# Elliptic Curves with Complex Multiplication

September 5, 2009

# Contents

**1 Introduction** **3**

**2 The endomorphism ring of an elliptic curve** **4**
2.1 Isogenies . . . . . 4
2.2 Some properties of $End(E)$ . . . . . 4
2.3 Dual isogenies . . . . . 6
2.4 The Tate module . . . . . 7
2.5 The action of $Gal(\bar{k}/k)$ on $E[m]$ . . . . . 7
2.6 The structure of $End(E)$ in characteristic zero . . . . . 8

**3 Elliptic curves over $\mathbb{C}$** **9**
3.1 A brief review of elliptic curves over $\mathbb{C}$ . . . . . 9
3.2 Endomorphisms . . . . . 10

**4 Complex multiplication - basic results** **11**
4.1 Fractional ideals . . . . . 11
4.2 Constructing elliptic curves with complex multiplication by $\mathfrak{o}_k$ . 12
4.3 The group of $\mathfrak{a}$-torsion points . . . . . 14

**5 Complex multiplication over algebraic extensions of $\mathbb{Q}$** **16**
5.1 Towards abelian extensions of quadratic imaginary fields . . . . . 17

**6 Abelian extensions of $\mathbb{Q}(i)$** **19**

# 1 Introduction

# 2 The endomorphism ring of an elliptic curve

Unless stated otherwise, all elliptic curves are defined over a field $k$ of characteristic not equal to 2 or 3.

## 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

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

Any isogeny is automatically a group homomorphism ([Sil86] III, §4, Thm 4.8). Furthermore, a non-zero isogeny is surjective ([Sha94] I, §5.3, Thm 4). Therefore, such 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 $\phi$ 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

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

We say $\phi$ is *separable*, *inseparable* or *purely inseparable* according to the extension.

TODO: write something about finiteness of kernels.

**Proposition 2.1.1.** *Let $E_1$ and $E_2$ be elliptic curves over a field $k$ of characteristic zero and suppose there exists an isogeny $\phi : E_1 \to E_2$. Then*

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

*Proof.* TODO: reference *something*. □

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. TODO: SHOW IT IS COMMUTATIVE!!

**Example 2.2.1.** Let $E$ be an elliptic curve. 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 is the familiar subgroup $E\,[m]$ of $E$. From the definition (and the tower law for field extensions) it follows that $[m] \circ [n] = [mn]$.

An elliptic curve $E$ has precisely three points of order 2. Since $E$ is infinite, there exists a point $P_1$ on $E$ of order not equal to 2 so that $[2]\,P_1 \neq \mathcal{O}$. Similarly, for a point $P_2$ of order 2, any odd integer $m$ satisfies $[m]\,P_2 = P_2$. Thus for all non-zero $m$ it follows that $[m] \neq [0]$.

As a $\mathbb{Z}$-module, the endomorphism ring of an elliptic curve $E$ is torsion-free; if $\phi \in End(E)$ and $m \in \mathbb{Z}$ satisfy

$$[m] \circ \phi = [0]$$

then by (1),

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

whence either $m = 0$ or $deg\left([m]\right) > 0$, in which case $\phi = [0]$ and $m \neq 0$.

Taking degrees also shows that $End(E)$ is an integral domain; if $\phi_1$ and $\phi_2$ are endomorphisms of $E$ such that

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

then

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

from which the result follows.

We summarise what we have shown in the following proposition.

**Proposition 2.2.1.** *Let $E$ be an elliptic curve. Then $End(E)$ is a characteristic zero integral domain.*

An elliptic curve whose endomorphism ring is strictly larger than $\mathbb{Z}$ is said to have *complex multiplication*.

**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.** TODO: Example showing all curves over finite fields have CM.

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

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

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

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 $\phi$ (when $\phi = [0]$ we define $\hat{\phi}$ to be $[0]$). We say $\hat{\phi}$ is the *dual isogeny* to $\phi$. 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 $k$ of characteristic zero, and let $m \in \mathbb{Z}$. Then*

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

## 2.4 The Tate module

Let $E$ be an elliptic curve over a field $k$ of characteristic zero, and let $\ell$ be a rational prime. For every positive integer $n$ the multiplication-by-$\ell$ map takes $E[\ell^{n+1}]$ into $E[\ell^n]$. We thus define the *$\ell$-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 $\ell^n$, 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 Proposition 2.3.1, it follows immediately from the definition that

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

TODO: Some commutative algebra giving a bound on the Z-rank of End(E).

## 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 $\sigma$ be an element of $Gal(\bar{k}/k)$. We define $P^\sigma$ to be the point $P^\sigma = (x^\sigma, y^\sigma)$. Now for an arbitrary point $P$ on $E$ there is no reason why $P^\sigma$ should also lie on $E$. However, 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 $\sigma$ 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.* We only need to check that $(P^{\sigma_1})^{\sigma_2} = P^{\sigma_1\sigma_2}$. TODO: finish, boring. □

A consequence of Lemma 2.5.1 is that we have a representation $\rho : Gal(\bar{k}/k) \to Aut(E[m])$, given by

$$\rho(\sigma)(P) = P^\sigma. \tag{3}$$

Note also, that by Proposition 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

TODO: Short introduction.

**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

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

where $\hat{\phi}$ is the dual isogeny to $\phi$. □

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 $\mathbb{C}$

Thus far we have established the general structure of the endomorphism ring of an elliptic curve, but we do not yet have a satisfactory way of determining whether a given elliptic curve has complex multiplication or not. TODO: more intro material.

Our ultimate aim is to develop the theory of elliptic curves over $\bar{\mathbb{Q}}$. In Section ? we prove that 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 $\mathbb{C}$

TODO: Reference A Course in Arithmetic.

Recall that a *lattice* in $\mathbb{C}$ is a subgroup of $\mathbb{C}$ of $\mathbb{Z}$-rank 2, with a $\mathbb{Z}$-basis $(\omega_1, \omega_2)$ which spans $\mathbb{C}$ over $\mathbb{R}$.

**Lemma 3.1.1.** *A subgroup $H$ of $\mathbb{C}$ is a lattice if and only if it is a discrete subgroup of $\mathbb{C}$.*

*Proof.* Todo: This. □

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

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

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 $\Lambda$ of weight $2k$:

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

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 $E_\Lambda$ is the curve in $\mathbb{P}^2_{\mathbb{C}}$ defined by the equation

$$y^2 = 4x^3 - g_2 x - g_3, \tag{4}$$

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

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

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

The curve defined in (4) is nonsingular 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 $\Lambda_1$ and $\Lambda_2$ be lattices in $\mathbb{C}$. Suppose $\alpha \in \mathbb{C}$ is such that $\alpha\Lambda_1 \subset \Lambda_2$. Then $\alpha$ defines a map $\phi_\alpha \colon \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ given by

$$\phi_\alpha(z + \Lambda_1) = \alpha z + \Lambda_2.$$

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 $\phi_\alpha$ are clearly holomorphic group homomorphisms.

**Proposition 3.2.1.** *Let $\Lambda_1$ and $\Lambda_2$ be lattices in $\mathbb{C}$ and let $E_{\Lambda_1}$ and $E_{\Lambda_2}$ be the corresponding elliptic curves given by* (4)*. Then $Hom(E_{\Lambda_1}, E_{\Lambda_2})$ is isomorphic to $\{\alpha \in \mathbb{C} \colon \alpha\Lambda_1 \subset \Lambda_2\}$.*

*Proof.* □

**Corollary 3.2.1.** *Let $\Lambda_1$ and $\Lambda_2$ be as above. Then the curves $E_{\Lambda_1}$ and $E_{\Lambda_2}$ are isomorphic if and only if $\Lambda_1$ is homothetic to $\Lambda_2$.*

From the general theory of elliptic curves we know that for any non-zero $d$ in an arbitrary field $k$ there exists an elliptic curve $E$ with discriminant $d$. When $k$ is the field of complex numbers there is a much stronger result, known as the *uniformisation thorem*, which states:

**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.* TODO: Reference Shimura. □

An obvious consequence of the uniformisation is the following corollary:

**Corollary 3.2.2.** *Let $E$ be an elliptic curve over $\mathbb{C}$.*

# 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 $o_k$ can be identified with $End(E)$. We will always use the following identification determined by the following commutative diagram (replacing $E$ by $E_\Lambda$ for some lattice $\Lambda$, which is possible by uniformisation):

$$\begin{array}{ccc} \mathbb{C}/\Lambda & \longrightarrow & \mathbb{C}/\Lambda \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f} \\ E_\Lambda & \longrightarrow & E_\Lambda \end{array} \tag{5}$$

where $f$ is the isomorphism described in (4). TODO: make this more clear and fix alignment.

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

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

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

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

A fractional ideal is principle 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.* TODO: make neat proof. □

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

TODO: intro.

**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 $E_{\mathfrak{a}}$:

$$End(E_{\mathfrak{a}}) \cong \{\alpha \in \mathbb{C} \colon \alpha\mathfrak{a} \subset \mathfrak{a}\} \quad \text{(by Proposition 3.2.1).}$$

Now, since $\mathfrak{a} \subset k$, any such $\alpha$ must be an element of $k$. But $\mathfrak{a}$ is a finitely generated $\mathfrak{o}_k$-submodule of $k$, so in fact $\alpha$ must be an element in $\mathfrak{o}_k$. Conversely, any element $\alpha$ 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 $\Lambda$ 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 $\Lambda$:

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

**Lemma 4.2.1.** *Suppose $\Lambda$ is such that the elliptic curve $E_\Lambda$ 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 squarefree 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. □

Suppose $\Lambda$ is a lattice such that $E_\Lambda$ 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 $E_\Lambda$ 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 $\mathfrak{a}^{-1}$ by convention. TODO: more on this.

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

*Proof.* TODO: this. □

**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 $\Lambda_1$ and $\Lambda_2$ be lattices in $\mathbb{C}$ such that the elliptic curves $E_{\Lambda_1}$ and $E_{\Lambda_2}$ have complex multiplication by $\mathfrak{o}_k$. Choose a non-zero element $\lambda_1$ in $\Lambda_1$ and consider the lattice $\mathfrak{a}_1 = \frac{a}{\lambda_1}\Lambda$. Let $(\omega_1, \omega_2)$ be a generating set for $\Lambda_1$ 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 $\lambda_2$ of $\Lambda_2$ 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 $E_{\Lambda_2}$ 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 $Cl(k)$. TODO: finish this. □

## 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 $\Lambda$ 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 $\phi_{\mathfrak{a}} : E_\Lambda \to E_\Lambda^{\mathfrak{a}}$ by (TODO: put in isogeny stuff in complex review):

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

**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* (5)*. 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 $\mathbb{Q}$

TODO: intro. nn nLet $E$ 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 $\sigma$ be a field automorphism of $\mathbb{C}$. We define $E^\sigma$ to be the elliptic curve obtained by letting $\sigma$ act on the coefficients of the equation of $E$, i.e. $E^\sigma$ 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

$$j(E^\sigma) = j(E)^\sigma \tag{6}$$

Now, if $\phi$ is an endomorphism of $E$, then $\phi$ 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 $\phi^\sigma$ of $E^\sigma$ in the obvious way:

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

Note that, if $(x\prime, y\prime)$ TODO: make this bit not messy.

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

$$End(E) \cong End(E^\sigma). \tag{7}$$

**Proposition 5.0.2.** *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 (6) and (7) 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 $\sigma$ is the restriction of an automorphism of $\mathbb{C}$. Thus, there are only finitely many such $\sigma$, so that $[\mathbb{Q}(j(E)) : \mathbb{Q}]$ is finite, which implies that $j(E)$ is algebraic over $\mathbb{Q}$. □

**Remark 5.0.1.** 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. TODO: give reference/do proof later.

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

*Proof.* By Proposition 5.0.2, 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 $\mathbb{Q}(j(E))$, given by the equation:

$$TODO. \tag{8}$$

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 5.0.1 says that the latter set, which is easily computed, will suit our purposes entirely.

## 5.1 Towards abelian extensions of quadratic imaginary fields

TODO: introduction.

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):

$$K_m = k(j(E), x_1, y_1, \ldots, x_r, y_r) \tag{9}$$

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

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

**Lemma 5.1.1.** *TODO: this.*

*Proof.* TODO: this. □

**Theorem 5.1.1.** *The field $K_m$ is an abelian extension of $k(j(E))$.*

*Proof.* We need to show that $K_m$ is a Galois extension of $k$, and its Galois group is abelian. Since $k$ is of characteristic zero, we only need to show that $\sigma(K_m) = K_m$ for any $K_m$-embedding $\sigma$. By Lemma 5.1.1 we know that $K_m$ is a finite extension of $k$, so any $K_m$-embedding is obtained from an element

$\sigma$ in $Gal(\bar{k}/k)$. Then by (TODO: fix reference), we have that $\sigma(x_i) = x_j$ and $\sigma(y_i) = y_j$ for all points $(x_i, y_i)$ in $E[m]$. So $K_m$ is a normal extension of $k$, and hence is Galois.

To see that $Gal(K_m/k)$ is abelian is more subtle. Recall the representation of $Gal(\bar{k}/k)$ given in (3):

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

We claim that $\rho$ 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 $\sigma$ is the identiy 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 $k(j(E))$ (by (8)), 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

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

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 5.1.1.** 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 $\mathbb{Q}(i)$

# References


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

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

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

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