a generating set for Λ over $\mathbb{Z}$. Then $\mathbb{Q}(\frac{\omega_1}{\omega_2})$ is a quadratic imaginary field, equal to k.*

Proof. Let $\tau = \frac{\omega_1}{\omega_2}$. In particular τ is non-real, by definition of Λ. We may assume that $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$, since homothetic lattices give rise to isomorphic curves. Let $R = \{\alpha \in \mathbb{C} : \alpha\Lambda \subset \Lambda\} \cong End(E_\Lambda)\}$. Then, since both 1 and τ belong to Λ, there exist rational integers a, b, c and d such that

$$\alpha = a + b\tau \quad \text{and} \quad \alpha\tau = c + d\tau,$$

for any α in R (so $R \subset \Lambda$). Re-arranging the above equations yields

$$b\tau^2 + a\tau = \alpha\tau = c + d\tau,$$

so that τ is a non-real root of an integral quadratic equation, and hence the field $\mathbb{Q}(\tau) = \mathbb{Q}(\frac{\omega_1}{\omega_2})$ is quadratic imaginary. Similarly, we have

$$(\alpha - a)(\alpha - d) = (\alpha - d)b\tau = bc,$$

so every α in $R \subset \mathbb{Q}(\tau)$ is a root of a monic integral quadratic equation, and hence is an integer in $\mathbb{Q}(\tau)$. This shows that $R \otimes \mathbb{Q} = \mathbb{Q}(\tau)$. On the other hand, we have $R \cong End(E)$ so $R \otimes \mathbb{Q} = k$. Hence $\mathbb{Q}(\frac{\omega_1}{\omega_2}) = k$, as required. □

Theorem 4.2.2. *The action of $Cl(k)$ on $Ell(\mathfrak{o}_k)$ is simply transitive. In particular,*

$$\#Ell(\mathfrak{o}_k) \leq h_k.$$

Proof. Let Λ_1 and Λ_2 be lattices in $\mathbb{C}$ such that the elliptic curves E_{Λ_1} and E_{Λ_2} have complex multiplication by $\mathfrak{o}_k$. Choose a non-zero element λ_1 in Λ_1 and consider the lattice $\mathfrak{a}_1 = \frac{a}{\lambda_1}\Lambda$. Let (ω_1, ω_2) be a generating set for Λ_1 over $\mathbb{Z}$. Then $\lambda_1 = c\omega_1 + d\omega_2$ for some rational integers c and d, and the elements of $\mathfrak{a}_1$ are of the form

$$\frac{a\omega_1 + b\omega_2}{c\omega_1 + d\omega_2}.$$

Multiplying the numerator and denominator by $\frac{1}{\omega_2}$ shows that $\mathfrak{a}_1$ is contained in k, by Lemma 4.2.2. Furthermore, since $\mathfrak{o}_k \cong E = \{\alpha \in \mathbb{C} : \alpha\Lambda_1 \subset \Lambda_1\}$ we see that there is a homomorphism $\mathfrak{o}_k \to End(\mathfrak{a}_1)$ determined by the following diagram:

$$\begin{array}{ccc} \mathfrak{o}_k & \longrightarrow & E \\ & \searrow & \downarrow f \\ & & End(\mathfrak{a}_1) \end{array}$$

where $f(\alpha)$ is the endomorphism of $\mathfrak{a}_1$ given by

$$f(\alpha)(x) = \alpha \cdot x.$$

Thus $\mathfrak{a}_1$ is a finitely-generated $\mathfrak{o}_k$-module, and is hence a fractional ideal of k. Similarly, choosing a non-zero element λ_2 of Λ_2 gives a fractional ideal $\mathfrak{a}_2 = \frac{1}{\lambda_2}$ of k. We have

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

so that

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

and $E_{\frac{\lambda_1}{\lambda_2}\Lambda_2}$ is isomorphic to E_{Λ_2} by Corollary 3.2.1. Thus $Cl(k)$ acts transitively on $Ell(\mathfrak{o}_k)$. It remains to prove that the action is simply transitive, i.e. if $E_\Lambda^{\mathfrak{a}} = E_\Lambda^{\mathfrak{b}}$ then $\mathfrak{a} = \mathfrak{b}$ in $Cl(k)$. So, suppose $E_\Lambda^{\mathfrak{a}} = E_\Lambda^{\mathfrak{b}}$. Then $\mathfrak{a}^{-1}\Lambda = \alpha\mathfrak{b}^{-1}\Lambda$ for some non-zero α in $\mathbb{C}$. Equivalently, we have the relations

$$\Lambda = \alpha\mathfrak{a}\mathfrak{b}^{-1}\Lambda \quad \text{and} \quad \Lambda = \alpha^{-1}\mathfrak{b}\mathfrak{a}^{-1},$$

from which it follows that both $\alpha\mathfrak{a}\mathfrak{b}^{-1}$ and $\alpha^{-1}\mathfrak{b}\mathfrak{a}^{-1}$ are both contained in $\mathfrak{o}_k$:

$$\alpha\mathfrak{a}\mathfrak{b}^{-1} \subset \mathfrak{o}_k \quad \text{and} \quad \alpha^{-1}\mathfrak{b}\mathfrak{a}^{-1} \subset \mathfrak{o}_k.$$

Multiplying the second containment by $\alpha\mathfrak{a}\mathfrak{b}^{-1}$ gives

$$\alpha\mathfrak{a}\mathfrak{b}^{-1}\mathfrak{o}_k \subset \mathfrak{o}_k \subset \alpha\mathfrak{a}\mathfrak{b}^{-1},$$

whence $\mathfrak{o}_k = \alpha\mathfrak{a}\mathfrak{b}^{-1}$. Then $\mathfrak{b} = \alpha\mathfrak{a}$, so α is in k, and $\mathfrak{a} = \mathfrak{b}$ in $Cl(k)$, as required. □

4.3 The group of $\mathfrak{a}$-torsion points

In section 2.2 we determined the structure of the group $E[m]$ of m-torsion points of an arbitrary elliptic curve E. In the case where E has complex multiplication by $\mathfrak{o}_k$ it will be helpful to consider other subgroups of E.

Let E be an elliptic curve with complex multiplication by $\mathfrak{o}_k$, and let $\mathfrak{a}$ be an integral ideal of k. Let Λ be a lattice in $\mathbb{C}$ such that $E \cong E_\Lambda$. By Lemma 4.2.1 we have

$$\mathfrak{a}\Lambda \subset \Lambda,$$

so that

$$\Lambda \subset \mathfrak{a}^{-1}\Lambda,$$

which induces an isogeny $\phi_\mathfrak{a} : E_\Lambda \to E_\Lambda^\mathfrak{a}$:

$$\begin{array}{ccc} \mathbb{C}/\Lambda & \longrightarrow & \mathbb{C}/\mathfrak{a}^{-1}\Lambda \\ \downarrow & & \downarrow \\ E_\Lambda & \xrightarrow{\phi_\mathfrak{a}} & E_\Lambda^\mathfrak{a}. \end{array}$$

Proposition 4.3.1. *The kernel of the isogeny $\phi_\mathfrak{a}$ is the set*

$$\ker \phi_\mathfrak{a} = \{P \in E : [\alpha]P = \mathcal{O} \text{ for all } \alpha \in \mathfrak{a}\},$$

where $[\alpha]$ is the endomorphism of E determined by (9)*. Furthermore, it is a free $\mathfrak{o}_k/\mathfrak{a}$-module of rank* 1*.*

Proof. See ([Sil94] II, Prop. 1.4). □

We thus define the kernel of $\phi_\mathfrak{a}$ to be the *group of $\mathfrak{a}$-torsion points of E* and denote it by $E[\mathfrak{a}]$.

5 Complex multiplication over algebraic extensions of $\mathbb{Q}$

Let E be an elliptic curve defined over $\mathbb{C}$, given by the equation

$$y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{C},$$

and let σ be a field automorphism of $\mathbb{C}$. We define E^σ to be the elliptic curve obtained by letting σ act on the coefficients of the equation of E, i.e. E^σ is obtained from the equation

$$y^2 = x^3 + A^\sigma x + B^\sigma.$$

It is clear that $E^\sigma = \{P^\sigma : P \in E\}$, for if $P = (x, y)$, then $P^\sigma = (x^\sigma, y^\sigma)$ satisfies

$$(y^\sigma)^2 - ((x^\sigma)^3 + A^\sigma(x^\sigma) + B^\sigma) = (y^2 - (x^3 + Ax + B))^\sigma = 0^\sigma = 0.$$

Note that, since $j(E)$ is given by a rational function in A and B we have

$$j(E^\sigma) = j(E)^\sigma \tag{10}$$

Now, if ϕ is an endomorphism of E, then ϕ is given by rational maps in the function field $\mathbb{C}(E)$:

$$\phi = (f_1, f_2), \quad f_i \in \mathbb{C}(E),$$

and we define an endomorphism ϕ^σ of E^σ in the obvious way:

$$\phi^\sigma = (f_1^\sigma, f_2^\sigma).$$

It turns out that every endomorphism of E^σ is defined in this way.

Thus for an elliptic curve E and an automorphism σ of $\mathbb{C}$ we have shown that

$$End(E) \cong End(E^\sigma). \tag{11}$$

In particular, if E has complex multiplication by $\mathfrak{o}_k$, then so does E^σ. Furthermore, for all α in $\mathfrak{o}_k$, we have

$$[\alpha]_E^\sigma = [\alpha^\sigma]_{E^\sigma} \tag{12}$$

(for a proof of this, see ([Sil94] II, Thm 2.2)).

5.1 Rationality properties

Proposition 5.1.1. *Let E be an elliptic curve with complex multiplication by $\mathfrak{o}_k$. Then $j(E)$ is algebraic over $\mathbb{Q}$.*

Proof. Consider the extension $K = \mathbb{Q}(j(E))$ of $\mathbb{Q}$. By Theorem 4.2.2 we know that there only finitely many values that the j-invariant of an elliptic curve with complex multiplication by $\mathfrak{o}_k$ can attain (recall that the j-invariant classifies elliptic curves up to isomorphism), and by (10) and (11) we have that the set

$$\{j(E)^\sigma : \sigma \in Aut(\mathbb{C})\}$$

is finite. Now every K-embedding $\sigma : K \to \mathbb{C}$ is determined by $\sigma(j(E))$. On the other hand, any such σ is the restriction of an automorphism of $\mathbb{C}$. Thus, there are only finitely many such σ, so that $[\mathbb{Q}(j(E)) : \mathbb{Q}]$ is finite, which implies that $j(E)$ is algebraic over $\mathbb{Q}$. □

Remark 5.1.1. There is a much stronger result, which states that for an elliptic curve E with complex multiplication by $\mathbb{O}_k$, we have that $j(E)$ is an algebraic integer.

Let $Ell_{\bar{\mathbb{Q}}}(\mathfrak{o}_k)$ denote the set of isomorphism classes of elliptic curves defined over $\bar{\mathbb{Q}}$. If E is an elliptic curve defined over $\bar{\mathbb{Q}}$ then its isomorphism class (in $Ell_{\bar{\mathbb{Q}}}(\mathfrak{o}_k)$) is certainly contained in the isomorphism class of E considered as an elliptic curve over $\mathbb{C}$. Let $i : Ell_{\bar{\mathbb{Q}}}(\mathfrak{o}_k) \to Ell(\mathfrak{o}_k)$ denote this map.

Theorem 5.1.1. *The map $i : Ell_{\bar{\mathbb{Q}}}(\mathfrak{o}_k) \to Ell(\mathfrak{o}_k)$ is a bijection.*

Proof. By Proposition 5.1.1, any elliptic curve E with complex multiplication by $\mathfrak{o}_k$ satisfies $j(E) \in \bar{\mathbb{Q}}$, and from the general theory of elliptic curves we know that E is isomorphic to a curve defined over $\mathbb{Q}(j(E))$, so i is surjective. Similarly, if E_1 and E_2 are elliptic curves over $\bar{\mathbb{Q}}$ with complex multiplication by $\mathfrak{o}_k$, such that $i(E_1) = i(E_2)$, then $j(E_1) = j(E_2)$, so the curves must be isomorphic. Hence i is injective, as required. □

The above theorem justifies our approach to an essentially algebraic phenomenon via analytic methods. From an arithmetic point of view the set $Ell_{\bar{\mathbb{Q}}}(\mathfrak{o}_k)$ is "more interesting" than $Ell(\mathfrak{o}_k)$, but Theorem 5.1.1 says that the latter set, which is easily computed, will suit our purposes entirely.

5.2 Towards abelian extensions of quadratic imaginary fields

Let E be an elliptic curve defined over $\mathbb{C}$ with complex multiplication by $\mathfrak{o}_k$. For every positive integer m let K_m be the field extension of K obtained by adjoining to K the value $j(E)$ and the co-ordinates of the (non-trivial) m-torsion points of E (c.f. section 2.2):

$$K_m = k(j(E), x_1, y_1, \ldots, x_r, y_r) \tag{13}$$

where (x_i, y_i) are the co-ordinates of the points in $E[m]$. To ease notation we write

$$K_m = k(j(E), E[m]).$$

Theorem 5.2.1. *The field K_m is a finite abelian extension of $k(j(E))$.*

Proof. Let $\sigma : K_m \to \mathbb{C}$ be a K_m-embedding. By Lemma 2.5.1 we know that $E[m]$ is stable under the action of $Gal(\bar{k}/k)$. In particular, we have

$$\sigma(x_i) = x_j \quad \text{and} \quad \sigma(y_i) = y_j$$

for all points $(x_i, y_i), (x_j, y_j)$ in $E[m]$. Thus it is clear that K_m is a normal extension of k, and hence is Galois since k is of characteristic zero. Furthermore, since $E[m]$ is finite for all m then each x_i and y_i have only finitely many Galois conjugates (as in the proof of Proposition 5.1.1), and are hence algebraic over k. This completes the first part of the theorem.

To see that $Gal(K_m/k)$ is abelian is more subtle. Recall the representation $\rho : Gal(\bar{k}/k) \to Aut(E[m])$ given in (5):

$$\rho(\sigma)(P) = P^\sigma.$$

We claim that ρ is injective. Indeed, suppose that $\sigma \in \ker \rho$. Then $P^\sigma = P$ for every P in $E[m]$. In particular, we have

$$\sigma(x_i) = x_i \quad \text{and} \quad \sigma(y_i) = y_i,$$

for every $P = (x_i, y_i)$ in $E[m]$. So σ is the identity on K_m, and hence $\ker \rho$ is trivial, as required.

Recall that $E[m]$ has the structure of an $\mathfrak{o}_k/m\mathfrak{o}_k$-module by Proposition 4.3.1. Furthermore, we may assume E is defined over $k(j(E))$, so that any endomorphism of E is defined over $k(j(E))$, i.e. given by rational functions with coefficients in $k(j(E))$. In particular, we have

$$([\alpha](P))^\sigma = [\alpha]^\sigma(P^\sigma) = [\alpha](P^\sigma), \quad \alpha \in \mathfrak{o}_k,$$

by (12). So $Gal(K_m/k(j(E)))$ injects into a subgroup of the $\mathfrak{o}_k/m\mathfrak{o}_k$-module automorphisms of $E[m]$, but by Proposition 4.3.1 we have

$$Aut_{\mathfrak{o}_k/m\mathfrak{o}_k}(E[m]) = (\mathfrak{o}_k/m\mathfrak{o}_k)^*,$$

thus completing the proof. □

Remark 5.2.1. In general the extension K_m is *not* an abelian extension of k. Of course, if $j(E)$ is rational then K_m is an abelian extension of k. We illustrate this explicitly in the next section.

6 Abelian extensions of $\mathbb{Q}(i)$

Let $k = \mathbb{Q}(i)$, so that $\mathfrak{o}_k = \mathbb{Z}[i]$. In Section 2.6 we established that the elliptic curve E given by the equation

$$y^2 = x^3 + x$$

has complex multiplication by $\mathbb{Z}[i]$. In particular, we know that $h_k = 1$ so $j(E)$ is rational (indeed, we have $j(E) = 1728$).

Consider the group $E[2]$ of 2-torsion points of E. Recall that a point $P = (x, y)$ on E has order 2 if and only if $y = 0$. So the x-co-ordinates are given by the roots of the equation

$$x^3 + x = 0,$$

which are clearly equal to 0, i and $-i$. In particular, the field $K_2 = \mathbb{Q}(i)(E[2])$ is generated by elements contained in $\mathbb{Q}(i)$, so that $K_2 = \mathbb{Q}(i)$.

Now consider the group of 3-torsion points of E. There are 8 non-trivial such points (since $\#E[3] = 9$), whose x-co-ordinates are determined by the roots of the quartic equation

$$3x^4 + 6x^2 - 1. \tag{14}$$

Solving the corresponding quadratic in $u = x^2$ we see that the roots of (14) are $\pm\alpha, \pm\frac{i}{\sqrt{3}\alpha}$[2], where

$$\alpha = \sqrt{\frac{2\sqrt{3} - 3}{3}}.$$

To find the y-co-ordinates, note that

$$\alpha^3 + \alpha = \alpha(\alpha^2 + 1) = \frac{2\alpha}{\sqrt{3}},$$

and

$$(\frac{i}{\sqrt{3}\alpha})^3 + \frac{i}{\sqrt{3}\alpha} = \frac{-2i}{3\alpha} = \frac{-4i}{\sqrt{27}(\frac{2\alpha}{\sqrt{3}})} = \frac{-4i}{\sqrt{27}\beta^2},$$

where

$$\beta = \sqrt{\frac{2\alpha}{\sqrt{3}}},$$

so that

$$E[3] = \{\mathcal{O}, (\alpha, \pm\beta), (-\alpha, \pm\beta), (\frac{i}{\sqrt{3}\alpha}, \pm\frac{2\sqrt{-i}}{\sqrt[4]{27}\beta}), (-\frac{i}{\sqrt{3}\alpha}, \frac{2\sqrt{i}}{\sqrt[4]{27}\beta})\}.$$

[2]This follows from the method of "Lagrange resultants"; a monic quadratic polynomial $x^2 + px + q$ over an algebraically closed field k factors as $(x - \alpha)(x - \beta)$ where α and β are roots of the polynomial in k. In particular, comparing coefficients gives the identities $\alpha + \beta = p$ and $\alpha\beta = q$, the second of which we use here.

We claim that $K_3 = \mathbb{Q}(i)(E[3]) = \mathbb{Q}(i, \beta)$, i.e. the co-ordinates of the points in $E[3]$ can be described by rational functions of i and β. Indeed, we have

$$\beta^2 = \frac{2\alpha}{\sqrt{3}} \tag{15}$$

$$\beta^4 = \frac{4}{9}(2\sqrt{3} - 3) \tag{16}$$

so (16) shows that $\sqrt{3}$ belongs to $\mathbb{Q}(i, \beta)$, which in turn (along with (15)) shows that α is also in $\mathbb{Q}(i, \beta)$, as required.

Now, the minimal polynomial for β over $\mathbb{Q}(i)$ is

$$x^8 + \frac{8}{3}x^4 - \frac{16}{27}, \tag{17}$$

so that $[K_3 : \mathbb{Q}(i)] = 8$. Since (17) has such a simple form, we are reduced to solving a quadratic equation (as we did with (14)), and we find that the roots of (17) are

$$\pm\beta, \pm i\beta, \pm\frac{2\sqrt{i}}{\sqrt[4]{27}\beta}, \pm\frac{2\sqrt{-i}}{\sqrt[4]{27}\beta}.$$

References

[Har77] Robin Hartshorne, *Algebraic geometry*, Springer, 1977.

[Ser73] Jean-Pierre Serre, *A course in arithmetic*, Springer, 1973.

[Sha94] Igor Shafarevich, *Basic algebraic geometry*, vol. 1, Springer-Verlag, 1994.

[Shi94] Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*, Princeton, 1994.

[Sil86] Joseph Silverman, *The arithmetic of elliptic curves*, Springer, 1986.

[Sil94] _____, *Advanced topics in the arithmetic of elliptic curves*, Springer, 1994.