Complex Multiplication on Elliptic Curves

Alexander Wertheim
Submitted for Graduation with Distinction:
Duke University Mathematics Department
Duke University
Durham, North Carolina
Advisor: Dr. Leslie Saper

April 24th, 2014

Abstract

We describe the theory of complex multiplication on elliptic curves as it pertains to constructing abelian extensions of imaginary quadratic fields. We also briefly explore how one may construct abelian extensions of real quadratic fields via an analogous theory termed real multiplication. Throughout, examples are computed.

Contents

Acknowledgments

I am deeply indebted to my mentor, Dr. Leslie Saper, for his tireless patience, support and guidance throughout this research project. I am additionally grateful to the PRUV program, headed by Dr. David Kraines, and in particular to Dr. Anita Layton, for supporting me. I would like to thank the Duke Mathematics department for the support, encouragement, and education which has made studying mathematics a fruitful and rewarding endeavor. Finally, I would like to thank my friends and family, and in particular my parents, for their love and support throughout my education at Duke.

1 Preliminaries: An Introduction to Elliptic Curves

In this section, we introduce elliptic curves from an algebraic perspective. In particular, we describe the group structure of rational points on elliptic curves, and derive explicit formulas for adding points. The exposition here relies deeply on Silverman and Tate. [1]

1.1 Cubic Curves and Elliptic Curves

Consider the general cubic curve C given by

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0 \tag{1}$$

We will say such a cubic is **rational** if the coefficients $a, b, \ldots, j$ are rational numbers. Similarly, we will call a point on C a **rational point** if its coordinates are rational numbers, and likewise for **real** and **complex** points if the coordinates are real and complex numbers, respectively. Equation (1) is a bit cumbersome; for the sake of convenience, it will be easier to work with cubic curves of the form

$$y^2 = f(x) = x^3 + ax^2 + bx^2 + c \tag{2}$$

where $a, b, c \in \mathbb{C}$.

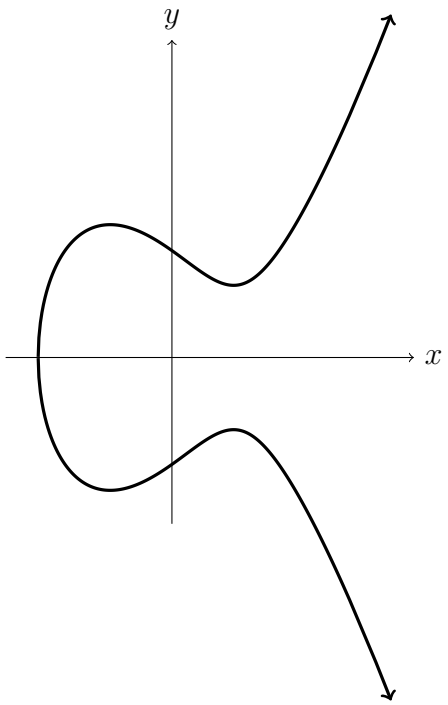


Figure 1: A cubic curve in Weierstrass form.

We say that cubics in the form of equation (2) are in **Weierstrass form**.[1] Electing to work with cubics in Weierstrass form is not a terribly restrictive choice. It is a well known

[1] Also sometimes referred to as **Weierstrass normal form**

result of projective geometry that if a general cubic curve C_1 of the form in equation (1) has a rational point, then it can be transformed rationally into a cubic curve C_2 of the form in equation (2), i.e. into Weierstrass form. C_1 and C_2 are said to be **birationally equivalent**, i.e. the coordinates on C_2 are given as rational functions of the coordinates on C_1, and so there is a natural correspondence between rational points on C_1 and rational points on C_2.[2]

If all complex roots of $f(x)$ in equation (2) are distinct, this special cubic curve is known as an **elliptic curve**, named for its appearance as the integrand in the calculation of arc lengths of ellipses. We note in passing that an alternative but equivalent version of Weierstrass form, which will be useful to us later, is

$$y^2 = 4x^3 + ax + b \tag{3}$$

While it is not immediately obvious, it is an exciting fact that there is a natural group structure on special subsets of points of an elliptic curve E. The special subsets of points, at least the ones we will be concerned with, are, namely, the rational, real, and complex points of E. This group structure can be motivated in particular by an old geometry problem: given a rational point on an elliptic curve E, can we obtain additional rational points on E? We will exclusively consider the problem of finding rational points on elliptic curves which we know have at least one rational point.

1.2 The Group of Rational Points on E

Let E be a nonsingular rational elliptic curve in Weierstrass form. Given a rational point on E, we might naturally wonder if there is a way to obtain additional rational points on E using the point that we start with. Projective geometry suggests a nice approach. Take two rational points on E and connect them to form a **rational line**, which will intersect E in one additional point.[3] These three intersection points appear algebraically as the solution to a cubic equation with rational coefficients. Since two of the known roots of this cubic, the x-coordinates of the two intersection points we started with, are rational, it follows that the third intersection point must also be rational. In other words, we have determined an additional rational point on E. This gives rise to a natural composition of points; namely, given two rational points P and Q on E, define $P \otimes Q$ to be the third point of intersection of the line connecting P and Q with E. If we start with just one rational point P, we can modify this idea accordingly. We compose P with P, i.e. we take the intersection point of the tangent line at P with E. The tangent line then meets E twice at P and hence, the intersection is of multiplicity two at P, and the third intersection point is rational by the previous argument. In this way, we can obtain many rational points on E starting with just one rational point on E. Denote the set of rational points on E by $E(\mathbb{Q})$ (likewise denote the set of real points on E by $E(\mathbb{R})$, and the set of complex points on E by $E(\mathbb{C})$). Clearly, $E(\mathbb{Q}) \subset E(\mathbb{R}) \subset E(\mathbb{C})$.

This composition operation $\otimes$ on $E(\mathbb{Q})$ seems to resemble a group law, but a few conditions are not satisfied. Under the composition operation $\otimes$, $E(\mathbb{Q})$ does not have an identity element, and a quick sketch on appropriately selected elements of $E(\mathbb{Q})$ shows that $\otimes$ is not

[2] With the exception of some points which may go to ∞.

[3] Assuming we include a point at infinity; more on this shortly

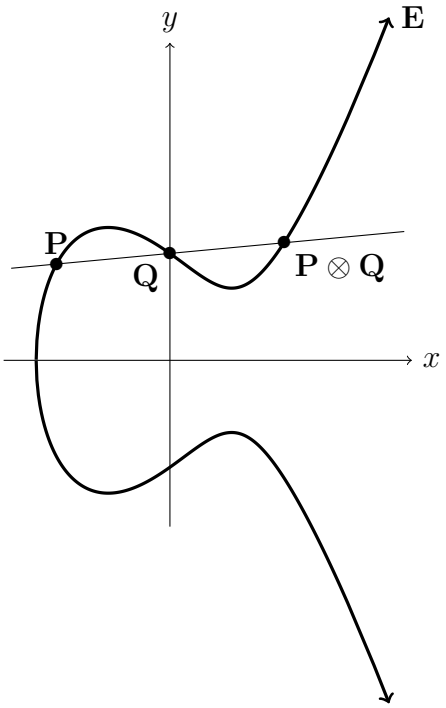


Figure 2: The composition operation $\otimes$ on E.

generally associative. We must modify our composition law if we would like $E(\mathbb{Q})$ to form a group.

Fortunately, with a small adjustment to the operation $\otimes$, we can make $E(\mathbb{Q})$ into a group. Let the given rational point on E be denoted by O. We describe our new operation $+$ geometrically as follows. Take rational points $P, Q \in E(\mathbb{Q})$ and join them in a line to get a third rational point $P \otimes Q$. Then, take $P \otimes Q$ and join it in a line with O to get a rational point $O \otimes (P \otimes Q)$. Now define $P + Q = O \otimes (P \otimes Q)$. We will show that this operation $+$ satisfies all the conditions require of a group composition law, demonstrating that $(E(\mathbb{Q}), +)$ is indeed a group. One may also note that this is an *abelian group*. The operation $\otimes$ is symmetric, as the line joining the line joining P and Q is the same as the line joining Q and P. Therefore, $P + Q = O \otimes (P \otimes Q) = O \otimes (Q \otimes P) = Q + P$, so $(E(\mathbb{Q}), +)$ is abelian.

Before we verify $(E(\mathbb{Q}), +)$ is a group, we have to take care of a few details concerning projective geometry. In particular, we must address two problems:

1) What happens when we add a rational point, P, and its reflection about the x-axis, P', together?

2) What is the identity under the group operation $+$?

To answer these questions, we need to move to the projective plane by switching to homogeneous coordinates. Starting with our equation for E given by equation (2), let us put E

in homogeneous form via the susbtitution $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$. We obtain

$$\frac{Y^2}{Z^2} = \frac{X^3}{Z^3} + a\frac{X^2}{Z^2} + b\frac{X}{Z} + c, \text{ or}$$

$$Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3$$

Among the solutions to the homogeneous cubic above, we only consider those with $(X, Y, Z) \neq \vec{0}$ and identify solutions that differ by a scalar multiple. We can determine the point at infinity by letting $Z = 0$. We see that substituting $Z = 0$ into this equation, we obtain $X^3 = 0$, which has a root at $X = 0$ of multiplicity three. E thus intersects the line at infinity $Z = 0$ with multiplicity three, so we have just one point at infinity. Geometrically, we can think of this point at infinity as the point at which the vertical lines in the affine xy plane meet. This is the point we will call the identity element O. By convention, we will take O as an element of $E(\mathbb{Q})$.

This convention simplifies the geometry of our group law considerably. Note from equation (2) that if (α, β) is a point on E, then $(\alpha, -\beta)$ is also a point on E. Thus, E is symmetric about the x-axis. To compute $P + Q$ for $P, Q \in E(\mathbb{Q})$, we must find $O \otimes (P \otimes Q)$. This is just the intersection of E with the vertical line through $P \otimes Q$, i.e. the reflection of $P \otimes Q$ about the x-axis. Since $P \otimes Q$ is rational, so is its reflection about the x-axis. Hence, $P + Q \in E(\mathbb{Q})$, and therefore $E(\mathbb{Q})$ is closed under addition.

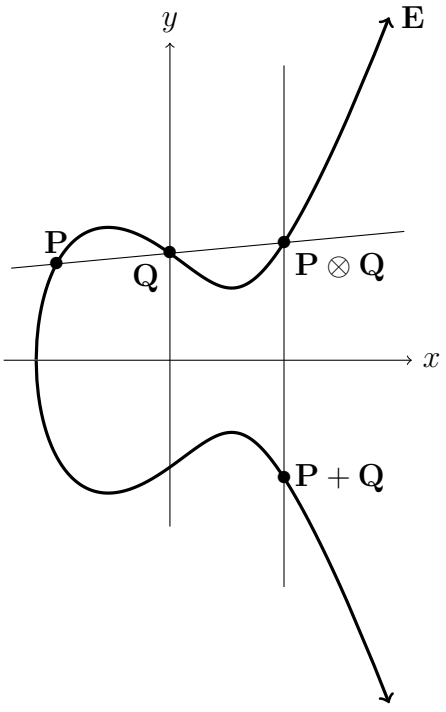


Figure 3: Addition of points on E.

We may also see that O is indeed the identity element, i.e. $P + O = O + P = P$. When we join P and O, we get the point of intersection $P \otimes O$, the reflection of P about the x-axis.

When we join $P \otimes O$ to O, the point of intersection with E is the reflection of $P \otimes O$ about the x-axis, i.e. P, so $P + O = P$.

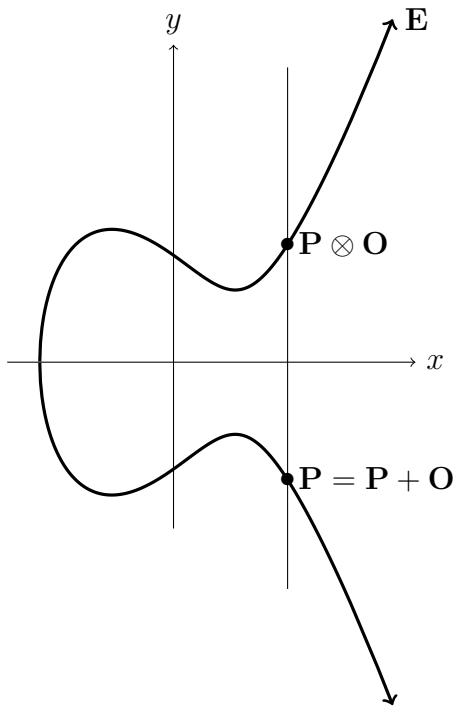


Figure 4: Verifying O is the identity element.

Verifying that O is the identity also establishes the inverse of a point P nicely. If we take a point $P = (x, y)$ and its reflection about the x-axis $(x, -y)$, the line joining these two points is vertical and intersects the cubic at O. The line joining O to O, that is, the tangent line at O, is $Z = 0$ which we have seen intersects E with multiplicity three. Hence, as $(x, y) + (x, -y) = O$, we have $-P = (x, -y)$. Since P was rational, it can easily be seen that $-P \in E(\mathbb{Q})$, and so $E(\mathbb{Q})$ is closed under taking inverses.

To finish proving that $(E(\mathbb{Q}), +)$ is a group, we must prove that the group law $+$ is associative. This is not prohibitively difficult, but can get messy quickly. For the sake of brevity, we defer proof of this fact to the appendix.

It is convenient to introduce the group operation using the problem of finding rational points as motivation, but none of the arguments we used were dependent on the fact that the underlying set of our group was $E(\mathbb{Q})$. The arguments given in fact apply equally well to $E(\mathbb{R})$ and $E(\mathbb{C})$. Hence, both $(E(\mathbb{R}), +)$ and $(E(\mathbb{C}), +)$ are groups; we will mostly be concerned later with $E(\mathbb{C})$.

Having proved that $E(\mathbb{Q})$ is a group, we come to the natural question of whether $E(\mathbb{Q})$ is finitely generated. The surprising answer to this question is yes, and this result was proved by Mordell in 1921. We conclude this section with the statement of Mordell's theorem.

Theorem 1.1 (Mordell, 1921)**.** *Let E be a non-singular cubic curve with rational coefficients. Then the group of rational points $E(\mathbb{Q})$ is a finitely generated abelian group.*

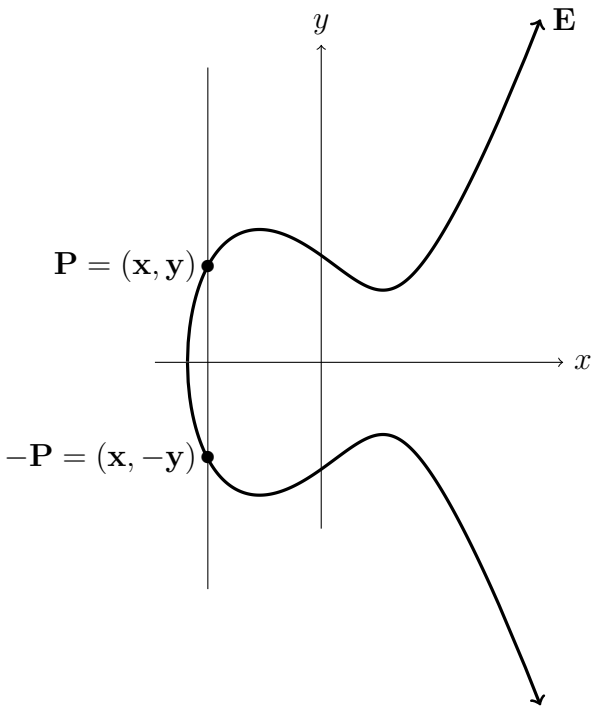


Figure 5: The negative of a point on E.

1.3 The Addition Formula

Having proven that $(E(\mathbb{Q}), +)$ is a group, we can develop an explicit formula for the group law. To make our task easier, let us introduce a bit of notation. Let $P_1, P_2 \in E(\mathbb{Q})$. Put $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$. Let $P_\times = P_1 \otimes P_2 = (x_3, y_3)$. From the discussion above, since $P_1 + P_2$ is equal to $P_\times$ reflected about the y-axis, it follows that $P_3 = P_1 + P_2 = (x_3, -y_3)$. We wish to explicitly compute P_3.

Denote the line through P_1 and P_2 by R. To compute the coordinates of $P_\times$, we need to compute the third point of intersection of R and E. First we compute the equation of the line R. Let

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \qquad \text{and} \qquad \sigma = y_1 - \lambda x_1 = y_2 - \lambda x_2. \tag{4}$$

Clearly, λ is the slope of R, and σ the y-intercept of R. Thus, the equation of this line R is given by $y = \lambda x + \sigma$. R intersects E at 3 points, P_1, P_2, and $P_\times$; since we know P_1 and P_2, we perform the following substitution into the equation for E to determine $P_\times$:

$$\begin{aligned} y^2 = (\lambda x + \sigma)^2 &= f(x) = x^3 + ax^2 + bx + c \\ \lambda x^2 + 2\lambda\sigma x + \sigma^2 &= x^3 + ax^2 + bx + c \\ x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\sigma)x + (c - \sigma^2) &= 0 \end{aligned}$$

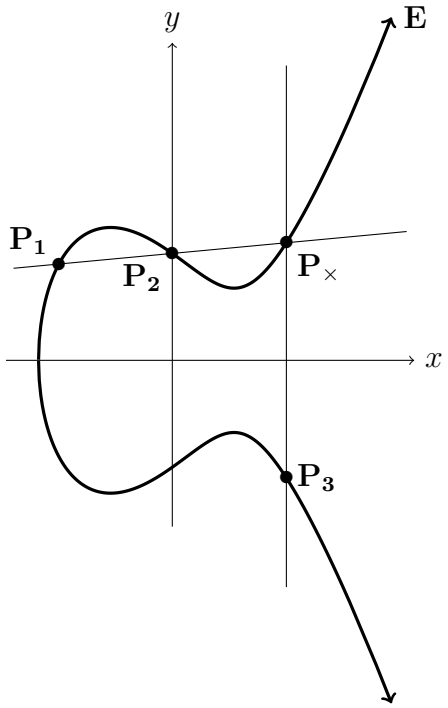


Figure 6: Developing a formula for the group law.

Let $g(x) = x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\sigma)x + (c - \sigma^2)$. We know that the roots of $g(x)$ are x_1, x_2, x_3, since they are the x-coordinates of the intersection points of R and E. We can factor $g(x)$ and set up the following equivalence to solve for x_3 by matching coefficients:

$$x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\sigma)x + (c - \sigma^2) = (x - x_1)(x - x_2)(x - x_3)$$
$$x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\sigma)x + (c - \sigma^2) = x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_1x_3 + x_2x_3)x - x_1x_2x_3$$

Hence, matching coefficients, we find:

$$x_3 = \lambda^2 - a - x_1 - x_2 \qquad \text{and} \qquad y_3 = \lambda x_3 + \sigma = \lambda(x_3 - x_1) + y_1 \tag{5}$$

Having determined $P_\times$, we can now compute $P_3 = (x_3, -y_3)$.

What if we wish to compute $P + P = 2P$ for $P = (x, y)$? In this case, we compute $P_\times$ as the intersection of the tangent line at P with E, so we must compute the slope of the tangent line at P, $\frac{dy}{dx}$. We do so by implicit differentiation:

$$\begin{aligned} y^2 = f(x) &= x^3 + ax^2 + bx + c \\ 2y\frac{dy}{dx} &= f'(x) \\ \frac{dy}{dx} &= \frac{f'(x)}{2y} \end{aligned}$$

Now, substitute in for λ in equation (5) to obtain the **duplication formula** for $2P = (x', y')$:

$$
\begin{aligned}
x' =& \lambda^2 - a - x - x \\
x' =& \frac{f'(x)^2}{4y^2} - a - 2x \\
x' =& \frac{(3ax^2 + 2bx + c)^2 - 4ay^2 - 2xy^2}{4y^2} \\
x' =& \frac{(3ax^2 + 2bx + c)^2 - 4a(x^3 + ax^2 + bx + c) - 2x(x^3 + ax^2 + bx + c)}{4(x^3 + ax^2 + bx + c)} \\
x' =& \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c}
\end{aligned}
$$

And of course, one can compute y' from equation (5) using $y' = -\lambda x' - \sigma$ as well:

$$
\begin{aligned}
y' =& \lambda(x - x') - y \\
y' =& \frac{x \cdot f'(x)}{2y} - \frac{f'(x)}{2y}\left(\frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4y^2}\right) - y \\
y' =& \frac{(4xy^2)(f'(x)) - (x^4 - 2bx^2 - 8cx + b^2 - 4ac)(f'(x)) - 8y^4}{8y^3}
\end{aligned}
$$

After some easily verifiable algebra, we obtain:

$$
y' = \frac{8a^2cx - 2ab^2x + 4abc + 20acx^2 + 2ax^5 - b^3 - 5b^2x^2 - 4bcx + 5bx^4 - 8c^2 + 20cx^3 + x^6}{8y^3}
$$

We note that in the process of duplication, the coordinates of $2P$ can be described completely in terms of rational functions of the coordinates of P and the coefficients of E. This fact will be important later in our study of isogenies.

2 Elliptic Functions: An Analytic Approach to Elliptic Curves

In the previous section, we explored the foundations of some of the exceptional algebraic properties of elliptic curves. We will now transition to a more analytic view of elliptic curves by considering a special class of functions known as **elliptic functions**. We will be primarily concerned with a special elliptic function, the Weierstrass $\wp$ function, which will help us show that an elliptic curve E is really a complex torus. This complex-analytic picture will be essential later in establishing the motivating foundations of complex multiplication. The material presented here closely follows the treatment given in Chapter 1 of Lang [2].

2.1 Properties of Elliptic Functions

In this first section, we will prove several important complex-analytic properties of elliptic functions. First, we must provide some important definitions.

Definition 2.1. *A* **lattice** L *in the complex plane* $\mathbb{C}$ *is a subgroup of* $\mathbb{C}$ *which is free of rank* 2 *over* $\mathbb{Z}$*, and generates* $\mathbb{C}$ *over the reals. If* ω_1, ω_2 *is a basis for* L*, we will write* $L = [\omega_1, \omega_2]$ *or*

$$L = a_1\omega_1 + a_2\omega_2 \qquad \textit{where} \qquad a_1, a_2 \in \mathbb{Z}$$

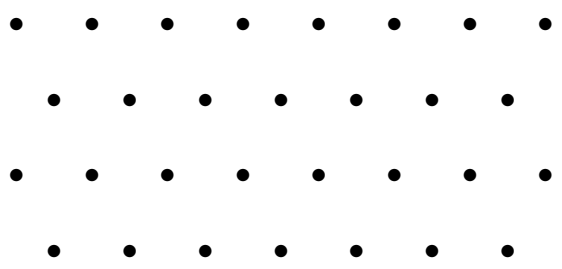


Figure 7: A lattice in $\mathbb{C}$.

Without loss of generality, we can assume that ω_1 and ω_2 are ordered such that $\mathrm{Im}(\omega_1/\omega_2) > 0$, i.e. $\omega_1/\omega_2 \in \mathbb{H}$, where $\mathbb{H}$ is the upper halfplane defined by $\mathbb{H} := \{a + bi \mid b > 0\}$.

We can now define precisely what we mean by an elliptic function.

Definition 2.2. *A* **elliptic** *function* f*, with respect to a lattice* $L = [\omega_1, \omega_2]$*, is a meromorphic function on* $\mathbb{C}$ *which is* L*-periodic, i.e.*

$$f(z) = f(z + \omega)$$

for all $z \in \mathbb{C}, \omega \in L$*.*

In other words, an elliptic function with respect to a lattice L is a function which is invariant under translation by elements of L. We can quickly prove the following useful proposition about elliptic functions.

Proposition 2.3. *A function f is periodic with respect to a lattice $L = [\omega_1, \omega_2]$ if and only if f is doubly periodic with respect to ω_1, ω_2, i.e.*

$$f(z + \omega_1) = f(z) = f(z + \omega_2)$$

for all $z \in \mathbb{C}$.

Proof. Suppose f is elliptic with respect to a lattice $L = [\omega_1, \omega_2]$. Then $f(z) = f(z + \omega)$ for all $z \in \mathbb{C}, \omega \in L$. Since $\omega_1, \omega_2 \in L$, we have $f(z + \omega_1) = f(z) = f(z + \omega_2)$.

Now suppose $f(z + \omega_1) = f(z) = f(z + \omega_2)$ for all $z \in \mathbb{C}$. We can see that $f(z - \omega_1) = f(z) = f(z - \omega_2)$, as

$$f(z) = f(z - \omega_1 + \omega_1) = f([z - \omega_1] + \omega_1) = f(z - \omega_1)$$

with an identical proof of the same fact for ω_2. Now we can use this to see that $f(z + k\omega_1) = f(z + k\omega_2)$ for any $k \in \mathbb{Z}$, as we inductively note that, for $k > 0$:

$$f(z + k\omega_1) = f([z + (k-1)\omega_1] + \omega_1) = f(z + (k-1)\omega_1) = \cdots = f(z + \omega_1) = f(z)$$

and for $k < 0$:

$$f(z + k\omega_1) = f([z + (k+1)\omega_1] - \omega_1) = f(z + (k+1)\omega_1) = \cdots = f(z - \omega_1) = f(z)$$

with an identical proof of the same fact for ω_2.
Since ω_1, ω_2 is a basis for L, we can write any element $\omega \in L$ as a $\mathbb{Z}$-linear combination of ω_1 and ω_2, i.e. there exist unique a_1 and a_2 in $\mathbb{Z}$ such that $\omega = a_1\omega_1 + a_2\omega_2$. Then we can see:

$$f(z + \omega) = f(z + a_1\omega_1 + a_2\omega_2) = f([z + a_1\omega_1] + a_2\omega_2) = f(z + a_1\omega_1) = f(z)$$

□

There is a more natural way to understand elliptic functions, using topology and geometry. Let $L = [\omega_1, \omega_2]$ be a lattice. If f is an elliptic function with respect to L, then f is meromorphic and invariant under translation by elements of L. Elliptic functions with respect to a given lattice L can therefore be seen as continuous functions on $\mathbb{C}/L$, where to form $\mathbb{C}/L$, we identify points in $\mathbb{C}$ which differ by an integer multiple of ω_1 plus an integer multiple of ω_2. Since this is the topological definition of a torus, $\mathbb{C}/L$ is in fact homeomorphic to a torus. Geometrically, this can be understood through the **fundamental parallelogram** for L (with respect to the basis ω_1, ω_1) defined by the set of points, where α is any element of $\mathbb{C}$:

$$P = \{\alpha + t_1\omega_1 + t_2\omega_2 | 0 \leq t_1, t_2 \leq 1\}$$

If we require strict inequality such that $t_1, t_2 < 1$, then we obtain unique equivalence class representatives of $\mathbb{C}/L$ in $\mathbb{C}$. If an elliptic function f is entire, then it must be constant; the homeomorphism between $\mathbb{C}/L$ and a torus tells us that $\mathbb{C}/L$ is compact, meaning f must be bounded and thus constant by Liouville's theorem.

With this in mind, we come to our first theorem on elliptic functions.

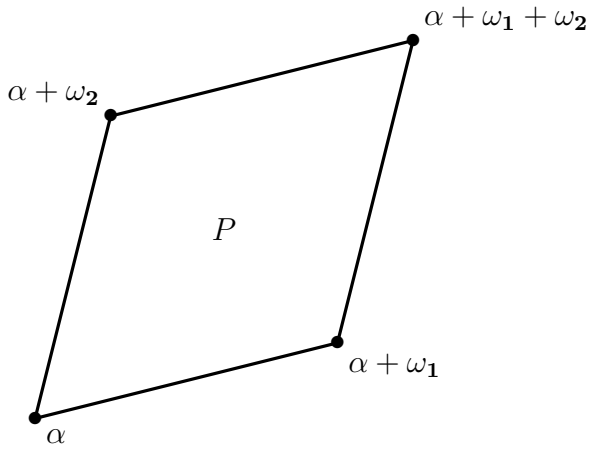


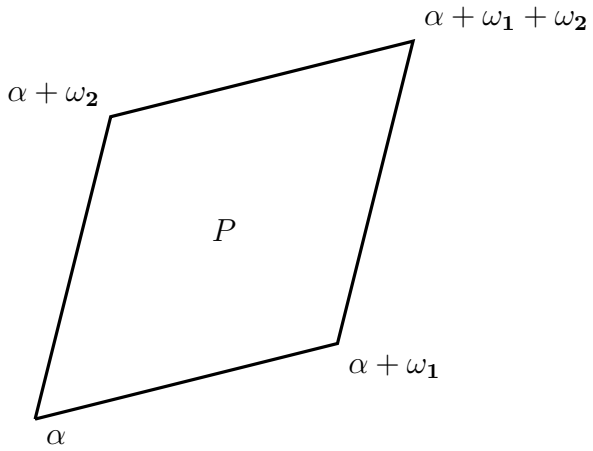
Figure 8: A fundamental parallelogram for $L = [\omega_1, \omega_2]$.

Theorem 2.4. *Let P be a fundamental parallelogram for a lattice L, and assume the elliptic function f has no poles on its boundary ∂P. Then the sum of the residues of f in P is 0.*

Proof. By the residue theorem, we have

$$2\pi i \sum \operatorname{Res} f = \int_{\partial P} f(z)dz$$

We can evaluate the right side of this equality as follows. Break up the integral into four sections by cutting the boundary of the fundamental parallelogram into each side.



Then, as we traverse the boundary ∂P counterclockwise, we obtain:

$$\begin{aligned}\int_{\partial P} f(z)dz &= \int_{\alpha}^{\alpha+\omega_1} f(z)dz + \int_{\alpha+\omega_1}^{\alpha+\omega_1+\omega_2} f(z)dz + \int_{\alpha+\omega_1+\omega_2}^{\alpha+\omega_2} f(z)dz + \int_{\alpha+\omega_2}^{\alpha} f(z)dz \\ &= \int_{\alpha}^{\alpha+\omega_1} f(z)dz + \int_{\alpha+\omega_1}^{\alpha+\omega_1+\omega_2} f(z)dz - \int_{\alpha+\omega_2}^{\alpha+\omega_1+\omega_2} f(z)dz - \int_{\alpha}^{\alpha+\omega_2} f(z)dz\end{aligned}$$

But by the periodicity of f, $f(z)$ takes the same values on the boundary from α to $\alpha+\omega_1$ as it does from $\alpha+\omega_2$ to $\alpha+\omega_1+\omega_2$; similarly, $f(z)$ takes the same values on the boundary from α to $\alpha+\omega_2$ as it does from $\alpha+\omega_1$ to $\alpha+\omega_1+\omega_2$. Hence,

$$\int_{\partial P} f(z)dz = \left(\int_{\alpha}^{\alpha+\omega_1} f(z)dz - \int_{\alpha+\omega_2}^{\alpha+\omega_1+\omega_2} f(z)dz\right)+\left(\int_{\alpha+\omega_1}^{\alpha+\omega_1+\omega_2} f(z)dz - \int_{\alpha}^{\alpha+\omega_2} f(z)dz\right) = 0$$

and thus

$$2\pi i \sum \operatorname{Res} f = \int_{\partial P} f(z)dz = 0$$

□

Viewing an elliptic function as a meromorphic continuous function on the torus $\mathbb{C}/L$, we obtain the following immediate corollary.

Corollary 2.5. *A non-constant elliptic function has at least two poles (counting multiplicity) on the torus.*

If we start with an elliptic function f with respect to a lattice $L = [\omega_1, \omega_2]$, can we use f to generate more elliptic functions? Clearly, cf for any scalar $c \in \mathbb{R}$ is elliptic with the same periods. We can yet say more, however, and do so in the following proposition.

Proposition 2.6. *Let f be an elliptic function with respect to a lattice $L = [\omega_1, \omega_2]$. Then f' and $\frac{f'}{f}$ are also elliptic with respect to L.*

Proof. Since f is elliptic, f is meromorphic and hence has a unique Laurent series representation about any c:

$$f(z) = \sum_{n=k}^{\infty} a_n (z-c)^n$$

Since f is meromorphic, this expansion has countably many poles. By differentiating the Laurent series expansion for f, f' must also have countably many poles. Thus, f' must therefore be meromorphic as well. We then note

$$f'(z) = \lim_{h\to 0} \frac{f(z+h)-f(z)}{h} = \lim_{h\to 0} \frac{f([z+h]+\omega)-f(z+\omega)}{h} = f'(z+\omega)$$

for all $\omega \in L$. So f' is elliptic with respect to L. Recall that meromorphic functions form a field, so $\frac{f'}{f}$ is meromorphic. Now as shown above, f' and f are both L-periodic, so letting $g(z) = \frac{f'(z)}{f(z)}$, we find:

$$g(z) = \frac{f'(z)}{f(z)} = \frac{f'(z+\omega)}{f(z)} = \frac{f'(z+\omega)}{f(z+\omega)} = g(z+\omega)$$

for all $\omega \in L$. So $\frac{f'}{f}$ is meromorphic and L-periodic. Hence, $\frac{f'}{f}$ is elliptic with respect to L. □

In proving $\frac{f'}{f}$ was elliptic, all we needed was that $\frac{f'}{f}$ was meromorphic and that f' and f are both L-periodic. We can generalize this in the immediate corollary.

Corollary 2.7. *Let f and g be two elliptic functions with respect to some lattice $L = [\omega_1, \omega_2]$, with g nonzero. Then $f \pm g, f \cdot g, \frac{f}{g}$ are all elliptic with respect to L. Hence, the set of elliptic functions with respect to a lattice L forms a field.*

Proof. Since the meromorphic functions form a field, we immediately have that $f \pm g, f \cdot g, \frac{f}{g}$ are all meromorphic. For any $\omega \in L$, we have:

$$(f \pm g)(z) = f(z) \pm g(z) = f(z+\omega) \pm g(z) = f(z+\omega) \pm g(z+\omega) = (f \pm g)(z+\omega)$$

$$(f \cdot g)(z) = f(z) \cdot g(z) = f(z+\omega) \cdot g(z) = f(z+\omega) \cdot g(z+\omega) = (f \cdot g)(z+\omega)$$

$$\left(\frac{f}{g}\right)(z) = \frac{f(z)}{g(z)} = \frac{f(z+\omega)}{g(z)} = \frac{f(z+\omega)}{g(z+\omega)} = \left(\frac{f}{g}\right)(z+\omega)$$

So $f \pm g, f \cdot g, \frac{f}{g}$ are all elliptic with respect to L. The remaining field axioms follow from the properties of functions. □

Using proposition 2.6, we can prove a useful theorem about the orders of the singular points of elliptic functions.

Theorem 2.8. *Let P be a fundamental parallelogram, and assume that the elliptic function f has no zero or pole on its boundary. Let $\{a_i\}$ be the singular points (zeros and poles) of f inside P, and let f have order m_i at a_i. Then*

$$\sum m_i = 0.$$

Proof. We use a clever trick. By Proposition 2.6, note that $\frac{f'}{f}$ is elliptic. Note that the residues of $\frac{f'}{f}$ are the orders of the singular points of f. Hence, by theorem 2.4, we find:

$$\int_{\partial P} \frac{f'}{f}(z)dz = 2\pi i \sum \operatorname{Res} \frac{f'}{f} = 2\pi i \sum m_i = 0$$

and thus,

$$\sum m_i = 0$$

□

2.2 The Weierstrass $\wp$ Function

We will now introduce the most important elliptic function of study in these notes, the Weierstrass $\wp$ function, defined as follows:

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in L'} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right]$$

where L' is the set of all nonzero elements of a lattice $L = [\omega_1, \omega_2]$. For us to show $\wp(z)$ is elliptic, we must first show $\wp(z)$ is uniformly convergent on compact sets not including lattice points, which are singularities.

Lemma 2.9. *Let M be any compact set not including any point of L. Then $\wp(z)$ is uniformly convergent (and hence analytic) on M.*

Proof. Since M is compact, $|z|$ is bounded; let $R \in \mathbb{R}$ such that $|z| \leq R$. Then, we can see:

$$\sum_{\omega \in L'} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right] = \sum_{|\omega|<2R} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right] + \sum_{|\omega| \geq 2R} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right]$$

Since L is a discrete set of points, the first sum is finite. Hence, it suffices to show that

$$\sum_{|\omega| \geq 2R} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right]$$

uniformly converges. As the magnitude of $|z|$ is bounded:

$$\begin{aligned}
\left| \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right| &= \left| \frac{\omega^2 - (z-\omega)^2}{(z-\omega)^2 \omega^2} \right| \\
&= \left| \frac{z^2 - 2\omega z}{(z-\omega)^2 \omega^2} \right| \\
&\leq \frac{|z^2| + 2|\omega||z|}{|(z-\omega)^2||\omega^2|} \quad \text{by the Triangle inequality} \\
&\leq \frac{R^2 + 2|\omega|R}{|(z-\omega)|^2 |\omega|^2} \quad \text{because } |z| \leq R \\
&\leq \frac{\frac{5}{2}|\omega|R}{|\omega|^2 |\omega|^2} \quad \text{because } |z| \leq 2R \leq |\omega| \text{ and } |z-\omega|^2 \geq |\omega|^2 \\
&= \frac{5R}{2|\omega|^3}
\end{aligned}$$

Thus, we must show

$$\sum_{|\omega| \geq 2R} \frac{1}{|\omega|^3}$$

uniformly converges. But we can do this by decomposing the partial sum for $|w| \leq N$ further into partial sums in annuli for each n; note that in each annulus $n-1 \leq |\omega| \leq n$, the number of lattice points has roughly order n. Take $\lambda > 2$. Then, where C is a constant for estimating the number of lattice points and replacing $n-1$ by n as needed, we have

$$\sum_{|\omega|} \frac{1}{|\omega|^\lambda} < C \sum_{1}^{\infty} \frac{n}{n^\lambda} = C \sum_{1}^{\infty} \frac{1}{n^{\lambda-1}}$$

which is uniformly convergent. If we let $\lambda = 3$, this completes the proof. □

We need to show that $\wp$ is elliptic, i.e. we must prove that $\wp(z)$ is meromorphic and L-periodic. The series expansion of $\wp(z)$ clearly shows that $\wp(z)$ has a double pole at each

lattice point, with no other poles. Hence, $\wp(z)$ has countably many poles, and is therefore meromorphic. Now we will show that $\wp$ is L-periodic. Note that $\wp(z)$ is even, as

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in L'} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right] = \frac{1}{(-z)^2} + \sum_{\omega \in L'} \left[\frac{1}{((-z)-\omega)^2} - \frac{1}{\omega^2} \right] = \wp(-z)$$

Differentiating term by term, we can find $\wp'(z)$:

$$\begin{aligned} \wp'(z) =& \left(\frac{1}{z^2} \right)' + \sum_{\omega \in L'} \left[\left(\frac{1}{(z-\omega)^2} \right)' - \left(\frac{1}{\omega^2} \right)' \right] \\ =& \frac{-2}{z^3} + \sum_{\omega \in L'} \frac{-2}{(z-\omega)^3} \\ =& \sum_{\omega \in L} \frac{-2}{(z-\omega)^3} \end{aligned}$$

We can see $\wp'(z)$ is odd, as

$$\wp'(z) = \sum_{\omega \in L} \frac{-2}{(z-\omega)^3} = \sum_{\omega \in L} \frac{2}{((-z)+\omega)^3} = \sum_{\omega \in L} \frac{2}{((-z)-\omega)^3} = -\wp'(-z)$$

We can also note that $\wp'(z)$ is periodic with respect to L. Fix $\omega' \in L$. We evaluate

$$\wp'(z+\omega') = \sum_{\omega \in L} \frac{-2}{(z-(\omega+\omega'))^3} = \sum_{\omega+\omega', \omega \in L} \frac{-2}{(z-\omega)^3}$$

Hence $\wp(z+\omega') = \wp(z)$ if and only if the map $\omega \mapsto \omega+\omega'$ is a bijection on L. This is true, as the map is invertible. Hence, $\wp'(z)$ is L-periodic. Since $\wp'(z)$ is L-periodic, $\wp'(z+\omega') = \wp'(z)$, and so, integrating both sides, we find:

$$\wp(z+\omega') = \wp(z) + C$$

for some constant C. Now, let $z = \frac{-\omega'}{2}$. Plugging in, this gives us

$$\wp(\frac{\omega'}{2}) = \wp(\frac{-\omega'}{2}) + C$$

Using the fact that $\wp(z)$ is even, we conclude $C = 0$. Since $\omega' \in L$ was arbitrary, we have that $\wp(z)$ is L-periodic. So $\wp(z)$ is elliptic.

2.3 Elliptic Curves as Complex Tori

We will now make the connection between elliptic curves and elliptic functions clear. In particular, we will use the Weierstrass $\wp$ function to construct an isomorphism between complex points on an elliptic curve E and $\mathbb{C}/L$ for some lattice L, showing that an elliptic curve E can be viewed as a complex torus. The ability to understand elliptic curves from

this analytic point of view has many rich consequences. Notably, it will be exceptionally valuable in our study of points of finite order on elliptic curves in §3.2.

The claim that elliptic curves are really complex tori might seem suspicious. Moreover, the series representation of $\wp(z)$ makes its relevance a bit opaque. To begin, we will develop power series expansions for $\wp(z)$ and $\wp'(z)$, which we will use to demonstrate an algebraic relationship between $\wp(z)$ and $\wp'(z)$.

$$\begin{aligned}
\wp(z) =& \frac{1}{z^2} + \sum_{\omega \in L'} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right] \\
=& \frac{1}{z^2} + \sum_{\omega \in L'} \left[\frac{1}{\omega^2} \left(1 + \frac{z}{\omega} + \left(\frac{z}{\omega} \right)^2 + \cdots \right)^2 - \frac{1}{\omega^2} \right] \quad \text{using the power series for } \frac{1}{(z-\omega)^2} \\
=& \frac{1}{z^2} + \sum_{\omega \in L'} \sum_{m=1}^{\infty} (m+1) (\frac{z}{\omega})^m \frac{1}{\omega^2} \quad \text{via the binomial expansion}
\end{aligned}$$

Using the notation

$$c_m = \sum_{\omega \in L'} \frac{(m+1)}{\omega^{m+2}} \qquad \text{and} \qquad s_m(L) = s_m = \sum_{\omega \in L'} \frac{1}{\omega^m}$$

we can rewrite $\wp(z)$ as follows:

$$\wp(Z) = \frac{1}{z^2} + \sum_{m=1}^{\infty} c_m z^m$$

Note that since $\omega \in L'$ implies $-\omega \in L'$, $c_m = 0$ if m is odd. Hence, we finally arrive at the following series expansion, which we can use to explicitly write out the first few terms:

$$\begin{aligned}
\wp(z) =& \frac{1}{z^2} + \sum_{n=1}^{\infty} c_{2n} z^{2n} = \frac{1}{z^2} + \sum_{n=1}^{\infty} (2n+1) s_{2n+2} z^{2n} \\
=& \frac{1}{z^2} + 3s_4 z^2 + 5s_6 z^4 + \cdots
\end{aligned}$$

If we differentiate term by term, we can obtain a similar series expansion for $\wp'(z)$, for which the first few terms are:

$$\wp'(z) = \frac{-2}{z^3} + 6s_4 z + 20 s_6 z^3 + \cdots$$

This is just what we need to complete our discussion.

Theorem 2.10. *Let $g_2 = 60 s_4$ and $g_3 = 140 s_6$. Then $\wp(z)$ satisfies the following differential equation:*

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

Proof. We will proceed by showing that the function

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

is constant, and 0 at the origin, thus proving the theorem. To do so, we expand out, keeping track of the polar and constant terms:

$$\begin{aligned}
\varphi(z) =& \wp'(z)^2 - 4\wp(z)^3 + g_2\wp(z) + g_3 \\
=& \left[\left(\frac{-2}{z^3} + 6s_4 z + 20 s_6 z^3 + \cdots \right)^2 - 4 \left(\frac{1}{z^2} + 3s_4 z^2 + 5 s_6 z^4 + \cdots \right)^3 + \right. \\
& \left. 60 s_4 \left(\frac{1}{z^2} + 3 s_4 z^2 + 5 s_6 z^4 + \cdots \right) + 140 s_6 \right] \\
=& \left(\frac{4}{z^6} - \frac{24 s_4}{z^2} - 80 s_6 + \cdots \right) - 4 \left(\frac{1}{z^6} + \frac{9 s_4}{z^2} + 15 s_6 \right) + 60 s_4 \left(\frac{1}{z^2} + \cdots \right) + 140 s_6 \\
=& k(z), \text{ where } k(z) \text{ is an infinite sum of positive powers of } z
\end{aligned}$$

Since $\varphi(z)$ is a sum of powers of elliptic functions with respect to the same lattice L, by corollary 2.7 $\varphi(z)$ is elliptic with respect to L too. But $\varphi(z)$ has no poles, so it must be constant, and since $\varphi(0) = 0$, our theorem is proved. □

We have thus shown that the points $(\wp(z), \wp'(z))$ are solutions to the curve E defined by

$$E\colon y^2 = 4x^3 - g_2 x - g_3 \tag{6}$$

It can be shown that the roots of $4x^3 - g_2 x - g_3$ are distinct. Hence, recalling §1.1, we may conclude that the set of points $\{(\wp(z), \wp'(z)) \mid z \in \mathbb{C} - L\}$ are the finite complex points on an elliptic curve E. If we add in the poles of $\wp(z)$ and $\wp'(z)$, then we get the point at infinity on E.

Letting $P(z) = (\wp(z), \wp'(z))$ for $z \in \mathbb{C}$ allows us to define a map from $\mathbb{C}$ to $E(\mathbb{C})$:

$$\begin{aligned}
\delta\colon \mathbb{C} &\to E(\mathbb{C}) \\
z &\mapsto \begin{cases} P(z) & \text{if } z \notin L \\ O & \text{if } z \in L \end{cases}
\end{aligned}$$

One can show δ is a homomorphism, and we can see that $\ker(\delta)$ consists precisely of points on the period parallelogram, i.e. points on the lattice L. Thus, by the first isomorphism theorem, we obtain the isomorphism

$$\mathbb{C}/L \cong E(\mathbb{C})$$

In other words, we have shown that E can be thought of as a complex torus. Having uncovered this isomorphism, we will have much more to say about its importance later in §3.2.

2.4 Elliptic Curves up to Isomorphism over $\mathbb{C}$

We will be more interested in isomorphism classes of elliptic curves[4] than with particular elliptic curves themselves. It is therefore natural to consider when two elliptic curves isomorphic. The complex-analytic view of an elliptic curve developed in the previous section

[4]In particular, $\mathbb{C}$-isomorphism classes of elliptic curves

provides valuable insight. In particular, if we have two elliptic curves E_1 and E_2 such that $E_1(\mathbb{C}) \cong \mathbb{C}/L_1$ for a lattice L_1 and $E_2(\mathbb{C}) \cong \mathbb{C}/L_2$ for a lattice L_2, then it suffices to consider when $\mathbb{C}/L_1 \cong \mathbb{C}/L_2$.

It can be shown that two complex tori $\mathbb{C}/L_1$ and $\mathbb{C}/L_2$ are isomorphic if and only if there exists $\alpha \in \mathbb{C}^\times$ such that $\alpha L_1 = L_2$. The lattices L_1 and L_2 are said to be **homothetic** if this is the case, and the corresponding isomorphism between $\mathbb{C}/L_1$ and $\mathbb{C}/L_2$ is multiplication by α. We will get an idea of why this condition for isomorphism is true in §3.3, when we introduce complex multiplication, but for now we accept this as true and build off of it. Hence, two elliptic curves are isomorphic if and only if their underlying lattices are homothetic.

Let $L = [\omega_1, \omega_2]$ be a lattice. Put $\tau = \frac{\omega_1}{\omega_2}$. One fact we immediately observe is that L is homothetic to the lattice $L_\tau = [\tau, 1]$, since $L = \omega_2 L_\tau$. Furthermore, we may assume $\mathrm{Im}(\tau) > 0$, since we can always order the basis for L so that this is true. Hence, each τ in the upper half-plane $\mathbb{H}$ can be associated with a $\mathbb{C}$-isomorphism class of elliptic curves via the lattice $L_\tau = [\tau, 1]$. From here on, we concern ourselves exclusively with elliptic curves E such that $E(\mathbb{C}) \cong \mathbb{C}/L_\tau$ for some $\tau \in HH$.

What we have seen so far is useful, but it would be better if we could could understand isomorphism between two elliptic curves E_1 and E_2 directly via the Weierstrass equations of E_1 and E_2. We have seen that information about a complex torus $\mathbb{C}/L$ can be translated into information about the corresponding elliptic curve E via the Weierstrass $\wp$ function. Isomorphism between elliptic curves has been phrased in terms of homothety of lattices thusfar. Since the $\wp(z)$ is really a function of z and a lattice L, we are thus interested in how $\wp(z)$ changes over homothetic lattices.

We can observe the following homogeneity property of $\wp(z)$ and $\wp'(z)$ respectively. For any $c \in \mathbb{C}^\times$,

$$\wp(cz, cL) = \frac{1}{(cz)^2} + \sum_{\omega \in cL'} \left[\frac{1}{(cz-\omega)^2} - \frac{1}{\omega^2} \right] = \frac{1}{c^2}\frac{1}{z^2} + \sum_{\omega \in L'} \left[\frac{1}{c^2}\frac{1}{(z-\omega)^2} - \frac{1}{c^2}\frac{1}{\omega^2} \right] = c^{-2}\wp(z, L)$$

$$\wp'(cz, cL) = \sum_{\omega \in cL} \frac{-2}{(cz-\omega)^3} = \sum_{\omega \in L} \frac{-2}{(cz-c\omega)^3} = \frac{1}{c^3} \sum_{\omega \in L} \frac{-2}{(z-\omega)^3} = c^{-3}\wp'(z, L)$$

Consider the quantities g_2 and g_3 defined in §2.3. These too are functions of a lattice L, and also have important homogeneity properties. For any $c \in \mathbb{C}^\times$,

$$g_2(cL) = 60 s_4 = 60 \sum_{\omega \in cL'} \frac{1}{\omega^4} = \frac{60}{c^4} \sum_{\omega \in L'} \frac{1}{\omega^4} = c^{-4} g_2(L)$$

$$g_3(cL) = 140 s_6 = 140 \sum_{\omega \in cL'} \frac{1}{\omega^4} = \frac{60}{c^6} \sum_{\omega \in L'} \frac{1}{\omega^6} = c^{-6} g_3(L)$$

Let E_1 and E_2 be isomorphic elliptic curves, where $E_1(\mathbb{C}) \cong \mathbb{C}/L_1$ and $E_2(\mathbb{C}) \cong \mathbb{C}/L_2$; denote the isomorphism between E_1 and E_2 by λ. Then lattices L_1 and L_2 are homothetic, so there is a $c \in \mathbb{C}^\times$ such that $L_1 = cL_2$. Moreover $\mathbb{C}/L_1$ and $\mathbb{C}/L_2$ are isomorphic via the map $z \mapsto cz$; call this map σ. By the isomorphism developed in §2.3, for $z \notin L_1$, the x and y-coordinates of points in $E_1(\mathbb{C})$ are given by $\wp(z, L_1)$ and $\wp'(z, L_1)$ respectively. Similarly,

for $z \notin L_2$, the x and y-coordinates of points in $E_2(\mathbb{C})$ are given by $\wp(z, L_2)$ and $\wp'(z, L_2)$ respectively. Let $x_1(P), y_1(P)$ be the x and y-coordinate respectively of a point $P \in E_1$. Let $x_2(P'), y_2(P')$ be defined similarly for a point $P' \in E_2$. Let $P = (\wp(\alpha), \wp'(\alpha)) \in E_1$. The respective homogeneity properties of $\wp(z)$ and $\wp'(z)$ tell us

$$x_2(\lambda(P)) = \wp(\sigma(\alpha), L_2) = \wp(c\alpha, cL_1) = c^{-2}\wp(\alpha, L_1) = c^{-2}x_1(P)$$

$$y_2(\lambda(P)) = \wp'(\sigma(\alpha), L_2) = \wp'(c\alpha, cL_1) = c^{-3}\wp(\alpha, L_1) = c^{-3}y_1(P)$$

Hence, we have proved the following proposition.

Proposition 2.11. *Suppose that E_1, E_2 are elliptic curves with Weierstrass equations*

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

and

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

respectively. Let $\lambda : E_1 \to E_2$ be an isomorphism defined over k. Then there exists $c \in \mathbb{C}^\times$ such that

$$g_2' = c^4 g_2, \quad g_3 = c^6 g_3$$

and if the points $(x_1, y_1) \in E_1$ and $(x_2, y_2) \in E_2$ correspond under λ, then

$$x_2 = c^2 x_1 \text{ and } y_2 = c^3 y_1$$

This proposition motivates the introduction of a useful invariant of elliptic curves, the **j-invariant**, defined for an elliptic curve E_1 by:

$$j(E_1) = 1728\frac{g_2^3}{g_2^3 - 27g_3^2}$$

One can see from Proposition 2.11 that if E_1 and E_2 are isomorphic elliptic curves, then $j(E_1) = j(E_2)$. In fact, one can show that the converse is also true, so that two elliptic curves are isomorphic if and only if they have equal j-invariants. Thus, $\mathbb{C}$-isomorphism classes of elliptic curves can be uniquely characterized by the j-invariant of a representative element.

3 A Motivating Example: Constructing Abelian Extensions of $\mathbb{Q}(i)$

In this section, we use complex multiplication on elliptic curves to construct abelian extensions of $\mathbb{Q}(i)$, following the treatment given in Silverman and Tate [1]. This example will provide the motivation and groundwork for the next section, where we take a more high level view of complex multiplication on elliptic curves. We will assume working knowledge of basic Galois theory, and hence will not say much about Galois theory beyond a few definitions and the statement of a few key theorems. For an excellent resource on Galois theory, see *Abstract Algebra* by Dummit and Foote [8], chapters 13 and 14.

3.1 Constructing Abelian Extensions of $\mathbb{Q}$

We begin with some important definitions.

Definition 3.1. *Let K/F be a field extension. Denote the set of all field automorphisms of K fixing F by $\mathrm{Gal}(K/F)$. We say that $\mathrm{Gal}(K/F)$ is the* **Galois group of** *K/F.*

Definition 3.2. *Let K/F be a field extension. We say that K/F is an abelian extension if $\mathrm{Gal}(K/F)$ is abelian.*

Our goal in this section will be to construct abelian extensions of $\mathbb{Q}$, to see how we might analagously construct abelian extensions of $\mathbb{Q}(i)$. Before we do so, we will need just one more definition and one more lemma.

Definition 3.3. *Let $K/\mathbb{Q}$ be a field extension with $\mathbb{Q} \subset K \subset \mathbb{C}$. If every nontrivial field homomorphism*

$$\sigma \colon K \hookrightarrow \mathbb{C}$$

is an automorphism of K, then we say that K is a **Galois extension of $\mathbb{Q}$.**

Lemma 3.4. *Let $K/\mathbb{Q}$ be a field extension. Then K is a Galois extension of $\mathbb{Q}$ if and only if K is the splitting field of a separable polynomial $f(x) \in \mathbb{Q}[x]$.*

Armed with these definitions, we wish to construct abelian extensions of $\mathbb{Q}$. The natural objects to study are cyclotomic fields. **Cyclotomic fields** are fields generated by primitive n^{th} roots of unity, or elements of order n in $(\mathbb{C})^\times$. Denote a primitive n^{th} root of unity by ζ_n, and consider the polynomial $f(x) = x^n - 1 \in \mathbb{Q}[x]$. Cyclotomic field theory tells us that $\mathbb{Q}(\zeta_n)$ is the splitting field of $f(x)$. To see this, note that the complex roots of $f(x)$ are precisely elements of order dividing n in $(\mathbb{C})^\times$. Elements of order dividing n in $\mathbb{C}^\times$ are, in fact powers of ζ_n; the roots of $f(x)$ are therefore the elements of $\langle \zeta_n \rangle$. Since $\mathbb{Q}(\zeta_n)$ is the smallest field extension of $\mathbb{Q}$ containing $\langle \zeta_n \rangle$, it is the splitting field of $f(x)$ and thus a Galois extension of $\mathbb{Q}$ by Lemma 3.4.[5]

One might correctly guess that we are going to show that $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is abelian. To prove this, we will identify a one-to-one homomorphism from $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ into an abelian group, demonstrating that $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is abelian.

[5]Since $\gcd(f(x), f'(x)) = \gcd(x^n - 1, nx^{n-1}) = 1$, it follows that $f(x)$ is separable. See [8] for more on this.

We start by determining the elements of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Since any automorphism $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ must fix $\mathbb{Q}$, the map σ is completely determined by the value of $\sigma(\zeta_n)$. Furthemore, since σ is an automorphism, $\sigma(\zeta_n)$ must also be of order n in $(\mathbb{C})^\times$. In other words, $\sigma(\zeta_n)$ must be another primitive n^{th} root of unity. Precisely, we must have $\sigma(\zeta_n) = \zeta_n^m$ for some $m \in \mathbb{N}$ relatively prime to n.

This allows us to define a map f from $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ into the group of integers relatively to prime to n, $(\mathbb{Z}/n\mathbb{Z})^\times$, by setting $f(\sigma) = m$ if $\sigma(\zeta_n) = \zeta_n^m$. We write this formally as:

$$\begin{aligned} f\colon \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) &\to (\mathbb{Z}/n\mathbb{Z})^\times, \text{where} \\ \sigma(\zeta_n) = \zeta_n^{f(\sigma)} \quad &\text{for} \quad \sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \end{aligned}$$

We claim that f is an injective homomorphism. That f is injective is clear: if $f(\sigma) = f(\tau)$ for some $\sigma, \tau \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, it follows that $\sigma(\zeta_n) = \tau(\zeta_n)$. Since any element of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is determined by where it maps ζ_n, it follows that $\sigma = \tau$. We can show that f is a homomorphism as follows. Let $\sigma, \tau \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Then:

$$\begin{aligned} \zeta_n^{f(\sigma\tau)} &= \sigma\tau(\zeta_n) \\ &= \sigma(\tau(\zeta_n)) \quad \text{by associativity} \\ &= \sigma(\zeta_n^{f(\tau)}) \\ &= (\sigma(\zeta_n))^{f(\tau)} \quad \text{since } \sigma \text{ is an automorphism} \\ &= (\zeta_n^{f(\sigma)})^{f(\tau)} \\ &= \zeta_n^{f(\sigma)f(\tau)} \end{aligned}$$

Hence, f is a one-to-one homomorphism. Since $(\mathbb{Z}/n\mathbb{Z})^\times$ is abelian, $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is also abelian as desired. This can also be seen directly, as for $\sigma, \tau \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, we have:

$$\sigma\tau(\zeta_n) = \zeta_n^{f(\sigma\tau)} = \zeta_n^{f(\sigma)f(\tau)} = \zeta_n^{f(\tau)f(\sigma)} = \zeta_n^{f(\tau\sigma)} = \tau\sigma(\zeta_n)$$

We can yet say more. Let F be an intermediate extension of $\mathbb{Q}$ and $\mathbb{Q}(\zeta_n)$ such that $\mathbb{Q} \subset F \subset \mathbb{Q}(\zeta_n)$. What can we say about the extension $F/\mathbb{Q}$? By the fundamental theorem of Galois theory, we get the following correspondence between subfields F and subgroups of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$:

$$\begin{array}{ccc} \mathbb{Q}(\zeta_n) & \longleftrightarrow & \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \\ \vert & & \vert \\ F & \longleftrightarrow & \mathrm{Gal}(\mathbb{Q}(\zeta_n)/F) \\ \vert & & \vert \\ \mathbb{Q} & \longleftrightarrow & \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n)) \end{array}$$

$F/\mathbb{Q}$ is a Galois extension if and only if $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/F)$ is a normal subgroup of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. But $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is abelian, and hence all subgroups are normal. Thus, $F/\mathbb{Q}$ is Galois. Furthermore, the fundamental theorem of Galois theory also tells us that

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})/\mathrm{Gal}(\mathbb{Q}(\zeta_n)/F) \cong \mathrm{Gal}(F/\mathbb{Q})$$

Since every quotient of an abelian group is abelian, $\mathrm{Gal}(F/\mathbb{Q})$ is abelian. So $F/\mathbb{Q}$ is an abelian extension of $\mathbb{Q}$.

Let us quickly recap what we have shown so far. We have seen that every cyclotomic field extension of $\mathbb{Q}$ is abelian, and so is every subfield of a cyclotomic extension of $\mathbb{Q}$. A natural question that arises thereof is whether the converse is true: does every finite abelian extension of $\mathbb{Q}$ arise as a subfield of a cyclotomic extension? The answer is yes, by the Kronecker-Weber theorem.

Theorem 3.5 (Kronecker, Weber)**.** *Let F be a finite Galois extension of $\mathbb{Q}$ whose Galois group $\mathrm{Gal}(F/\mathbb{Q})$ is abelian. Then there exists a cyclotomic extension $\mathbb{Q}(\zeta_n)$ of $\mathbb{Q}$ such that $F \subset \mathbb{Q}(\zeta_n)$.*

There is valuable perspective to be gained by examining what we have just shown from a slightly different point of view. Consider the exponential function

$$\begin{aligned} g\colon \mathbb{C} &\to \mathbb{C} \\ g(z) &= e^{2\pi i z} \end{aligned}$$

We note that $g(z)$ is everywhere holomorphic on $\mathbb{C}$. Furthermore, by taking $z = \frac{1}{n}$ as our input, we obtain primitive n^{th} roots of unity. Because of the correspondence established by our one-to-one homomorphism f between $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ and $(\mathbb{Z}/n\mathbb{Z})^\times$, we can describe $\sigma(\zeta_n)$ in terms of g as follows:

$$\sigma(g\left(\frac{1}{n}\right)) = g\left(\frac{f(\sigma)}{n}\right)$$

Finally, we can reframe our characterization of abelian extensions of $\mathbb{Q}$ using $g(z)$. A finite extension F of $\mathbb{Q}$ is abelian if and only if $F \subset \mathbb{Q}(g(\frac{1}{n}))$ for some $n \in \mathbb{N}$. Thus, abelian extensions of $\mathbb{Q}$ can be thought of as subfields of extensions of $\mathbb{Q}$ formed by adjoining special values of an everywhere holomorphic function.

With $\mathbb{Q}$ in mind, a natural question is whether it is possible to construct an analogous characterization of abelian extensions of any number field F? That is, does there exist an everywhere holomorphic function g such that any Galois extension K of F is abelian if and only if $K \subset F(g(a_1), g(a_2), \ldots, g(a_n))$ for special values $g(a_1), g(a_2), \ldots, g(a_n)$? The goal of achieving such a construction is known as Kronecker's "Jugendtraum", or Kronecker's "youthful dream". Clearly, it is true for the case $F = \mathbb{Q}$, as was just shown. It turns out that it is also true for quadratic imaginary fields (i.e. extensions of $\mathbb{Q}$ of the form $\mathbb{Q}(\sqrt{-D})$ for some positive squarefree integer D), in a way that is closely related to the theory of elliptic curves and elliptic functions. We will explore this question by constructing abelian extensions of $\mathbb{Q}(i)$ before ultimately returning to the broader scope of general quadratic imaginary fields.

3.2 Establishing an Analogue Between $\mathbb{Q}$ and $\mathbb{Q}(i)$

In order to build an analagous theory between $\mathbb{Q}$ and $\mathbb{Q}(i)$, we are going to need a number of ingredients. Let us recount what we know about abelian extensions of $\mathbb{Q}$.

To start, it will be more natural for us to view primitive n^{th} roots of unity as the kernel of n^{th} power map

$$\begin{aligned}\lambda_n \colon (\mathbb{C})^\times &\to (\mathbb{C})^\times \\ \lambda_n(z) &= z^n\end{aligned}$$

Primitive n^{th} roots of unity were the special values of the exponential function $e^{2\pi iz}$ we adjoined to $\mathbb{Q}$ to form abelian extensions. In finding abelian extensions of $\mathbb{Q}(i)$, we will be seeking an analogous map, the kernel of which will contain the special values we will adjoin to $\mathbb{Q}(i)$. In turn, we also need an everywhere holomorphic function whose image contains these special values for the right inputs. Finally, a key point in establishing that $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ was the injective homomorphism f between $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ and the abelian group $(\mathbb{Z}/n\mathbb{Z})^\times$. We will need to develop an analagous homomorphism for abelian extensions of $\mathbb{Q}(i)$. As one might guess, elliptic curves will be at the heart of this analogous construction.

Consider the following table summarizing what we need in order to construct abelian extensions of $\mathbb{Q}(i)$:

	What we know about $\mathbb{Q}$	What we want to know for $\mathbb{Q}(i)$
I)	$\zeta_n \in \ker(\lambda_n)$	What kernel do we seek?
II)	$f \colon \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times$	What homomorphism can we establish?
III)	$g(z) = e^{2\pi iz}$	What function?

We will tackle the matters of **I)**, **II)** and **III)** separately and in sequential order. Let's start by diving into **I)**.

I): Finding a Kernel

Let E be a non-singular rational elliptic curve given by a Weierstrass equation

$$y^2 = x^3 + ax^2 + bx + c$$

with group of complex points $E(\mathbb{C})$. In this section, we will establish the connection between Kronecker's Jugendtraum for quadratic imaginary fields and elliptic curves. It turns out that the natural map (and corresponding kernel) to study is the multiplication by n map for points on $E(\mathbb{C})$, i.e.:

$$\begin{aligned}\Omega_n \colon E(\mathbb{C}) &\to E(\mathbb{C}) \\ \Omega_n(P) &= nP\end{aligned}$$

The kernel of this map is the set of points such that $nP = O$, i.e. points of order dividing n in $E(\mathbb{C})$. We denote $\ker(\Omega_n)$ as

$$E[n] = \ker(\Omega_n) = \{P \in E(\mathbb{C}) \mid nP = O\}$$

Now we will use the isomorphic representation of $E(\mathbb{C})$ as a complex torus developed in §2.3. Let L be the lattice associated with $E(\mathbb{C})$ given by

$$L = \mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \tau, \text{ where } \tau \in \mathbb{H}$$

such that $E(\mathbb{C}) \cong \mathbb{C}/L$. The lattice representation of $E(\mathbb{C})$ allows us to develop an explicit isomorphism $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z} \cong E[n]$ via the map

$$(a_1, a_2) \mapsto \frac{a_1}{n} + \frac{a_2}{n}\tau \text{ for } (a_1, a_2) \in \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$$

These are clearly are the points of order dividing n on $E(\mathbb{C})$, since they are the points of order dividing n in $\mathbb{C}/L$. This is shown nicely by the figure 3.2 below.

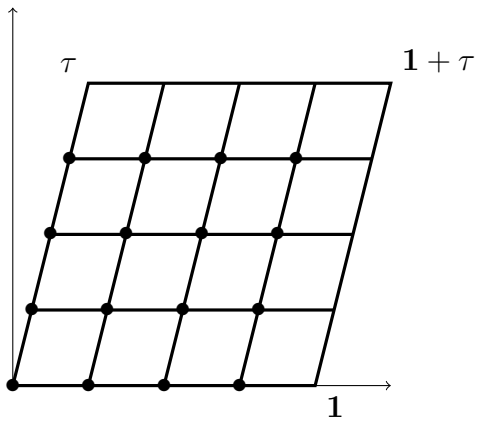


Figure 9: Points of order four on a complex torus.

Much like we studied roots of cyclotomic extensions of $\mathbb{Q}$, we will similarly study the field extension

$$\mathbb{Q}(i)(E[n]) := \mathbb{Q}(i)(x_1, y_1, x_2, y_2, \ldots, x_m, y_m, O)$$

where x_i, y_i are the coordinates of the point $P_i \in E[n]$ for $1 \leq i \leq m$. We can see there are n^2 points of order dividing n via the isomorphism between $E[n]$ and $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$. Before we proceed further, we must prove two important claims about $E[n]$ and the extension $\mathbb{Q}(E[n])/\mathbb{Q}$:

Theorem 3.6. *$\mathbb{Q}(E[n])/\mathbb{Q}$ is a Galois extension of $\mathbb{Q}$.*

Proof. Let $\kappa_n = \mathbb{Q}(E[n])$, and let σ be a nontrivial field homomorphism

$$\sigma\colon \kappa_n \hookrightarrow \mathbb{C}$$

We will show κ_n is a Galois extension of $\mathbb{Q}$ by showing that $\sigma(\kappa_n) = \kappa_n$. Recall that any field homomorphism is either injective or trivial, as a field has no nontrivial ideals; hence, σ is injective. Futhermore, note that $\sigma(1) = 1$, and so σ fixes $\mathbb{Q}$. Hence, the map σ is completely determined by where it takes the generators $x_1, y_1, \cdots, x_m, y_m, O$. Let us now take care of some notation. For a point $P = (x, y) \in \kappa_n$, we define

$$\sigma(P) = (\sigma(x), \sigma(y))$$

and we furthermore take $\sigma(O) = O$. Furthermore, using the fact that σ is a homomorphism which fixes $\mathbb{Q}$, we can show that $\sigma(P)$ is a point on E for $P = (x, y) \in E$ as follows:

$$\begin{aligned}
y^2 =& x^3 + ax^2 + bx + c \\
y^2 - & x^3 - ax^2 - bx - c = 0 \\
& \sigma(y^2 - x^3 - ax^2 - bx - c) = \sigma(0) \quad \text{applying } \sigma \\
& \sigma(y)^2 - \sigma(x)^3 - \sigma(a)\sigma(x)^2 - \sigma(b)\sigma(x) - \sigma(c) = 0 \quad \text{using the fact that } \sigma \text{ is a homomorphism} \\
& \sigma(y)^2 - \sigma(x)^3 - a\sigma(x)^2 - b\sigma(x) - c = 0 \quad \text{because } \sigma \text{ fixes } \mathbb{Q} \\
& \sigma(y)^2 = \sigma(x)^3 + a\sigma(x)^2 + b\sigma(x) + c \\
\implies & \sigma(P) = (\sigma(x), \sigma(y)) \in E
\end{aligned}$$

We will now prove a lemma that will help us complete this proof.

Lemma 3.7. *Let $P \in E(\mathbb{C}), n \in \mathbb{N}$. Then $\sigma(nP) = n\sigma(P)$.*

Proof. We will first show $\sigma(P + Q) = \sigma(P) + \sigma(Q)$ for $P, Q \in E(\mathbb{C})$ where $P \neq \pm Q$. Let

$$P = (x_1, y_1), \quad Q = (x_2, y_2) \qquad \text{and} \qquad P + Q = (x_3, y_3).$$

Then by the formulas for the addition law, we have:

$$\begin{aligned}
x_3 &= \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - a - x_1 - x_2, \\
y_3 &= \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1.
\end{aligned}$$

Since σ is a homomorphism fixing $\mathbb{Q}$, we find

$$\begin{aligned}
\sigma(x_3) &= \left(\frac{\sigma(y_2) - \sigma(y_1)}{\sigma(x_2) - \sigma(x_1)}\right)^2 - a - \sigma(x_1) - \sigma(x_2), \\
\sigma(y_3) &= \left(\frac{\sigma(y_2) - \sigma(y_1)}{\sigma(x_2) - \sigma(x_1)}\right)(\sigma(x_1) - \sigma(x_3)) - \sigma(y_1).
\end{aligned}$$

These are just the addition formulas on the points $\sigma(P)$ and $\sigma(Q)$. Thus:

$$\begin{aligned}
\sigma(P + Q) =& (\sigma(x_3), \sigma(y_3)) \\
=& (\sigma(x_1), \sigma(y_1)) + (\sigma(x_2), \sigma(y_2)) \\
=& \sigma(P) + \sigma(Q).
\end{aligned}$$

Now suppose $P = -Q$, i.e. $Q = (x_1, -y_1)$. We want to show that $\sigma(P+Q) = \sigma(O) = O = \sigma(P) + \sigma(Q)$. We must hence show that $\sigma(Q)$ is $\sigma(P)$ reflected about the x-axis. This follows from the fact that σ is a homomorphism fixing $\mathbb{Q}$, as $\sigma(P) = (\sigma(x_1), \sigma(y_1))$ and $\sigma(Q) = (\sigma(x_1), \sigma(-y_1)) = (\sigma(x_1), -\sigma(y_1)) = -\sigma(P)$.

Now, to prove the lemma, we proceed by induction. First, we will show that $\sigma(2P) = 2\sigma(P)$ using the duplication formula derived in §1.1. Recall that for $P = (x, y)$, we have the coordinates of $2P = (x', y')$, where

$$x' = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c},$$
$$y' = \frac{8a^2cx - 2ab^2x + 4abc + 20acx^2 + 2ax^5 - b^3 - 5b^2x^2 - 4bcx + 5bx^4 - 8c^2 + 20cx^3 + x^6}{8y^3}.$$

Again using the fact that σ is a homomorphism fixing $\mathbb{Q}$, we find that the coordinates of $\sigma(2P)$ are given by:

$$\sigma(x') = \frac{\sigma(x)^4 - 2b\sigma(x)^2 - 8c\sigma(x) + b^2 - 4ac}{4\sigma(x)^3 + 4a\sigma(x)^2 + 4b\sigma(x) + 4c}$$

$$\sigma(y') = \frac{\begin{pmatrix} 8a^2c\sigma(x) - 2ab^2\sigma(x) + 4abc + 20ac\sigma(x)^2 + 2a\sigma(x)^5 - b^3 \\ \quad - 5b^2\sigma(x)^2 - 4bc\sigma(x) + 5b\sigma(x)^4 - 8c^2 + 20c\sigma(x)^3 + \sigma(x)^6 \end{pmatrix}}{8\sigma(y)^3}$$

Hence, we have $\sigma(2P) = 2\sigma(P)$, as desired. Now suppose $\sigma((n-1)P) = (n-1)\sigma(P)$. We wish to show that this implies $\sigma(nP) = n\sigma(P)$. But we have $nP = (n-1)P + P$. We break into two cases.

Suppose $(n-1)P \neq P$. Then, by our induction hypothesis

$$\sigma(nP) = \sigma((n-1)P + P) = \sigma((n-1)P) + \sigma(P) = (n-1)\sigma(P) + \sigma(P) = n\sigma(P)$$

Now suppose $(n-1)P = P$. Then $nP = (n-1)P + P = P + P = 2P$, and so $\sigma(nP) = \sigma(2P) = 2\sigma(P) = \sigma(P) + \sigma(P) = \sigma((n-1)P) + \sigma(P)$. Again by induction, this equals $n\sigma(P)$. □

Now, by Lemma 3.7, for any $P_i \in E[n]$

$$O = \sigma(O) = \sigma(nP_i) = n\sigma(P_i)$$

and therefore $\sigma(P_i) \in E[n]$. Hence, σ permutes points in $E[n]$, i.e. σ permutes the generators of κ_n. Thus, we have $\sigma(\kappa_n) \subset \kappa_n$, and so we are done. □

Theorem 3.8. *If $P = (x, y) \in E[n]$, then x and y are algebraic over $\mathbb{Q}$.*

Proof. Recall from Theorem 3.6 that every nontrivial homomorphism $\sigma\colon \kappa_n \hookrightarrow \mathbb{C}$ is a permutation of the generators $x_1, y_1, \ldots, x_n, y_n$ of κ_n. Since there are finitely many[6] generators of κ_n, it follows that there must be only finitely many homomorphisms. But if the coordinates of $P = (x, y) \in E[n]$ are not algebraic, this implies that $[\kappa_n\colon \mathbb{Q}]$ is infinite, and there would therefore be infinitely many homomorphisms σ, a contradiction. Hence, if $P = (x, y) \in E[n]$, then x, y are algebraic over $\mathbb{Q}$. □

II): Constructing a Galois Representation

When we previously studied the field extension $\mathbb{Q}(\zeta_n)$, we found we could describe elements $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ by where σ sent ζ_n. Using this result and the fact that automorphisms are order preserving, we established an injective homomorphism between $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ and $(\mathbb{Z}/n\mathbb{Z})^\times$. In other words, letting $\mu_n = \langle \zeta_n \rangle$, understanding $\mathrm{Aut}(\mu_n)$ gave us information about $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$.

Similarly, automorphisms of $\mathbb{Q}(E[n])$ fixing $\mathbb{Q}$ (and hence elements $\sigma \in \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$) are completely determined by where they map elements of $E[n]$. Analogously, understanding $\mathrm{Aut}(E[n])$ will therefore help us determine elements of $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$.

So how do we proceed? Previously, we chose a generator ζ_n of μ_n and constructed an automorphism of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ by looking at maps between ζ_n and another generator of μ_n. This is precisely what we will do with $E[n]$. We will choose generators of $E[n]$, and then establish automorphisms of $E[n]$ by constructing maps between generators of $E[n]$. Recall

$$E[n] \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$$

From this isomorphism, we see that $E[n]$ is generated by *two* basis elements, P_1 and P_2, though our choice of basis is not unique. Every element of $E[n]$ can therefore be written as a linear combination $a_1P_1 + a_2P_2$ for some unique $a_1, a_2 \in \mathbb{Z}/n\mathbb{Z}$. Hence, for any isomorphism $h\colon E[n] \to E[n]$, we have

$$h(a_1P_2 + a_2P_2) = a_1h(P_1) + a_2h(P_2)$$

i.e., the map h is completely determined by where it sends the generating basis, or the values of $h(P_1)$ and $h(P_2)$. Hence, the map $h\colon E[n] \to E[n]$ can be expressed as

$$a_1P_2 + a_2P_2 \mapsto a_1h(P_1) + a_2h(P_2),$$

This is akin to doing linear algebra over an R-module with a basis, which simplifies matters quite a bit. Since h is an isomorphism from $E[n]$ to $E[n]$, P_1 and P_2 are still a basis for the image of h. Hence, we can write $h(P_1)$ and $h(P_2)$ as a unique linear combination of P_1 and P_2 with coefficients in $\mathbb{Z}/n\mathbb{Z}$. Furthermore, the coefficients are completely determined by the map h as follows:

$$\begin{aligned} h(P_1) &= \alpha_h P_1 + \gamma_h P_2 \\ h(P_2) &= \beta_h P_1 + \delta_h P_2 \end{aligned}$$

[6] Recall $|E[n]| = n^2$

or in matrix notation:

$$(h(P_1), h(P_2)) = (P_1, P_2) \begin{pmatrix} \alpha_h & \beta_h \\ \gamma_h & \delta_h \end{pmatrix}.$$

Suppose we had another isomorphism $g\colon E[n] \to E[n]$ where

$$\begin{aligned} g(P_1) =& \alpha_g P_1 + \gamma_g P_2, \\ g(P_2) =& \beta_g P_1 + \delta_g P_2. \end{aligned}$$

Can we easily find a similar formula for $g \circ h$? Thanks to linear algebra, the answer is yes. We easily compute the composition on P_1 as follows:

$$\begin{aligned} (g \circ h)(P_1) =& g(h(P_1)) \\ =& g(\alpha_h P_1 + \gamma_h P_2) \\ =& \alpha_h g(P_1) + \gamma_h g(P_2) \\ =& \alpha_h(\alpha_g P_1 + \gamma_g P_2) + \gamma_h(\beta_g P_1 + \delta_g P_2) \\ =& (\alpha_h \alpha_g + \gamma_h \beta_g) P_1 + (\alpha_h \gamma_g + \gamma_h \delta_g) P_2 \end{aligned}$$

An identical computation can be made for P_2, and in this way, we can compute a matrix representation for the action of any composition of isomorphisms of $E[n]$. We obtain the following matrix representation for $g \circ h$:

$$((g \circ h)(P_1), (g \circ h)(P_2)) = (P_1, P_2) \begin{pmatrix} \alpha_{g\circ h} & \beta_{g\circ h} \\ \gamma_{g\circ h} & \delta_{g\circ h} \end{pmatrix} = (P_1, P_2) \begin{pmatrix} \alpha_g & \beta_g \\ \gamma_g & \delta_g \end{pmatrix} \begin{pmatrix} \alpha_h & \beta_h \\ \gamma_h & \delta_h \end{pmatrix}.$$

Since we are looking at *isomorphisms* of $E[n]$, we also know that these maps are invertible. Let $h\colon E[n] \to E[n]$ be an isomorphism and let h^{-1} be its inverse. Then since $h^{-1} \circ h$ is the identity on $E[n]$, we have:

$$\begin{aligned} (h^{-1} \circ h)(P_1) =& P_1 = 1 \cdot P_1 + 0 \cdot P_2, \\ (h^{-1} \circ h)(P_2) =& P_2 = 0 \cdot P_1 + 1 \cdot P_2. \end{aligned}$$

In other words, we have:

$$((h^{-1} \circ h)(P_1), (h^{-1} \circ h)(P_2)) = (P_1, P_2) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = (P_1, P_2) \begin{pmatrix} \alpha_{h^{-1}} & \beta_{h^{-1}} \\ \gamma_{h^{-1}} & \delta_{h^{-1}} \end{pmatrix} \begin{pmatrix} \alpha_h & \beta_h \\ \gamma_h & \delta_h \end{pmatrix}.$$

And thus, we conclude:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \alpha_{h^{-1}} & \beta_{h^{-1}} \\ \gamma_{h^{-1}} & \delta_{h^{-1}} \end{pmatrix} \begin{pmatrix} \alpha_h & \beta_h \\ \gamma_h & \delta_h \end{pmatrix}.$$

Hence, the matrix representations of isomorphisms we have been concerned with are invertible, and in fact, the inverse h^{-1} of an isomorphism $h\colon E[n] \to E[n]$ has matrix representation equal to the inverse of the matrix representation of h. This means that invertible

matrices with coefficients in $\mathbb{Z}/n\mathbb{Z}$ correspond to isomorphisms of $E[n]$. Thus, for each automorphism $\sigma \in \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$, we obtain an isomorphism of $E[n]$ which has a unique invertible matrix representation.

This suggests that our analogue of $(\mathbb{Z}/n\mathbb{Z})^\times$ will be $GL_2(\mathbb{Z}/n\mathbb{Z})$, or the group of 2×2 invertible matrices with entries in $\mathbb{Z}/n\mathbb{Z}$.[7] This is indeed the case, and in fact, we will build a one-to-one homomorphism between $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ and $GL_2(\mathbb{Z}/n\mathbb{Z})$. In the same spirit as with $\mathbb{Q}(\zeta_n)$, we define the mapping

$$\rho_n \colon \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) \to GL_2(\mathbb{Z}/n\mathbb{Z})$$

defined by

$$\rho_n(\sigma) = \begin{pmatrix} \alpha_\sigma & \beta_\sigma \\ \gamma_\sigma & \delta_\sigma \end{pmatrix}, \text{ where } \sigma \in \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) \text{ such that}$$
$$\sigma(P_1) = \alpha_\sigma P_1 + \gamma_\sigma P_2,$$
$$\sigma(P_2) = \beta_\sigma P_1 + \delta_\sigma P_2.$$

We now prove that ρ_n is indeed an injective homomorphism.

Lemma 3.9. *Let $\rho_n \colon \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) \to GL_2(\mathbb{Z}/n\mathbb{Z})$ be defined above. Then ρ_n is a one-to-one homomorphism.*

Proof. We show that ρ_n is a homomorphism first. In fact, we have effectively already shown it. Let $\sigma, \tau \in \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$. Then

$$\rho_n(\sigma \circ \tau) = \begin{pmatrix} \alpha_\sigma & \beta_\sigma \\ \gamma_\sigma & \delta_\sigma \end{pmatrix} \begin{pmatrix} \alpha_\tau & \beta_\tau \\ \gamma_\tau & \delta_\tau \end{pmatrix} = \rho_n(\sigma)\rho_n(\tau).$$

Now, we will show that ρ_n is injective by showing its kernel is trivial. Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ be in $\ker(\rho_n)$. Then it follows that

$$\rho_n(\sigma) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Hence, for an appropriate choice of generators P_1 and P_2 of $E[n]$, we have $\sigma(P_1) = P_1$ and $\sigma(P_2) = P_2$. As P_1 and P_2 generate $E[n]$, every $P \in E[n]$ can be written uniquely as some linear combination of P_1 and P_2 with coefficients in $\mathbb{Z}/n\mathbb{Z}$, i.e. $P = a_1P_1 + a_2P_2$ for some $a_1, a_2 \in \mathbb{Z}/n\mathbb{Z}$. Since σ is a homomorphism,

$$\sigma(a_1P_1 + a_2P_2) = a_1\sigma(P_1) + a_2\sigma(P_2) = a_1P_1 + a_2P_2$$

Hence, $\sigma(P) = P$ for all $P \in E[n]$. Since $\sigma(x, y) = (\sigma(x), \sigma(y))$, we can see that σ fixes every coordinate of every point in $E[n]$. Thus, σ fixes every generator of $E[n]$, and hence must be the identity on $\mathbb{Q}(E[n])/\mathbb{Q}$. In other words, σ is the identity in $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$, and so the kernel of ρ_n is trivial. Hence, ρ_n is injective. □

[7] Equivalently, the group of 2×2 matrices with entries in $\mathbb{Z}/n\mathbb{Z}$ whose determinant is a unit in $\mathbb{Z}/n\mathbb{Z}$.

Unfortunately, our story gets a bit more complicated from here. Unlike $(\mathbb{Z}/n\mathbb{Z})^\times$, $GL_2(\mathbb{Z}/n\mathbb{Z})$ is *not* abelian, as matrix multiplication is not generally commutative. Fortunately, ρ_n is not onto, and $\mathrm{Im}(\rho_n) \leq GL_2(\mathbb{Z}/n\mathbb{Z})$ *is* abelian in some special cases. However, whereas it was obvious that $\mathrm{Im}(f) = (\mathbb{Z}/n\mathbb{Z})^\times$ was abelian, that $\mathrm{Im}(\rho_n) \leq GL_2(\mathbb{Z}/n\mathbb{Z})$ is abelian is not immediate from inspection. Indeed, to show that $\mathrm{Im}(\rho_n)$ is sometimes abelian, we will need the exceptional property of some elliptic curves known as complex multiplication.

3.3 Complex Multiplication: a First Look

We saw in §3.2 that the multiplication by n map from $E(\mathbb{C})$ to $E(\mathbb{C})$ has kernel $E[n]$, and can be defined exclusively in terms of rational functions on the coordinates of the input point. Furthemore, this map is a homomorphism as proved by Lemma 3.7. Generally, we say that a homomorphism φ is an **isogeny** if φ can be defined completely in terms of rational functions. Hence, our multiplication by n map Ω_n is an isogeny. Many valuable isogenies are mappings between different elliptic curves. Nevertheless, we will be primarily interested in isogenies between an elliptic curve and itself. These special isogenies are called **endomorphisms**. We have just seen that Ω_n defines one such isogeny for each integer n. However, a natural question to ask is whether there are any other kinds of endomorphisms on elliptic curves. The answer is yes, and it gives rise to the following definition.

Definition 3.10. *Let E be an elliptic curve. Then E is said to have complex multiplication if there is an endomorphism $\phi\colon E \to E$ which is not a multiplication by n map.*

Let us give an example. Let E be the curve defined by the solutions to $y^2 = x^3 + x$. Then E has complex multiplication with the additional endomorphism map

$$\begin{aligned} \phi\colon E(\mathbb{C}) &\to E(\mathbb{C}) \\ (x, y) &\mapsto (-x, iy) \end{aligned}$$

It may be observed that ϕ is a homomorphism,[8] and ϕ is defined in terms of rational functions of the input coordinates. Hence, ϕ is an isogeny. We can also see that ϕ is not a multiplication by n map from the complex coefficient of the y-coordinate. E therefore has complex multiplication. In general, what kind of endomorphisms of elliptic curves exist other than multiplication by n maps? In fact, we can completely characterize any other kind of endomorphism of an elliptic curve E.[9]

We may do so by looking to the lattice representation of an elliptic curve E. Let L be the lattice associated with $E(\mathbb{C})$ given by

$$L = \mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \tau, \text{ where } \tau \in \mathbb{H}$$

such that $E(\mathbb{C}) \cong \mathbb{C}/L$. Let $\phi\colon E \to E$ be an endomorphism which is not a multiplication by n map. Then the endomorphism ϕ induces a holomorphic map

$$g\colon \mathbb{C}/L \to \mathbb{C}/L$$

[8] A useful theorem presented by Silverman [3] tells us that any map φ between two elliptic curves E and $\bar{E}$ given by rational functions such that $\varphi(O) = \bar{O}$ is a homomorphism.

[9] By doing so, we explain the perhaps arcane terminology of "complex multiplication".

Since g is holomorphic, it can be represented as a convergent power series in the neighborhood of 0, i.e.

$$g(z) = \sum_{n=0}^{\infty} c_n z^n.$$

Since ϕ is a homomorphism, g is also a homomorphism, so for z_1, z_2 in an appropriate neighborhood around 0,

$$g(z_1 + z_2) = g(z_1) + g(z_2) \in \mathbb{C}/L \implies g(z_1 + z_2) - g(z_1) - g(z_2) \equiv 0 \pmod{L}.$$

But we know that L is a set of discrete points, and therefore contains no non-empty open set. The image of any non-constant holomorphic function is open, and so $g(z_1+z_2)-g(z_1)-g(z_2)$ must be constant. If we take $z_1 = z_2 = 0$, then we see

$$\begin{aligned} g(z_1 + z_2) - g(z_1) - g(z_2) =& g(0) - 2g(0) = -g(0) = c_0; \text{ so} \\ g(z_1 + z_2) + c_0 =& g(z_1) + g(z_2) \end{aligned}$$

for all z_1, z_2 in the appropriate neighborhood about 0 in $\mathbb{C}$. Furthemore, since $g(z_1 + z_2) - g(z_1) - g(z_2) \equiv 0 \pmod{L}$, we find $c_0 \equiv 0 \pmod{L}$, or equivalently, $c_0 \in L$. Let $f(z) = g(z) - c_0$. Since f is a translation of g by an element of L, they are the same map when considered modulo L. In other words, the maps given by

$$\begin{aligned} z &\mapsto f(z) \\ z &\mapsto g(z) \end{aligned}$$

are the same endomorphism in $\mathbb{C}/L$. With this shift, we can take $c_0 = 0$, and so

$$f(z_1 + z_2) = f(z_1) + f(z_2)$$

for all z_1, z_2 in the appropriate neighborhood about 0 in $\mathbb{C}$. There are very few functions which satisfy this property, and in fact, this property is enough to determine f.

Proposition 3.11. *$f(z) = cz$ for some $c \in \mathbb{C}$.*

Proof. First, take $z = 0$. Then $f(0 + 0) = f(0) + f(0) = 2f(0) \implies f(0) = 2f(0)$, so $f(0) = 0$. Next, we will compute $f'(z)$ and show that it is constant as follows:

$$\begin{aligned} f'(z) =& \lim_{h \to 0} \frac{f(z + h) - f(z)}{h} \\ =& \lim_{h \to 0} \frac{f(z) + f(h) - f(z)}{h} \\ =& \lim_{h \to 0} \frac{f(0 + h) - f(0)}{h} \\ =& f'(0). \end{aligned}$$

So $f'(z)$ is constant, and $f(z) = cz + c'$ for some $c, c' \in \mathbb{C}$. But $f(0) = 0$, so $f(z) = cz$. $\square$

We would like f to be well defined, and we see that this is true if $[z_1] = [z_2] \implies [cz_1] = [cz_2]$ in $\mathbb{C}/L$. This naturally restricts the possible values of c. The condition $[z_1] = [z_2]$ is equivalent to the condition $z_1 - z_2 \equiv 0 \pmod{L}$. We thus restrict our attention to c such that $z_1 - z_2 \equiv 0 \pmod{L} \implies cz_1 - cz_2 \equiv 0 \pmod{L}$. By distributivity, this is equivalent to $z_1 - z_2 \equiv 0 \pmod{L}$. Since the lattice is closed under subtraction, this is equivalent to $z \equiv 0 \pmod{L} \implies cz \equiv 0 \pmod{L}$, or simply $cL \subset L$.

If $cL \subset L$, we have that

$$\begin{aligned} c \cdot 1 =& n_1 + m_1\tau, \text{ and} \\ c \cdot \tau =& n_2 + m_2\tau \end{aligned}$$

where $n_1, n_2, m_1, m_2 \in \mathbb{Z}$. But we can see that this leaves two options. We could have $c \in \mathbb{Z}$, with $m_1 = 0$; if this is the case, then we see that f is a multiplication by n map, as multiplication by n in $\mathbb{C}/L$ is same as muliplication by n on E. However, if $m_1 \neq 0$, then $c \in \mathbb{C}$ and $c \notin \mathbb{R}$. This gives rise to the natural terminology *complex multiplication*.

3.4 Abelian Extensions of $\mathbb{Q}(i)$

III): Putting it All Together

Consider the nonsingular elliptic curve defined over the rational numbers

$$E\colon y^2 = x^3 + x.$$

As seen before, E has complex multiplication given by the map:

$$\begin{aligned} \phi\colon E(\mathbb{C}) &\to E(\mathbb{C}) \\ (x, y) &\mapsto (-x, iy) \end{aligned}$$

One might rightfully wonder why we have chosen $\mathbb{Q}(i)$ as our example quadratic imaginary base field, and why E is the corresponding curve to study. We can answer this question in light of complex multiplication.

Let $K/\mathbb{Q}$ be a Galois extension such that $i \in K$, and let $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. For a point $P = (x, y) \in E(K)$, we can get a new point in $E(K)$ by applying the endomorphism ϕ, or by applying σ. As we are studying abelian groups, we might wonder under what conditions ϕ and σ commute; that is, when is it true that

$$\sigma(\phi(P)) = \phi(\sigma(P))$$

We see that

$$\begin{aligned} \sigma(\phi(P)) =& \sigma(-x, iy) = (\sigma(-x), \sigma(iy)) = (-\sigma(x), \sigma(i)\sigma(y)) \\ \phi(\sigma(P)) =& \phi(\sigma(x), \sigma(y)) = (-\sigma(x), i\sigma(y)). \end{aligned}$$

We thus have $\sigma(\phi(P)) = \phi(\sigma(P))$ for all P if and only $\sigma(i) = i$. In other words, we have equality if every $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ fixes i, i.e. $\sigma \in \mathrm{Gal}(K/\mathbb{Q}(i))$. Hence, if we want to use ϕ to study Galois groups, it is natural to look at Galois extensions of $\mathbb{Q}(i)$, which is just what we wanted. We now give a construction of abelian extensions of $\mathbb{Q}(i)$.

Theorem 3.12. *Let E be the nonsingular rational elliptic curve*

$$E\colon y^2 = x^3 + x.$$

For each integer $n \geq 1$, let

$$K_n = \mathbb{Q}(i)(E[n])$$

be the field extension of $\mathbb{Q}$ generated by i and the coordinates of the points of order diving n in $E(\mathbb{C})$. Then K_n is a Galois extension of $\mathbb{Q}(i)$, and its Galois group is abelian.

Proof. It is clear that $\mathbb{Q}(i)$ is Galois, as it is a quadratic extension of $\mathbb{Q}$. Furthermore, in Theorem 3.6 we proved that $\mathbb{Q}(E[n])$ is also Galois. Hence, K_n, which is the compositum of these two extensions, must also be Galois over $\mathbb{Q}$, and hence is Galois over $\mathbb{Q}(i)$.

Just as we observed there is a homomorphism from $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ into $GL_2(\mathbb{Z}/n\mathbb{Z})$, there is a homomorphism $\rho_n\colon \mathrm{Gal}(K_n/\mathbb{Q}(i)) \to GL_2(\mathbb{Z}/n\mathbb{Z})$ defined by

$$\rho_n(\sigma) = \begin{pmatrix} \alpha_\sigma & \beta_\sigma \\ \gamma_\sigma & \delta_\sigma \end{pmatrix}, \text{ where } \sigma \in \mathrm{Gal}(K_n/\mathbb{Q}(i)) \text{ such that}$$
$$\begin{aligned} \sigma(P_1) =& \alpha_\sigma P_1 + \gamma_\sigma P_2 \\ \sigma(P_2) =& \beta_\sigma P_1 + \delta_\sigma P_2 \end{aligned}$$

where P_1 and P_2 are a generating basis for $E[n]$. As ϕ is also a homomorphism from $E[n]$ to itself, since $n\phi(P) = \phi(nP) = \phi(O) = O$, $\phi(P) \in E[n]$. We may therefore also give $\phi : E(\mathbb{C}) \to E(\mathbb{C})$ a matrix representation just as we did for elements of $\mathrm{Gal}(K_n/\mathbb{Q}(i))$. Just as in our matrix representation of $\sigma \in \mathrm{Gal}(K_n/\mathbb{Q}(i))$, there exist $a, b, c, d \in \mathbb{Z}/n\mathbb{Z}$ such that

$$\begin{aligned} \phi(P_1) =& aP_1 + cP_2, \\ \phi(P_2) =& bP_1 + dP_2. \end{aligned}$$

So for ϕ, the corresponding matrix representation is

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

We saw before that for $\sigma \in \mathrm{Gal}(K_n/\mathbb{Q}(i))$ and all $P \in E(K_n)$,

$$\sigma(\phi(P)) = \phi(\sigma(P)),$$

For P_1 this means

$$\begin{aligned} \sigma(\phi(P_1)) = \sigma(aP_1 + cP_2) =& a\sigma(P_1) + c\sigma(P_2) \\ =& a(\alpha_\sigma P_1 + \gamma_\sigma P_2) + c(\beta_\sigma P_1 + \delta_\sigma P_2) \\ =& (a\alpha_\sigma + c\beta_\sigma)P_1 + (a\gamma_\sigma + c\delta_\sigma)P_2 \end{aligned}$$

and

$$\begin{aligned} \phi(\sigma(P_1)) = \phi(\alpha_\sigma P_1 + \delta_\sigma P_2) =& \alpha_\sigma \phi(P_1) + \delta_\sigma \phi(P_2) \\ =& \alpha_\sigma(aP_1 + cP_2) + \delta_\sigma(bP_1 + dP_2) \\ =& (a\alpha_\sigma + b\gamma_\sigma)P_1 + (c\alpha_\sigma + d\gamma_\sigma)P_2. \end{aligned}$$

Maching coefficients, we find

$$\begin{aligned} a\alpha_\sigma + b\delta_\sigma &= a\alpha_\sigma + c\beta_\sigma, \\ a\gamma_\sigma + c\delta_\sigma &= c\alpha_\sigma + d\gamma_\sigma. \end{aligned}$$

And plugging in P_2, we similarly get

$$\begin{aligned} b\alpha_\sigma + d\beta_\sigma &= a\beta_\sigma + b\delta_\sigma, \\ b\gamma_\sigma + d\delta_\sigma &= c\beta_\sigma + d\delta_\sigma. \end{aligned}$$

In other words, the matrix representations of ϕ and σ commute, just as ϕ and σ do:

$$\begin{pmatrix} \alpha_\sigma & \beta_\sigma \\ \gamma_\sigma & \delta_\sigma \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \alpha_\sigma & \beta_\sigma \\ \gamma_\sigma & \delta_\sigma \end{pmatrix}.$$

So how does this help? We will demonstrate is that any matrices that commute with

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

also commute with each other. Then since this will mean the image of ρ_n is an abelian subgroup of $GL_2(\mathbb{Z}/n\mathbb{Z})$, we will be able to conclude $\mathrm{Gal}(K_n/\mathbb{Q}(i))$ is abelian because ρ_n is injective. However, we must ensure that A is not a scalar multiple of the identity matrix, since in that case, all matricies would commute with A and we would not be able to conclude anything about $\mathrm{Gal}(K_n/\mathbb{Q}(i))$. We do this now.

Lemma 3.13. *Let*

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

be the matrix representation of ϕ. Then:

(a) $A \in GL_2(\mathbb{Z}/n\mathbb{Z})$

(b) For every prime $l \mid n$, at least one of the conditions is true:

- *(i)* $b \not\equiv 0 \pmod{l}$
- *(ii)* $c \not\equiv 0 \pmod{l}$
- *(iii)* $a \not\equiv d \pmod{l}$

Proof. For (a), we need to show that $\det(A)$ is a unit in $\mathbb{Z}/n\mathbb{Z}$. We note that for any $P = (x, y) \in E(K_n)$,

$$\phi(\phi(P)) = \phi(\phi(x, y)) = \phi(-x, iy) = (x, -y) = -P.$$

Plugging in P_1 and P_2, we see this means

$$A^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

Hence, $\det(A^2) = \det(A)^2 = 1$, so $\det(A) = \pm 1$. Hence, $A \in GL_2(\mathbb{Z}/n\mathbb{Z})$.

For (b), suppose, seeking a contradiction, that there is some prime $l|n$ such that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} m & 0 \\ 0 & m \end{pmatrix} \pmod{l}$$

This would mean $\phi : E[l] \to E[l]$ is the same as the multiplication by m map $\phi(P) = mP$ for all $P \in E[l]$. Let $\tau : \mathbb{C} \to \mathbb{C}$ be complex conjugation. We can think of τ as an element of $\mathrm{Gal}(K_n/\mathbb{Q})$. We know $\tau(mP) = m\tau(P)$; but $\tau(i) = -i$, so for every $P \in E(K_n)$

$$\tau(\phi(P)) = \tau((-x, iy)) = (-\tau(x), -i\tau(y)) = -\phi(\tau(P)).$$

Since $E[l] \subset E(K_n)$, it thus holds that for all points $P \in E[l]$:

$$\begin{aligned} m\tau(P) =& \tau(mP) \\ =& \tau(\phi(P)) \\ =& -\phi(\tau(P)) \\ =& -m\tau(P). \end{aligned}$$

Hence, $2m\tau(P) = O$ for all $P \in E[l]$. Since $\tau(lP) = l\tau(P)$, it follows that $\tau(P)$ is also in $E[l]$. Thus, τ permutes elements of $E[l]$, so $2mP = O$ for all $P \in E[l]$. Hence, either $l = 2$ or $l|m$; but if $l|m$, then $\phi(P) = mP = O$ for every $P \in E[l]$, which can't be true since $\phi(\phi(P)) = -P$. So $l = 2$. Fortunately, we can compute A for $l = 2$; let $P_1 = (0, 0)$ and $P_2 = (i, 0)$ be generators for $E[2]$. Then it is easy to verify

$$\phi(P_1) = (0, 0) = P_1, \qquad \text{and} \qquad \phi(P_2) = (-i, 0) = P_1 + P_2$$

Hence, we have that $\phi : E[2] \to E[2]$ has the representation

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

whch is not a scalar multiple of the identity matrix, so we eliminate $l = 2$. □

We now prove the lemma which will complete our proof.

Lemma 3.14. *Let $A \in GL_2(\mathbb{Z}/n\mathbb{Z})$ be a non-scalar matrix mod l for all primes $l \mid n$. Then*

$$G = \{B \in GL_2(\mathbb{Z}/n\mathbb{Z}) \mid AB = AB\}$$

is an abelian subgroup of $GL_2(\mathbb{Z}/n\mathbb{Z})$.

Proof. To prove G is abelian, we will prove A can be put into rational normal form via a change of basis T so that

$$T^{-1}AT = \begin{pmatrix} 0 & * \\ 1 & * \end{pmatrix}$$

and then show that matricies commuting with A commute with each other. Furthermore, via a localization argument, to show two matrices are congruent $\pmod{n}$, it suffices to show they are congruent mod l^e for all prime powers $l^e \mid n$. Hence, we can take n to be a prime power l^e. We will proceed by proving two important sublemmas:[10]

[10]These proofs follow primarily from [1].

Lemma 3.15. *Let*

$$A = \begin{pmatrix} 0 & * \\ 1 & * \end{pmatrix} \in GL_2(\mathbb{Z}/n\mathbb{Z})$$

Then

$$G' = \{B \in GL_2(\mathbb{Z}/n\mathbb{Z}) \mid AB = AB\}$$

is an abelian subgroup of $GL_2(\mathbb{Z}/n\mathbb{Z})$.

Proof. We have $AB = BA$ if and only if

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} 0 & b \\ 1 & d \end{pmatrix} = \begin{pmatrix} 0 & b \\ 1 & d \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

So

$$\begin{pmatrix} \beta & b\alpha + d\beta \\ \delta & b\gamma + d\delta \end{pmatrix} = \begin{pmatrix} b\gamma & b\delta \\ \alpha + d\gamma & \beta + d\delta \end{pmatrix}.$$

Treating b, d as fixed quantities, and $\alpha, \beta, \gamma, \delta$ as variables, we get four linear equations. We can see outright that

$$\begin{aligned} \beta &= b\gamma, \\ \delta &= \alpha + d\gamma. \end{aligned}$$

and the other two equations follow from there. Hence,

$$G' = \left\{ \begin{pmatrix} \alpha & b\gamma \\ \gamma & \alpha + d\gamma \end{pmatrix} \in GL_2(\mathbb{Z}/n\mathbb{Z}) \mid \alpha, \gamma \in \mathbb{Z}/n\mathbb{Z} \right\}$$

To see that matrices in G' commute, we verify:

$$\begin{aligned} \begin{pmatrix} \alpha & b\gamma \\ \gamma & \alpha + d\gamma \end{pmatrix} \begin{pmatrix} \alpha' & b\gamma' \\ \gamma' & \alpha' + d\gamma' \end{pmatrix} &= \begin{pmatrix} (\alpha\alpha' + b\gamma\gamma') & (b\alpha\gamma' + b\gamma\alpha' + bd\gamma\gamma') \\ (\gamma\alpha' + \alpha\gamma' + d\gamma\gamma') & (b\gamma\gamma' + (\alpha + d\gamma)(\alpha' + d\gamma')) \end{pmatrix} \\ &= \begin{pmatrix} (\alpha'\alpha + b\gamma'\gamma) & (b\alpha'\gamma + b\alpha\gamma' + bd\gamma\gamma') \\ (\gamma'\alpha + \gamma\alpha' + d\gamma'\gamma) & (b\gamma\gamma' + (\alpha' + d\gamma')(\alpha + d\gamma)) \end{pmatrix} \\ &= \begin{pmatrix} \alpha' & b\gamma' \\ \gamma' & \alpha' + d\gamma' \end{pmatrix} \begin{pmatrix} \alpha & b\gamma \\ \gamma & \alpha + d\gamma \end{pmatrix}. \end{aligned}$$

Hence, G' is abelian. □

Lemma 3.16. *Let* $A \in GL_2(\mathbb{Z}/l^e\mathbb{Z})$ *be a matrix which is not scalar* (mod l). *Then there exists* $T \in GL_2(\mathbb{Z}/l^e\mathbb{Z})$ *such that*

$$T^{-1}AT = \begin{pmatrix} 0 & * \\ 1 & * \end{pmatrix}.$$

Proof. We must find an invertible T such that

$$AT = T \begin{pmatrix} 0 & * \\ 1 & * \end{pmatrix}$$

Recall that A is not a scalar multiple of the identity matrix, and so one of the following conditions must hold:

i. $b \not\equiv 0 \pmod{l}$

ii. $c \not\equiv 0 \pmod{l}$

iii. $a \not\equiv d \pmod{l}$

We then choose T case by case:

i. If $b \not\equiv 0 \pmod{l}$, then take

$$T = \begin{pmatrix} 0 & b \\ 1 & d \end{pmatrix}$$

in which case, $\det(T) = b \not\equiv 0 \pmod{l}$, so $T \in GL_2(\mathbb{Z}/l^e\mathbb{Z})$. Then we may verify:

$$\begin{aligned} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & b \\ 1 & d \end{pmatrix} &= \begin{pmatrix} b & b(a+d) \\ d & cb+d^2 \end{pmatrix} \\ &= \begin{pmatrix} 0 & b \\ 1 & d \end{pmatrix} \begin{pmatrix} 0 & cb-ad \\ 1 & a+d \end{pmatrix}. \end{aligned}$$

ii. If $c \not\equiv 0 \pmod{l}$, then take

$$T = \begin{pmatrix} 1 & a \\ 0 & c \end{pmatrix}$$

in which case, $\det(T) = c \not\equiv 0 \pmod{l}$, so $T \in GL_2(\mathbb{Z}/l^e\mathbb{Z})$. Then we may verify:

$$\begin{aligned} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & a \\ 0 & c \end{pmatrix} &= \begin{pmatrix} a & a^2+bc \\ c & c(a+d) \end{pmatrix} \\ &= \begin{pmatrix} 1 & a \\ 0 & c \end{pmatrix} \begin{pmatrix} 0 & cb-ad \\ 1 & a+d \end{pmatrix}. \end{aligned}$$

iii. If $a \not\equiv d \pmod{l}$ and $b \equiv c \equiv 0 \pmod{l}$, then take

$$T = \begin{pmatrix} 1 & a+c \\ 1 & b+d \end{pmatrix}$$

in which case, $\det(T) = (b+d) - (a+c) \equiv d - a \not\equiv 0 \pmod{l}$, so $T \in GL_2(\mathbb{Z}/l^e\mathbb{Z})$. One may verify that

$$AT = T \begin{pmatrix} 0 & -ad \\ 1 & a+d \end{pmatrix}$$

□

Now to finish proving Lemma 3.14, let $T \in GL_2(\mathbb{Z}/l^e\mathbb{Z})$ be given by Lemma 3.16 such that

$$T^{-1}AT = \begin{pmatrix} 0 & * \\ 1 & * \end{pmatrix}.$$

Then, let $B, B' \in GL_2(\mathbb{Z}/l^e\mathbb{Z})$ be matrices commuting with A. Then $T^{-1}BT$ and $T^{-1}B'T$ commute with $T^{-1}AT$. From Lemma 3.15, $T^{-1}BT$ and $T^{-1}B'T$ commute, i.e.

$$\begin{aligned}(T^{-1}BT)(T^{-1}B'T) =& (T^{-1}B'T)(T^{-1}BT),\\ T^{-1}BB'T =& T^{-1}B'BT,\\ BB' =& B'B.\end{aligned}$$

This completes the proof. □

Now we have the tools to prove Theorem 3.12. We do so sequentially.

1. By acting on $E[n]$ we have representations

   $$\rho_n : \mathrm{Gal}(K_n/\mathbb{Q}(i)) \to GL_2(\mathbb{Z}/n\mathbb{Z})$$

   and (for ϕ)

   $$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z}/n\mathbb{Z}).$$

2. By Lemma 3.13, A is not a scalar matrix $(\mathrm{mod}\ l)$ for any $l|n$.

3. The action on $E[n]$ of σ and ϕ commute for $\sigma \in \mathrm{Gal}(K_n/\mathbb{Q}(i))$, which implies A and $\rho_n(\sigma)$ commute: $A\rho_n(\sigma) = \rho_n(\sigma)A$

4. We conclude by Lemma 3.14 that the set $\{\rho_n(\sigma) \mid \sigma \in \mathrm{Gal}(K_n/\mathbb{Q}(i))\}$ is an abelian subgroup of $GL_2(\mathbb{Z}/n\mathbb{Z})$.

5. Since ρ_n is an injective homomorphism, $\mathrm{Gal}(K_n/\mathbb{Q}(i))$ is abelian.

□

We have not yet provided the quadratic imaginary analogue of the exponential function $g(z) = e^{2\pi iz}$. Our analogous function is in fact $\wp(z)$, the Weierstrass elliptic function. $\wp(z)$ is the connection between the lattice representation of an elliptic curve E and the group of complex points on the curve. Specifically, we recall the isomorphism

$$\begin{aligned}\delta' : \mathbb{C}/L &\to E(\mathbb{C})\\ z &\mapsto (\wp(z), \wp'(z)).\end{aligned}$$

Special values of g gave us primitive n^{th} roots of unity, or equivalently, points of order dividing n in the group $(\mathbb{C})^\times$. Similarly, since the x and y-coordinates on $E(\mathbb{C})$ are the values of $\wp(z)$ and $\wp'(z)$ respectively, we can see that special values of $\wp(z)$ and $\wp'(z)$ yield the coordinates of the points of order dividing n on $E(\mathbb{C})$. Explicitly, since points of order diving n in $\mathbb{C}/L$ for $L = [1, \tau]$ take the form

$$\frac{a_1 + a_2\tau}{n}$$

for some $a_1, a_2 \in \mathbb{Z}$, it follows that K_n is generated by i and the coordinates

$$\wp\left(\frac{a_1 + a_2\tau}{n}\right), \wp'\left(\frac{a_1 + a_2\tau}{n}\right)$$

for $0 \leq a_1, a_2 \leq n$. Furthermore, $\wp(z)$ is mermorphic since it is elliptic. Finally, we can characterize how σ affects the special values of $\wp(z)$ and $\wp'(z)$ in terms of an action on z. Let $x(P)$ denote the x-coordinate of a point $P \in E$. Then

$$\begin{aligned}
\sigma\left(\wp\left(\frac{a_1 + a_2\tau}{n}\right)\right) =& \sigma(x(a_1P_1 + a_2P_2)) \\
=& x(a_1\sigma(P_1) + a_2\sigma(P_2)) \\
=& x((a_1\alpha_\sigma + a_2\beta_\sigma)P_1 + (a_1\gamma_\sigma + a_2\delta_\sigma)P_2) \\
=& \wp\left(\frac{a_1\alpha_\sigma + a_2\beta_\sigma}{n} + \frac{(a_1\gamma_\sigma + a_2\delta_\sigma)\tau}{n}\right).
\end{aligned}$$

4 Complex Multiplication and Abelian Extensions of Quadratic Imaginary Fields

In this section, we try to understand complex multiplication from a more general perspective. The example of $\mathbb{Q}(i)$ is illustrative of a broader phenomenon of how complex multiplication can be used to construct abelian extensions of quadratic imaginary fields. Here, we will develop the machinery that is necessary to understand this phenomenon. The principal basis for this material comes from Silverman [4] and Lang [2].

4.1 The Endomorphism Ring of an Elliptic Curve E

In this section, our goal is to more completely describe the set of endomorphisms of an elliptic curve E, which we denote $\mathrm{End}(E)$. Previously, we saw that most endomorphisms of elliptic curves can be characterized as multiplication by n maps for $n \in \mathbb{Z}$, i.e.

$$\begin{aligned} \Omega_n \colon E &\to E, \\ P &\mapsto nP. \end{aligned}$$

In some cases, the elements of $\mathrm{End}(E)$ are exclusively multiplication by n maps, in which case, we obtain the obvious isomorphism $\mathrm{End}(E) \cong \mathbb{Z}$. The more interesting case to study is when E has complex multiplication, i.e. when $\mathrm{End}(E)$ contains an element which is not a multiplication by n map. To better understand $\mathrm{End}(E)$ when E has complex multiplication, we consider the complex-analytic representation of E.

Let $L = [\omega_1, \omega_2]$ be the lattice associated with E such that $E(\mathbb{C}) \cong \mathbb{C}/L$. In §3.3, we saw that endomorphisms of $\mathbb{C}/L$ can be characterized as multiplication by α maps, where α is a complex number such that $\alpha L \subset L$. If α is not an integer, we saw that α is strictly nonreal. We assume $\alpha \notin \mathbb{Z}$. If $\alpha L \subset L$, this places two algebraic conditions on α, namely that

$$\alpha\omega_1 = a\omega_1 + b\omega_2,$$

$$\alpha\omega_2 = c\omega_1 + d\omega_2,$$

for $a, b, c, d \in \mathbb{Z}$, because α takes any element of L to another element of L, and $[\omega_1, \omega_2]$ is a basis for L. With a bit of algebraic rearrangment, we see that

$$\omega_1(\alpha - a) = b\omega_2,$$

$$\omega_2(\alpha - d) = c\omega_1.$$

Dividing[11], this gives

$$\frac{\alpha - a}{c} = \frac{b}{\alpha - d}.$$

This implies

$$(\alpha - a)(\alpha - d) - bc = 0.$$

[11] We may divide, as α is not an integer by assumption, so $\alpha \neq d$.

In other words, α is a root of the monic quadratic polynomial with integer coefficients

$$f(x) = x^2 - (a+d)x - bc.$$

Furthermore, $f(x)$ is the minimal polynomial for α over $\mathbb{Q}$, since α is nonreal by assumption. Hence, α is a quadratic irrational over $\mathbb{Q}$, and is an algebraic integer in $\mathbb{Q}(\alpha)$. Since we wish to characterize all such α for a given elliptic curve E, we will not want to work with the extension $\mathbb{Q}(\alpha)$, as it is specific to α. We observe that

$$\alpha = c\left(\frac{\omega_1}{\omega_2}\right) + d$$

Since ω_1, ω_2 span a lattice, ω_1/ω_2 cannot be real. Put $\tau = \omega_1/\omega_2$. Since α is nonreal, it follows that $c \neq 0$, and thus $\mathbb{Q}(\alpha) = \mathbb{Q}(\tau)$. Let $K = \mathbb{Q}(\tau)$; α is therefore an element of the ring of algebraic integers in K, denoted $\mathcal{O}_k$. We observe that the set $R = \{\alpha \in \mathbb{Q}(\tau) \mid \alpha L \subset L\}$ is in fact a ring, since, for $\alpha_1, \alpha_2 \in R$

$$\alpha_1\alpha_2 L \subset L$$

and

$$(\alpha_1 - \alpha_2)L = \alpha_1 L - \alpha_2 L \subset L$$

Since $R \subset \mathcal{O}_K$, R is therefore a subring of $\mathcal{O}_K$, and we have $\mathrm{End}(E) \cong R$. We say that E has *complex multiplication by* R.

We end this section with an important note about $\mathrm{End}(E)$. If E has complex multiplication, then there are two ways to embed $\mathrm{End}(E)$ into $\mathbb{C}$, namely the identity map and its complex conjugate. It is important to choose one of these embeddings. This can be done via the following proposition, which we will state but not prove.

Proposition 4.1. *Let $E/\mathbb{C}$ be an elliptic curve with complex multiplication by the ring $R \subset \mathbb{C}$. There is a unique isomorphism*

$$[\cdot]\colon R \to \mathrm{End}(E)$$

such that for any invariant differential $\omega \in \Omega_E$ on E

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

We say in this case that the pair $(E, [\cdot])$ is normalized.

4.2 Elliptic Curves up to Isomorphism and the Ideal Class Group

The following material derives closely from Sections 1–3, Chapter II of Silverman.[4] Let $\Lambda = [\tau, 1]$ be a lattice in $\mathbb{C}$, and E_Λ be the elliptic curve such that $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$. Let K be the quadratic imaginary field $\mathbb{Q}(\tau)$. In the previous section, we saw that if E has complex multiplication, then $\mathrm{End}(E) \cong R \subset \mathcal{O}_K$. We will be mainly concerned with E such that $\mathrm{End}(E) \cong \mathcal{O}_K$. In fact, instead of focusing on a particular elliptic curve, it is most natural to study the set of elliptic curves (up to isomorphism) which have the same endomorphism ring. Hence, we define

$$\mathcal{E}(R) = \frac{\text{elliptic curves } E/\mathbb{C} \text{ with } \mathrm{End}(E) \cong R}{\text{isomorphism over } \mathbb{C}}.$$

We saw in section §2.4 that isomorphism classes of elliptic curves can be thought of as lattices up to homothety, so $\mathcal{E}(R)$ can be reframed as

$$\mathcal{E}(R) = \frac{\text{lattices } \Lambda \text{ with } \operatorname{End}(E_\Lambda) \cong R}{\text{homothety}}.$$

Our goal is to use complex multiplication to construct abelian extensions of quadratic imaginary fields. Instead of starting with an elliptic curve with complex multiplication, therefore, we will be more interested in starting with a quadratic imaginary field K and constructing an elliptic curve with complex multiplication by $\mathcal{O}_K$. We will need a lattice in K, and commutative algebra indicates a source. Consider a non-zero fractional ideal $\mathfrak{a} \subset K$. Since K is a quadratic imaginary field, $\mathfrak{a}$ is a $\mathbb{Z}$-module of rank 2 which is not contained in $\mathbb{R}$, and by the embedding $\mathfrak{a} \subset K \subset \mathbb{C}$ it is clear that $\mathfrak{a}$ is a lattice in $\mathbb{C}$. We may thus construct an elliptic curve $E_\mathfrak{a}$ with endomorphism ring

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

Hence, each non-zero fractional ideal of K gives rise to an elliptic curve with complex multiplication by $\mathcal{O}_K$. We really want to consider the set of elliptic curves with complex multiplication by $\mathcal{O}_K$ up to isomorphism, which can be accounted for by considering fractional ideals up to homothety. Since two fractional ideals $\mathfrak{a}, \mathfrak{b}$ are homothetic if $\mathfrak{a} = c\mathfrak{b}$ for some $c \in \mathbb{C}^\times$, we observe that two fractional ideals that differ by a non-zero principal ideal of K give the same elliptic curve. We are thus interested in the group of fractional ideals modulo principal ideals, i.e. the class group of $\mathcal{O}_K$:

$$\mathcal{CL}(\mathcal{O}_K) = \frac{\{\text{non-zero fractional ideals of } K\}}{\{\text{non-zero principal ideals of } K\}}.$$

We denote the ideal class of a fractional ideal $\mathfrak{a} \subset K$ by $\overline{\mathfrak{a}}$. If we start with a lattice Λ such that $E_\Lambda \in \mathcal{E}(\mathcal{O}_K)$ and a non-zero fractional ideal $\mathfrak{a} \subset K$, then we can form the product

$$\mathfrak{a}\Lambda = \{\alpha_1\lambda_1 + \cdots + \alpha_r\lambda_r \mid \alpha_i \in \mathfrak{a}, \lambda_i \in \Lambda\}$$

What does this product look like? We will soon show that $\mathfrak{a}\Lambda$ is in fact a lattice in $\mathbb{C}$, and moreover, $E_{\mathfrak{a}\Lambda}$ satisfies $\operatorname{End}(E_{\mathfrak{a}\Lambda}) \cong \mathcal{O}_K$. Using these facts, we can define a group action of $\mathcal{CL}(\mathcal{O}_k)$ on $\mathcal{E}(\mathcal{O}_k)$. We summarize this and more in the following proposition.

Proposition 4.2. *(a) Let Λ be a lattice such that $E_\Lambda \in \mathcal{E}(\mathcal{O}_K)$, and let $\mathfrak{a}, \mathfrak{b} \subset K$ be non-zero fractional ideals. Then*

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

(ii) The elliptic curve $E_{\mathfrak{a}\Lambda}$ satisfies $\operatorname{End}(E_{\mathfrak{a}\Lambda}) \cong \mathcal{O}_K$.

(iii) $E_{\mathfrak{a}\Lambda} \cong E_{\mathfrak{b}\Lambda}$ if and only if $\overline{\mathfrak{a}} = \overline{\mathfrak{b}}$ in $\mathcal{CL}(\mathcal{O}_K)$.

Thus there is a well-defined action of $\mathcal{CL}(\mathcal{O}_K)$ on $\mathcal{E}(\mathcal{O}_K)$ determined by

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

(b) The action of $\mathcal{CL}(\mathcal{O}_K)$ on $\mathcal{E}(\mathcal{O}_K)$ defined in part (a) is simply transitive. In particular,

$$|\mathcal{CL}(\mathcal{O}_K)| = |\mathcal{E}(\mathcal{O}_K)|$$

Proof. (a) (i) We must show that $\mathfrak{a}\Lambda$ is a discrete subgroup of $\mathbb{C}$ that spans $\mathbb{C}$ over $\mathbb{R}$. By assumption $\mathrm{End}(E_\Lambda) = \mathcal{O}_K$, so $\mathcal{O}_K\Lambda = \Lambda$. Since $\mathfrak{a}$ is a fractional ideal, there exists a non-zero integer $d \in \mathbb{Z}$ such that $d\mathfrak{a} \subset \mathcal{O}_K$. Right multiplying by Λ and left multiplying by d^{-1}, we obtain

$$d\mathfrak{a}\Lambda \subset \mathcal{O}_K\Lambda = \Lambda \implies \mathfrak{a}\Lambda \subset \frac{1}{d}\Lambda.$$

so $\mathfrak{a}\Lambda$ is a discrete subgroup of $\mathbb{C}$. Since we are in a Dedekind domain, $\mathfrak{a}$ has an inverse, $\mathfrak{a}^{-1}$, such that $\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}_K$. Since $\mathfrak{a}^{-1}$ is also a fractional ideal, we can similarly choose a non-zero integer $d' \in \mathbb{Z}$ such that $d'\mathfrak{a}^{-1} \subset \mathcal{O}_K$. Right multiplying both sides by $\mathfrak{a}$, we obtain

$$d'\mathfrak{a}^{-1}\mathfrak{a} \subset \mathcal{O}_K\mathfrak{a} \implies d'\mathcal{O}_K \subset \mathfrak{a}.$$

Right multiplying by Λ we obtain

$$d'\mathcal{O}_K\Lambda \subset \mathfrak{a}\Lambda \implies d'\Lambda \subset \mathfrak{a}\Lambda.$$

Thus, $\mathfrak{a}\Lambda$ spans $\mathbb{C}$, proving $\mathfrak{a}\Lambda$ is a lattice.

(ii) For any $\alpha \in \mathbb{C}$, we have

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

Therefore, $\alpha \in \mathrm{End}(E_{\mathfrak{a}\Lambda})$ if and only if $\alpha \in \mathrm{End}(E_\Lambda) = \mathcal{O}_K$, so $\mathrm{End}(E_{\mathfrak{a}\Lambda}) = \mathcal{O}_K$.

(iii) From §2.4, $E_{\mathfrak{a}\Lambda} \cong E_{\mathfrak{b}\Lambda}$ if and only if $\mathfrak{a}\Lambda$ is homothetic to $\mathfrak{b}\Lambda$, i.e. if there exists $c \in \mathbb{C}^\times$ such that $\mathfrak{a}\Lambda = c\mathfrak{b}\Lambda$. Left multiplying by $\mathfrak{a}^{-1}$ tells us that

$$\mathfrak{a}\Lambda = c\mathfrak{b}\Lambda \iff \mathfrak{a}^{-1}\mathfrak{a}\Lambda = c\mathfrak{a}^{-1}\mathfrak{b}\Lambda \iff \mathcal{O}_K\Lambda = c\mathfrak{a}^{-1}\mathfrak{b}\Lambda \iff \Lambda = c\mathfrak{a}^{-1}\mathfrak{b}\Lambda$$

where we have used the fact that $\mathcal{O}_K\Lambda = \Lambda$. Similarly, if we left multiply by $c^{-1}\mathfrak{b}^{-1}$, we see

$$\mathfrak{a}\Lambda = c\mathfrak{b}\Lambda \iff c^{-1}\mathfrak{b}^{-1}\mathfrak{a}\Lambda = c^{-1}\mathfrak{b}^{-1}c\mathfrak{b}\Lambda \iff c^{-1}\mathfrak{a}\mathfrak{b}^{-1}\Lambda = \mathcal{O}_K\Lambda \iff \Lambda = c^{-1}\mathfrak{a}\mathfrak{b}^{-1}\Lambda$$

Hence, if $\mathfrak{a}$ is homothetic to $\mathfrak{b}$, then both $c\mathfrak{a}^{-1}\mathfrak{b}$ and $c^{-1}\mathfrak{a}\mathfrak{b}^{-1}$ take Λ to itself, so they both are contained in $\mathcal{O}_K$. Thus

$$c\mathfrak{a}^{-1}\mathfrak{b} \subset \mathcal{O}_K \implies c\mathfrak{a}\mathfrak{a}^{-1}\mathfrak{b} \subset \mathfrak{a}\mathcal{O}_K \implies c\mathcal{O}_K\mathfrak{b} \subset \mathfrak{a} \implies c\mathfrak{b} \subset \mathfrak{a}$$

and

$$c^{-1}\mathfrak{a}\mathfrak{b}^{-1} \subset \mathcal{O}_K \implies cc^{-1}\mathfrak{a}\mathfrak{b}^{-1}\mathfrak{b} \subset c\mathfrak{b}\mathcal{O}_K \implies \mathfrak{a}\mathcal{O}_K \subset c\mathfrak{b} \implies \mathfrak{a} \subset c\mathfrak{b}$$

so

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

Since both $\mathfrak{a}, \mathfrak{b} \subset K$, it follows that $c \in K$ and thus $\overline{\mathfrak{a}} = \overline{\mathfrak{b}}$. Conversely, if $\overline{\mathfrak{a}} = \overline{\mathfrak{b}}$, then $c^{-1}\mathfrak{a}\mathfrak{b}^{-1} = \mathcal{O}_K$ for some $c \in \mathbb{C}^\times$ and hence $\mathfrak{a}\Lambda$ and $\mathfrak{b}\Lambda$ are homothetic. We observe that

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

showing that $\overline{\mathfrak{a}} * E_\Lambda = E_{\mathfrak{a}^{-1}\Lambda}$ gives a left group action of $\mathcal{CL}(\mathcal{O}_K)$ on $\mathcal{E}(\mathcal{O}_K)$.

(b) To show that the class group $\mathcal{CL}(\mathcal{O}_K)$ acts transitively on $\mathcal{E}(\mathcal{O}_K)$, we must show that there is one orbit under the action $*$. Let two elliptic curves $E_{\Lambda_1}, E_{\Lambda_2} \in \mathcal{E}(\mathcal{O}_K)$ be given. We must find a fractional ideal $\mathfrak{a}$ such that $\overline{\mathfrak{a}} * E_{\Lambda_1} = E_{\Lambda_2}$. Choose any non-zero element $\lambda_1 \in \Lambda_1$, and note that the lattice $\mathfrak{a}_1 = \frac{1}{\lambda_1}\Lambda_1$ is a fractional ideal of K, because $\mathfrak{a}_1 \subset K$ and by assumption it is a finitely generated $\mathcal{O}_K$-module. We similarly choose a non-zero $\lambda_2 \in \Lambda_2$ to obtain the second fractional ideal $\mathfrak{a}_2 = \frac{1}{\lambda_2}\Lambda_2$. Then

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

Hence we construct $\mathfrak{a} = \mathfrak{a}_2^{-1}\mathfrak{a}_1$ and observe

$$\overline{\mathfrak{a}} * E_{\Lambda_1} = E_{\mathfrak{a}^{-1}\Lambda_1} = E_{\mathfrak{a}_2\mathfrak{a}_1^{-1}\Lambda_1} = E_{\frac{\lambda_1}{\lambda_2}\Lambda_2} \cong E_{\Lambda_2}.$$

To prove that the action is simply transitive, we must show that $\mathfrak{a} * E_\Lambda = \mathfrak{b} * E_\lambda$ implies $\overline{\mathfrak{a}} = \overline{\mathfrak{b}}$. This is clear, as

$$\mathfrak{a} * E_\Lambda = \mathfrak{b} * E_\Lambda \implies E_{\mathfrak{a}^{-1}\Lambda} = E_{\mathfrak{b}^{-1}\Lambda}$$

which by part (iii) of (a) implies that $\overline{\mathfrak{a}^{-1}} = \overline{\mathfrak{b}^{-1}}$, whence we obtain $\overline{\mathfrak{a}} = \overline{\mathfrak{b}}$.

□

Since the ideal class group $\mathcal{CL}(\mathcal{O}_K)$ is always finite, we immediately obtain the following corollary from part (b) above.

Corollary 4.3. *There is a one-to-one correspondence between isomorphism classes of elliptic curves in $\mathcal{E}(\mathcal{O}_K)$ and ideal classes in $\mathcal{CL}(\mathcal{O}_K)$. There are only finitely many isomorphism classes of elliptic curves with multiplication by $\mathcal{O}_K$.*

To construct abelian extensions of $\mathbb{Q}(i)$, it was necessary in §3.2 to study the points of order m on an elliptic curve E for various integers m, which we denoted $E[m]$. If E has complex multiplication by a quadratic imaginary field K, we will still be interested in torsion points, but there is a broader class of finite subgroups to look at. Namely, if $\mathfrak{a}$ is an integral ideal of $\mathcal{O}_K$, then we define the **group of $\mathfrak{a}$-torsion points of** E to be

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

We can describe the m-torsion points $E[m]$ as $\mathfrak{a}$-torsion points by setting $\mathfrak{a} = m\mathcal{O}_K$. Note that in the definition of $E[\mathfrak{a}]$ we have chosen an embedding of $\mathrm{End}(E)$ into $\mathbb{C}$; we can always do this by Proposition 4.1 and we will always choose the normalized isomorphism.

Previously, we understood $E[m]$ as the kernel of the multiplication-by-m endomorphism. There is a similar way to understand $E[\mathfrak{a}]$. If $\mathfrak{a}$ is an integral ideal of $\mathcal{O}_K$, then

$$\mathfrak{a}\Lambda \subset \mathcal{O}_K\Lambda = \Lambda \implies \mathfrak{a}^{-1}\mathfrak{a}\Lambda \subset \mathfrak{a}^{-1}\Lambda \iff \Lambda \subset \mathfrak{a}^{-1}\Lambda.$$

Hence, there an inclusion homomorphism of quotient groups

$$\mathbb{C}/\Lambda \to \mathbb{C}/\mathfrak{a}^{-1}\Lambda, \quad z \mapsto z.$$

Since $\mathbb{C}/\Lambda \cong E_\Lambda$ and $\mathbb{C}/\mathfrak{a}^{-1}\Lambda \cong E_{\mathfrak{a}^{-1}\Lambda} = \overline{\mathfrak{a}} * E$, this induces a coresponding isogeny

$$E_\Lambda \to \overline{\mathfrak{a}} * E_\Lambda.$$

This isogeny provides a valuable way to understand $E[\mathfrak{a}]$, noted in the proposition below.

Proposition 4.4. *Let $E \in \mathcal{E}(\mathcal{O}_K)$, and let $\mathfrak{a}$ be an integral ideal of $\mathcal{O}_K$. Then $E[\mathfrak{a}]$ is the kernel of the isogeny $E \to \overline{\mathfrak{a}} * E$.*

Proof. Let Λ be a lattice corresponding to E. Since $C/\Lambda \cong E(\mathbb{C})$, we observe

$$\begin{aligned} E[\mathfrak{a}] \cong &\{z \in \mathbb{C}/\Lambda \mid \alpha z = 0 \text{ for all } \alpha \in \mathfrak{a}\} \\ =&\{z \in \mathbb{C} \mid \alpha z \in \Lambda \text{ for all } \alpha \in \mathfrak{a}\}/\Lambda \\ =&\{z \in \mathbb{C} \mid z\mathfrak{a} \subset \Lambda\}/\Lambda \\ =&\mathfrak{a}^{-1}\Lambda/\Lambda \\ =&\ker\left(\mathbb{C}/\Lambda \to \mathbb{C}/\mathfrak{a}^{-1}\Lambda\right) \\ =&\ker(E \to \overline{\mathfrak{a}} * E). \end{aligned}$$

□

In Proposition 4.4, we observed that $E[\mathfrak{a}] \cong \mathfrak{a}^{-1}\Lambda/\Lambda$ as $\mathcal{O}_K/\mathfrak{a}$-modules. We may further describe $E[\mathfrak{a}]$ as follows.

Proposition 4.5. *$E[\mathfrak{a}]$ is a free $\mathcal{O}_K/\mathfrak{a}$-module of rank 1.*

We now prove an important proposition about the j-invariant.

Proposition 4.6. *(a) Let $E/\mathbb{C}$ be an elliptic curve, and let $\sigma : \mathbb{C} \to \mathbb{C}$ be any field automorphism of $\mathbb{C}$. Then*

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

(b) Let $E/\mathbb{C}$ be an elliptic curve with complex multiplication by the ring of integers $\mathcal{O}_K$ of a quadratic imaginary field K. Then $j(E)$ is algebraic.

Proof. (a) This is evident. Let $\phi\colon E \to E$ be an endomorphism of E. Since ϕ^σ is obtained from ϕ by letting σ act on the coefficients of ϕ, it is clear that ϕ^σ is an endomorphism of the elliptic curve obtained from E by letting σ act on the coefficients of a Weierstrass equation for E, i.e. E^σ. Hence, $\phi^\sigma\colon E^\sigma \to E^\sigma$ is an endomorphism of E^σ.

(b) Let $\sigma \in \mathrm{Aut}(\mathbb{C})$ as in (a). Let E be given by the Weierstrass equation $y^2 = 4x^3 - g_2x - g_3$. Then E^σ is given by the Weierstrass equation $y^2 = 4x^3 - \sigma(g_2)x - \sigma(g_3)$. From the definition of the j-invariant in §2.4, we see

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

From part (a), we know $\mathrm{End}(E^\sigma) \cong \mathcal{O}_K$, so E^σ is in a unique $\mathbb{C}$-isomorphism class in $\mathcal{E}(\mathcal{O}_K)$. But from Proposition 4.2, $|\mathcal{E}(\mathcal{O}_K)| = |\mathcal{CL}(O_K)|$, which is finite. Let $|\mathcal{CL}(O_K)| = h_K$. Then we see that E^σ is an element of one of h_K $\mathbb{C}$-isomorphism classes of elliptic curves. From §2.4, an elliptic curve's $\mathbb{C}$-isomorphism class is determined by its j-invariant, and so in particular, we see that $j(E)^\sigma$ takes on at most h_K values as σ ranges over $\mathrm{Aut}(\mathbb{C})$. Thus, we have $[\mathbb{Q}(j(E))]\colon \mathbb{Q}] \leq h_K$, so $j(E)$ is algebraic.

□

Starting with an elliptic curve E over $\mathbb{C}$, Proposition 4.6 can be used to prove the important fact that $\mathcal{E}(\mathcal{O}_K)$ can be defined up to isomorphism over $\overline{\mathbb{Q}}$. We state this without proof, as well as two important facts about the field of definition of complex multiplication elliptic curves and their endomorphisms, in the following proposition.

Proposition 4.7. *(a)*

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

(b) Let E be an elliptic curve defined over a field $L \subset \mathbb{C}$ and with complex multiplication by the imaginary quadratic field $K \subset \mathbb{C}$. Then every endomorphism of E is defined over the compositum LK.

(c) 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'.

In §3.1, we constructed abelian extensions of $\mathbb{Q}$ by showing there was an injective homomorphism from $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ into $(\mathbb{Z}/n\mathbb{Z})^\times$. Similarly, in §3.2, we showed there was an injective homomorphism from $\mathrm{Gal}(\mathbb{Q}(i)(E[n]))/\mathbb{Q}(i))$ into a subgroup of $GL_2(\mathbb{Z}/n\mathbb{Z})$, which we later showed was abelian. We now introduce a yet more general form of this idea using the torsion points on E.

Theorem 4.8. *Let $E/\mathbb{C}$ be an elliptic curve with complex multiplication by the ring of integers $\mathcal{O}_K$ of a quadratic imaginary field K, and let*

$$L = K(j(E), E_{\mathrm{tors}})$$

be the field generated by the j-invariant of E and the coordinates of all of the torsion points of E. Then L is an abelian extension of $K(j(E))$.

Proof. Let $H = K(j(E))$, and let

$$L_m = H(E[m])$$

be the extension of H generated by the m-torsion points of E for $m \in \mathbb{N}$. Since L is the compositum of all the L_m's, it suffices to show that L_m is an abelian extension of H. The principle is the same as before. Elements of the Galois group $\mathrm{Gal}(L_m/H)$ are determined by where they map the generators of L_m over H, i.e. the m-torsion points of E. Hence, elements of $\mathrm{Gal}(L_m/H)$ are in correspondence with elements of $\mathrm{Aut}(E[m])$. In formal terms, there is a representation

$$\rho\colon\ \mathrm{Gal}(\overline{K}/H) \to \mathrm{Aut}(E[m])$$

determined by the condition

$$\rho(\sigma)P = P^\sigma \qquad \text{for all } \sigma \in \mathrm{Gal}(\overline{K}/H) \text{ and all } P \in E[m].$$

We saw before that from this alone, we could deduce that the restriction of ρ to $\mathrm{Gal}(L_m/H)$ gives an injection into the automorphism group of $E[m]$, which we found was a subgroup of $GL_2(\mathbb{Z}/m\mathbb{Z})$.

The fact that our elliptic curve E has complex multiplication tells us more. We take a model for E defined over H, and then Proposition 4.7 tells us that every element of $\mathrm{End}(E)$ is also defined over H. Hence, elements of $\mathrm{End}(E)$ are fixed by every $\sigma \in Gal(L_m/H)$, and so elements of $\mathrm{Gal}(L_m/H)$ commute with elements of $\mathrm{End}(E)$ in their action on $E[m]$:

$$([\alpha]P)^\sigma = [\alpha]P^\sigma \qquad \text{for all } \sigma \in \mathrm{Gal}(\overline{K}/H), P \in E[m] \text{ and } \alpha \in \mathcal{O}_K$$

Hence, ρ is a homomorphism from $\mathrm{Gal}(\overline{K}/H)$ to the group of $\mathcal{O}_K/m\mathcal{O}_K$-module automorphisms of $E[m]$. Therefore, ρ induces the injection

$$\phi : \mathrm{Gal}(L_m/H) \to \mathrm{Aut}_{\mathcal{O}_K/m\mathcal{O}_K}(E[m])$$

By applying Proposition 4.5, this says that $E[m]$ is a free $\mathcal{O}_K/m\mathcal{O}_K$-module of rank one. Hence, the $\mathcal{O}_K/m\mathcal{O}_K$-module automorphisms of $E[m]$ are the units of $\mathcal{O}_K/m\mathcal{O}_K$, i.e.

$$\mathrm{Aut}_{\mathcal{O}_K/m\mathcal{O}_K}(E[m]) \cong (\mathcal{O}_K/m\mathcal{O}_K)^\times$$

Since $(\mathcal{O}_K/m\mathcal{O}_K)^\times$ is abelian, we therefore have $\mathrm{Gal}(L_m/H)$ is abelian. □

We can readily see the power of Theorem 4.8. We saw in §3.4 that the elliptic curve $E : y^2 = x^3 + x$ has complex multiplication via the map $(x, y) \mapsto (-x, iy)$. In fact, it can be shown that E has complex multiplication by $\mathbb{Z}[i]$, the ring of integers in $\mathbb{Q}(i)$. Put $K = \mathbb{Q}(i)$. We may readily see that

$$j(E) = 1728\frac{(-1)^3}{(-1)^3 - 0^2} = 1728$$

Hence, $K(j(E)) = K(1728) = K$. Thus, by Theorem 4.8, $K(j(E), E_{\mathrm{tors}}) = K(E_{\mathrm{tors}})$ is an abelian extension of $K(j(E)) = K$. This is just what we saw in §3.4 but now from a considerably more general point of view.

We continue to push our understanding of this general point of view. Let K be a quadratic imaginary field, and let E be a curve with complex multiplication by $\mathcal{O}_K$. We will be

interested in characterizing $K(j(E))$ in a similar way to how we have have characterized $K(j(E), E_{\text{tors}})$ above. In particular, we will show that $K(j(E))$ is an abelian extension of K[12]. This will require some additional machinery, which we will develop shortly, but in principle, the way we understood $K(j(E), E_{\text{tors}})$ was through the description of how elements of $\text{Gal}(\overline{K}/K(j(E)))$ act on $E[m]$. Similarly, we will understand $K(j(E))$ through the description of how elements of $\text{Gal}(\overline{K}/K)$ act on $j(E)$.

We may use Proposition 4.7 to identify $\mathcal{E}(\mathcal{O}_K)$ as the $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves having complex multiplication by $\mathcal{O}_K$ from here on. This way, there is a natural action of $\text{Gal}(\overline{K}/K)$ on $\mathcal{E}(\mathcal{O}_K)$ where $\sigma \in \text{Gal}(\overline{K}/K)$ sends the isomorphism class of E to the isomorphism class of E^σ. This is not so different from the action we described in Proposition 4.2. In particular, because the action of the class group $\mathcal{CL}(\mathcal{O}_K)$ on $\mathcal{E}(\mathcal{O}_K)$ is simply transitive, there is a unique ideal class $\overline{\mathfrak{a}} \in \mathcal{CL}(\mathcal{O}_K)$ depending on σ such that $\mathfrak{a} * E = E^\sigma$. This gives rise to a well-defined map

$$F\colon \text{Gal}(\overline{K}/K) \to \mathcal{CL}(\mathcal{O}_K)$$

characterized by the property

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

We can put this correspondence in terms of the analytic picture of E as well, primarily through the j-invariant, since isomorphism classes of E correspond to classes of elliptic curves sharing the same j-invariant. In particular, let $j(\Lambda)$ be the j-invariant of the elliptic curve E_Λ. Then since

$$E_\Lambda^\sigma = F(\sigma) * E_\Lambda = E_{F(\sigma)^{-1}\Lambda} \text{ for all } \sigma \in \text{Gal}(\overline{K}/K).$$

Since the j-invariant of E_Λ^σ is σ applied to the j-invariant of E_Λ, we obtain

$$j(\Lambda)^\sigma = j(F(\sigma)^{-1}\Lambda).$$

Hence, by understanding the map F, we can precisely describe the field $K(j(E))$. We now prove that F is a homomorphism, and in fact, F is independent of the choice of the elliptic curve $E \in \mathcal{E}(\mathcal{O}_K)$.

Proposition 4.9. *Let $K/\mathbb{Q}$ be a quadratic imaginary field. There exists a homomorphism*

$$F\colon \text{Gal}(\overline{K}/K) \to \mathcal{CL}(\mathcal{O}_K)$$

uniquely characterized by the condition

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

Proof. We have already defined F. To show F is a homomorphism, for $\sigma, \tau \in \text{Gal}(\overline{K}/K)$, we compute

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

[12]In fact, $K(j(E))$ is the maximal unramified abelian extension of K, or the **Hilbert class field** of K. See [4] for more.

where we have used that $\mathcal{CL}(\mathcal{O}_K)$ is abelian. Thus, $F(\sigma\tau) = F(\sigma)F(\tau)$ as desired.

Let $E_1, E_2 \in \mathcal{E}(\mathcal{O}_K)$ and $\sigma \in \mathrm{Gal}(\overline{K}/K)$. We have just shown that for $\sigma \in \mathrm{Gal}(\overline{K}/K)$, there exist ideal classes $\overline{\mathfrak{a}}_1, \overline{\mathfrak{a}}_2 \in \mathcal{CL}(\mathcal{O}_K)$ such that $E_1^\sigma = \overline{\mathfrak{a}}_1 * E_1$ and $E_2^\sigma = \overline{\mathfrak{a}}_2 * E_2$. To show that F is independent of the choice of E, we must show that $\overline{\mathfrak{a}}_1 = \overline{\mathfrak{a}}_2$. By Proposition 4.2(b), there exists an ideal class $\overline{\mathfrak{b}} \in \mathcal{CL}(\mathcal{O}_K)$ such that $E_2 = \overline{\mathfrak{b}} * E_1$. Note that $\overline{\mathfrak{b}}^\sigma = \overline{\mathfrak{b}}$, since $\mathfrak{b} \subset K$ and σ fixes K. Then

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

If σ commutes with the action of $\mathcal{CL}(\mathcal{O}_K)$ on $\mathcal{E}(\mathcal{O}_K)$, i.e. $(\overline{\mathfrak{b}} * E_1)^\sigma = \overline{\mathfrak{b}} * E_1^\sigma$, then we can cancel $\overline{\mathfrak{b}}$ from both sides to deduce $E_1^\sigma = (\overline{\mathfrak{a}}_2\overline{\mathfrak{a}}_1^{-1}) * E_1^\sigma$, which by Proposition 4.2(iii) gives $\overline{\mathfrak{a}}_1 = \overline{\mathfrak{a}}_2$. This is the analogue of $\mathrm{End}(E)$ commuting with the Galois action on $E[m]$. We state this in the following lemma which we do not prove, completing the proof.

Lemma 4.10. *Let $E/\overline{\mathbb{Q}}$ be an elliptic curve representing an element of $\mathcal{E}(\mathcal{O}_K)$, let $\overline{\mathfrak{a}} \in \mathcal{CL}(\mathcal{O}_K)$, and let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Then*

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

□

Having proved Proposition 4.9, we can now show that $K(j(E))$ is an abelian extension of K.

Theorem 4.11. *Let K be an imaginary quadatic field, and let E be an elliptic curve representing an isomorphism class in $\mathcal{E}(\mathcal{O}_K)$. Then $K(j(E))$ is an abelian extension of K.*

Proof. With the help of Proposition 4.9, the proof is surprisingly simple. Let L be the fixed field of the kernel of the homomorphism $F\colon \mathrm{Gal}(\overline{K}/K) \to \mathcal{CL}(\mathcal{O}_K)$, i.e. $\mathrm{Gal}(\overline{K}/L) = \ker F$. Then

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

Hence, $L = K(j(E))$. Furthermore, since

$$\mathrm{Gal}(L/K) \cong \mathrm{Gal}(\overline{K}/K)/\mathrm{Gal}(\overline{K}/L) = \mathrm{Gal}(\overline{K}/K)/\ker F$$

it follows that F maps $\mathrm{Gal}(L/K)$ injectively into $\mathcal{CL}(\mathcal{O}_K)$. $\mathcal{CL}(\mathcal{O}_K)$ is an abelian group, hence $\mathrm{Gal}(L/K)$ is abelian. □

Recall from §2.4 that isomorphic elliptic curves have the same j-invariant, and two elliptic curves are isomorphic if and only if their underlying lattices are homothetic. Since each τ in the upper half-plane $\mathbb{H}$ gives a unique lattice up to homothety, it follows that we can view the j-invariant as a function on $\mathbb{H}$. It can in fact be shown that the function $j(\tau)$ is holomorphic on $\mathbb{H}$. Hence, by showing that $K(j(E))$ is an abelian extension of K when E has complex multiplication by $\mathcal{O}_K$, we have constructed an abelian extension of K by adjoining special values of a holomorphic function.

5 Real Multiplication

We conclude our survey of the theory of complex multiplication with a brief excursion into the work of Shimura on constructing abelian extensions of real quadratic fields. We will be primarily be concerned with Shimura's seminal paper "Class Fields over Real Quadratic Fields and Hecke Operators", which gives the axiomatic formulation of the theory of "real multiplication"[5], and shows how the necessary components may be constructed, first from certain modular forms and secondly from certain elliptic curves. This theory is built out of machinery that closely resembles the tools we have just developed in the theory of complex multiplication. The following material heavily draws from Shimura's exposition in [7].

Let F be a totally real algebraic number field of finite degree, and K a totally imaginary quadratic extension of F. We call such a K a **CM-field**.

Let ρ denote complex conjugation. Consider the following objects A, θ, η, k satisfying the following conditions:

1) k is a real quadratic extension of $\mathbb{Q}$.

2) A is an abelian variety of dimension $[K\colon \mathbb{Q}]$.

3) θ is an injective homomorphism of K into $\mathrm{End}(A) \otimes \mathbb{Q}$.

4) A and the elements of $\theta(K) \cap \mathrm{End}(A)$ are rational over $\mathbb{Q}$.

5) η is an automorphism of A rational over k, $\eta^2 = 1$, $\eta \circ \theta(a) = \theta(a^\rho) \circ \eta$ for all $a \in K$, and $\eta^\varepsilon = -\eta$, where ε denotes the generator of $\mathrm{Gal}(k/\mathbb{Q})$.

Our goal in this section is to construct abelian extensions of k. Let $\mathcal{O}_F$ and $\mathcal{O}_K$ denote the ring of integers in F and K, respectively. Changing A by isogeny over $\mathbb{Q}$, we may assume

$$\theta(\mathcal{O}_K) \subset \mathrm{End}(A)$$

Put $n = [F\colon \mathbb{Q}]$ and let $B = (1+\eta)A$. Then $\dim(A) = [K\colon \mathbb{Q}] = [K\colon F][F\colon \mathbb{Q}] = 2n$, and

$$B^\varepsilon = ((1+\eta)A)^\varepsilon = (1+\eta^\varepsilon)A^\varepsilon = (1-\eta)A$$

since A is rational over $\mathbb{Q}$. Further, we observe

$$A = B + B^\varepsilon$$

Since ε is a k-linear isomorphism between B and B^ε, it follows that $\dim(B) = n$. One can also show that $B \cap B^\epsilon$ is a finite group annihilated by 2. Let $\mathfrak{b}_0$ be the ideal of $\mathcal{O}_K$ generated by all x in $\mathcal{O}_K$ such that $x^\rho = -x$. We can define the "odd part" $\mathfrak{b}$ of $\mathfrak{b}_0$ by the properties

(i) $\mathfrak{b}$ is a divisor of $\mathfrak{b}_0$ relatively prime to 2;

(ii) $N(\mathfrak{b}^{-1}\mathfrak{b}_0)$ is a power of 2.

We will be interested in the $\mathfrak{b}$-torsion points of A, so we are interested in how $\mathfrak{b}$ factors as a product of prime ideals in $\mathcal{O}_K$. We will need to make a brief number-theoretic digression to address this consideration. Let $\alpha \in \mathcal{O}_K$, and let $f(x)$ be the minimal polynomial of α over F. Note $\deg(f(x)) \leq 2$. We define the **different of** α, denoted $\delta_{K/F}(\alpha)$ by

$$\delta_{K/F}(\alpha) = \begin{cases} f'(\alpha) & \text{if } K = F(\alpha) \\ 0 & \text{otherwise.} \end{cases}$$

Suppose $\deg(f(x)) = 2$. Then $f(x) = x^2 + bx + c$ for some $b, c \in F$, and $f'(x) = 2x + b$. Put $\Delta_{f(x)} = b^2 - 4c$. Then since K is a totally imaginary quadratic extension of F and $\deg(f(x)) = 2$, we have $\Delta_{f(x)} < 0$ and

$$\alpha = \frac{-b \pm \sqrt{\Delta_{f(x)}}}{2}$$

and

$$\delta_{K/F}(\alpha) = f'(\alpha) = \pm\sqrt{\Delta_{f(x)}}.$$

Hence, since $\Delta_{f(x)} < 0$, $\delta_{K/F}(\alpha) \in \mathfrak{b}_0$. Define the **different of** K **relative to** F, denoted $D_{K/F}$, by the ideal generated by $\delta_{K/F}(\alpha)$ for all $\alpha \in \mathcal{O}_K$. Then it is clear that $\mathfrak{b}_0$ divides $D_{K/F}$, so $\mathfrak{b}$ divides $D_{K/F}$. Rewrite $\mathfrak{b}$ as a product of prime ideals so that

$$\mathfrak{b} = \mathfrak{P}_1^{l_1}\mathfrak{P}_2^{l_2}\cdots\mathfrak{P}_k^{l_k}$$

where each $\mathfrak{P}_i$ is a prime ideal in $\mathcal{O}_K$ lying over a prime ideal $\mathfrak{p}_i$ in $\mathcal{O}_F$ and each l_i is a positive integer. Let e_i be the ramification index of $\mathfrak{p}_i$ in K. Since $[K\colon F] = 2$, each e_i satisfies $1 \leq e_i \leq 2$. Furthermore, since $\mathfrak{b} \mid D_{K/F}$ it follows that each $\mathfrak{P}_i$ divides $D_{K/F}$. Algebraic number theory tells us that $\mathfrak{P}_i \mid D_{K/F}$ if and only if $\mathfrak{p}_i$ is ramified in $\mathcal{O}_K$ *and* $s_i = e_i - 1$ is the largest integer such that $\mathfrak{P}_i^{s_i} \mid D_{K/F}$. Then we see immediately that $e_i = 2$ and $s_i = 1$ for all i. Hence, $l_i = 1$ for all i, and thus $\mathfrak{b}$ is square-free, so

$$\mathfrak{b} = \mathfrak{P}_1\mathfrak{P}_2\cdots\mathfrak{P}_k.$$

Furthermore, since $e_i = 2$ for each i, we have

$$\mathfrak{P}_i^2 = \mathcal{O}_K\mathfrak{p}_i$$

Note that $\mathfrak{P}_i^\rho$ is another prime ideal lying over $\mathfrak{p}_i$. Since $\mathfrak{P}_i^2 = \mathcal{O}_K\mathfrak{p}_i$, it follows that $\mathfrak{P}_i^\rho = \mathfrak{P}_i$. Hence, $\mathfrak{b}^\rho = \mathfrak{b}$. Put $\tau = \prod_{i=1}^k \mathfrak{p}_i$. By definition, τ is square-free. We see

$$\mathfrak{b}^2 = \mathfrak{P}_1^2\mathfrak{P}_2^2\cdots\mathfrak{P}_k^2 = \mathcal{O}_K\mathfrak{p}_1\mathcal{O}_K\mathfrak{p}_2\ldots\mathcal{O}_K\mathfrak{p}_k = \mathcal{O}_K\prod_{i=1}^k \mathfrak{p}_i = \mathcal{O}_K\tau.$$

Since each $\mathfrak{p}_i$ is ramified with $e_i = 2 = [K\colon F]$, the inertial degree of $\mathfrak{p}_i$ is 1. Hence, this tells us

$$\mathcal{O}_K/\mathfrak{P}_i \cong \mathcal{O}_F/\mathfrak{p}_i$$

for each i. Using the Chinese remainder theorem, it is clear that $\mathcal{O}_K/\mathfrak{b}$ is isomorphic to $\mathcal{O}_F/\tau$ as $\mathcal{O}_F$-modules, as

$$\mathcal{O}_K/\mathfrak{b} = \mathcal{O}_K/\mathfrak{P}_1 \times \mathcal{O}_K/\mathfrak{P}_2 \times \cdots \times \mathcal{O}_K/\mathfrak{P}_k = \mathcal{O}_F/\mathfrak{p}_1 \times \mathcal{O}_F/\mathfrak{p}_2 \times \cdots \times \mathcal{O}_F/\mathfrak{p}_k = \mathcal{O}_F/\tau$$

We may now fruitfully study the $\mathfrak{b}$-torsion points of A. Put

$$\mathcal{C} = \{t \in A \mid \theta(\mathfrak{b})t = 0\}$$

Proposition 7.20 of [6] tells us that $\mathcal{C}$ is isomorphic to $(\mathcal{O}_K/\mathfrak{b})^2$ as $\mathcal{O}_K$-modules, which means that $\mathcal{C}$ is isomorphic to $(\mathcal{O}_F/\tau)^2$ as $\mathcal{O}_F$-modules. Put

$$\mathcal{Y} = B \cap \mathcal{C},\ \mathcal{Z} = B^\varepsilon \cap \mathcal{C}.$$

The elements of $B \cap B^\varepsilon$ have order 2, so an element $\kappa \in \mathcal{Y} \cap \mathcal{Z}$ is killed by $\theta(2)$ and $\theta(\mathfrak{b})$. But $\mathfrak{b}$ is relatively prime to 2, so κ is also killed by 1 and hence is zero. Thus, one can see that $\mathcal{C} = \mathcal{Y} \oplus \mathcal{Z}$. Furthermore, one may observe that ε is an automorphism of $\mathcal{C}$, as θ is rational over $\mathbb{Q}$ and therefore commutes with ε. Hence, ε is an isomorphism between $\mathcal{Y}$ and $\mathcal{Z}$, and thus, $\mathcal{Y}$ and $\mathcal{Z}$ are isomorphic to $\mathcal{O}_F/\tau$ as $\mathcal{O}_F$-modules.

Let $k(\mathcal{Y})$ denote the field generated over k by the coordinates of the points of $\mathcal{Y}$. Let $\sigma\colon k(\mathcal{Y}) \to \mathbb{C}$ be an injective homomorphism of fields which is the identity on k. Then σ induces an action on points of A (denoted also by σ) and since elements of $\theta(\mathfrak{b})$ are rational over $\mathbb{Q}$, it follows that σ commutes with $\theta(\mathfrak{b})$, and hence σ takes $\mathcal{C}$ to itself. Furthermore, σ commutes with η since η is rational over k, so we can see that σ takes B to itself. Thus σ takes $\mathcal{Y}$ to itself, and it follows that $\sigma(k(\mathcal{Y})) \subset k(\mathcal{Y})$. The extension $k(\mathcal{Y})$ is therefore normal over k. Much like in the case of quadratic imaginary fields, the action of $\mathrm{Gal}(k(\mathcal{Y})/k)$ on $\mathcal{Y}$ gives an injection from $\mathrm{Gal}(k(\mathcal{Y})/k)$ into $\mathrm{Aut}(\mathcal{Y})$. As above, the action of Galois elements commutes with the action of $\mathcal{O}_F$ via θ, so this injection lands in the $\mathcal{O}_F$-automorphisms of $\mathcal{Y}$. Since $\mathcal{Y}$ is isomorphic to $\mathcal{O}_F/\tau$ as an $\mathcal{O}_F$-module, the $\mathcal{O}_F$-automorphisms of $\mathcal{Y}$ are the $\mathcal{O}_F$-module automorphisms of $\mathcal{O}_F/\tau$, i.e. the units $(\mathcal{O}_F/\tau)^\times$. Hence, we obtain an injective homomorphism

$$\mathrm{Gal}(k(\mathcal{Y})/k) \to (\mathcal{O}_F/\tau)^\times.$$

Since $(\mathcal{O}_F/\tau)^\times$ is an abelian group, $\mathrm{Gal}(k(\mathcal{Y})/k)$ must also be abelian, as desired. We see that this construction quite closely resembles the construction of abelian extensions of quadratic imaginary fields.

To conlcude, we remark that we can in fact construct A, θ, η satisfying the axiomatic conditions outlined above. The following construction is due entirely to Shimura [5]. Let k be a real quadratic field, and let E be an elliptic curve rational over k satisfying the following condition: If ε is the generator of $\mathrm{Gal}(k/\mathbb{Q})$, then there is an isogeny μ of E onto E^ε rational over k such that $\mu^\varepsilon \circ \mu = -c \cdot \mathrm{id}_E$ with a positive integer c. E and E^ε will, respectively, be identified with the subvarieties B and B^ε of A. Let f be an isomorphism of $E \times E^\varepsilon$ onto $E^\varepsilon \times E$ defined by $f(x, y) = (y, x)$. With an elliptic curve E satisfying the above condition, we can find an abelian variety A rational over $\mathbb{Q}$ and an isomorphism g of $E \times E^\varepsilon$ onto A rational over k such that $g = g^\varepsilon \circ f$. Let $K = \mathbb{Q}(\sqrt{-c})$. Then we can define an injective homomorphism of K into $\mathrm{End}(A) \otimes \mathbb{Q}$ and an automorphism η of A by

$$[g^{-1} \circ \theta(\sqrt{-c}) \circ g](x, y) = (\mu^\varepsilon y, \mu),$$

$$[g^{-1} \circ \eta \circ g](x, y) = (x, -y) \quad (x \in E, y \in E^{\varepsilon})$$

One can verify that A, θ, η satisfy axiomatic conditions 1–5. Furthermore, if c is an odd prime, then $F = \mathbb{Q}, \tau = c\mathbb{Z}$, and we identify $\mathcal{Y}$ with $\ker(\mu)$.

A Select Proofs

A.1 Associativity of the Group Law (§ 1.1)

The following proof is due to Silverman and Tate; see pages 19–20 from [1]. We will verify the associativity of + in the case of three distinct points $P, Q, R \in E(\mathbb{Q})$, excluding the cases in which any of P, Q, and R are inverses of each other. Of course, one must compute the exceptional cases, a task which we leave to the reader. For proof, we will need a bit of extra machinery in the form of two theorems which we will not prove.

Theorem A.1 (Bézout)**.** *Let C_1 and C_2 be two non-singular algebraic plane curves of dimension n and m respectively. Then, counting multiplicities, C_1 and C_2 intersect in nm points.*

Theorem A.2. *Let C_1, C_2, C_3 be three non-singular cubic curves. Let $P_1, P_2, \ldots, P_9$ be the nine intersection points of C_1 and C_2 given by Theorem A.1. Then if C_3 goes through eight of $P_1, P_2, \ldots, P_9$, then C_3 goes through the ninth intersection point.*

We will not prove Theorem A.1 or Theorem A.2, but we sketch an informal proof of Theorem A.2 as follows. Consider a general cubic C_3 in the form of equation (1). There are nine coefficients, each of which gives C_3 a "degree of freedom", so to speak. By requiring that C_3 goes through eight of the points of intersection of C_1 and C_2, by substituting in for each of the x, y coordinates in the equation for C_3, we impose a linear condition on the nine coefficients of C_3. With each linear condition imposed, we lose one degree of freedom. In other words, after having imposed eight linear conditions on the coefficients of C_3, we have but one degree of freedom before C is completely determined. Formally, this means that C_3 belongs to the space of cubic curves given by linear combinations of C_1 and C_2. If we let $F(x, y), G(x, y)$ and $H(x, y)$ be the equations giving the cubic curves C_1, C_2 and C_3 respectively, this means that $H(x, y) = \lambda_1 F(x, y) + \lambda_2 G(x, y)$ for some λ_1, λ_2. But as $F(x, y)$ and $G(x, y)$ vanish at the ninth point, this means $H(x, y)$ does too. So C_3 goes through the ninth point of intersection.

With this in mind, we may now proceed with proving + is associative - it will likely help to refer to figure 10. We wish to show that $(P + Q) + R = P + (Q + R)$. However, since $(P+Q)+R$ is the reflection of $(P+Q)\otimes R$ about the x-axis, and $P+(Q+R)$ is the reflection of $P \otimes (Q + R)$ about the x-axis, it will suffice to show that $(P + Q) \otimes R = P \otimes (Q + R)$. Since $(P+Q)\otimes R$ is the third point of intersection of the line L_1 through $P+Q$ and R with E and $P \otimes (Q + R)$ is the third point of intersection of the line L_2 through P and $Q + R$ with E, we can see that this is equivalent to showing that L_1 and L_2 intersect at a point on E.

Consider the nine points $O, P, Q, R, P\otimes Q, P+Q, Q\otimes R, Q+R$, and the point of intersection between L_1 and L_2. Let L_3 be the line through P and Q, L_4 be the line through $Q \otimes R$ and $Q+R$. Let L_5 be the line through R and Q, and L_6 be the line through $P\otimes Q$ and $P+Q$. We can define a degenerate cubic by looking at union of solutions of three lines; hence, define $C_1 = \{A | A \in L_1 \cup L_3 \cup L_4\}$ and $C_2 = \{B | B \in L_2 \cup L_5 \cup L_6\}$. From our definitions, we see that C_1 and C_2 intersect at the nine points $O, P, Q, R, P \otimes Q, P + Q, Q \otimes R, Q + R$, and the point of intersection between L_1 and L_2. But we have that $O, P, Q, R, P \otimes Q, P + Q, Q \otimes R, Q + R$

lie on E, so by Theorem A.2, we have that the intersection of L_1 and L_2 lies on E. So $+$ is associative.

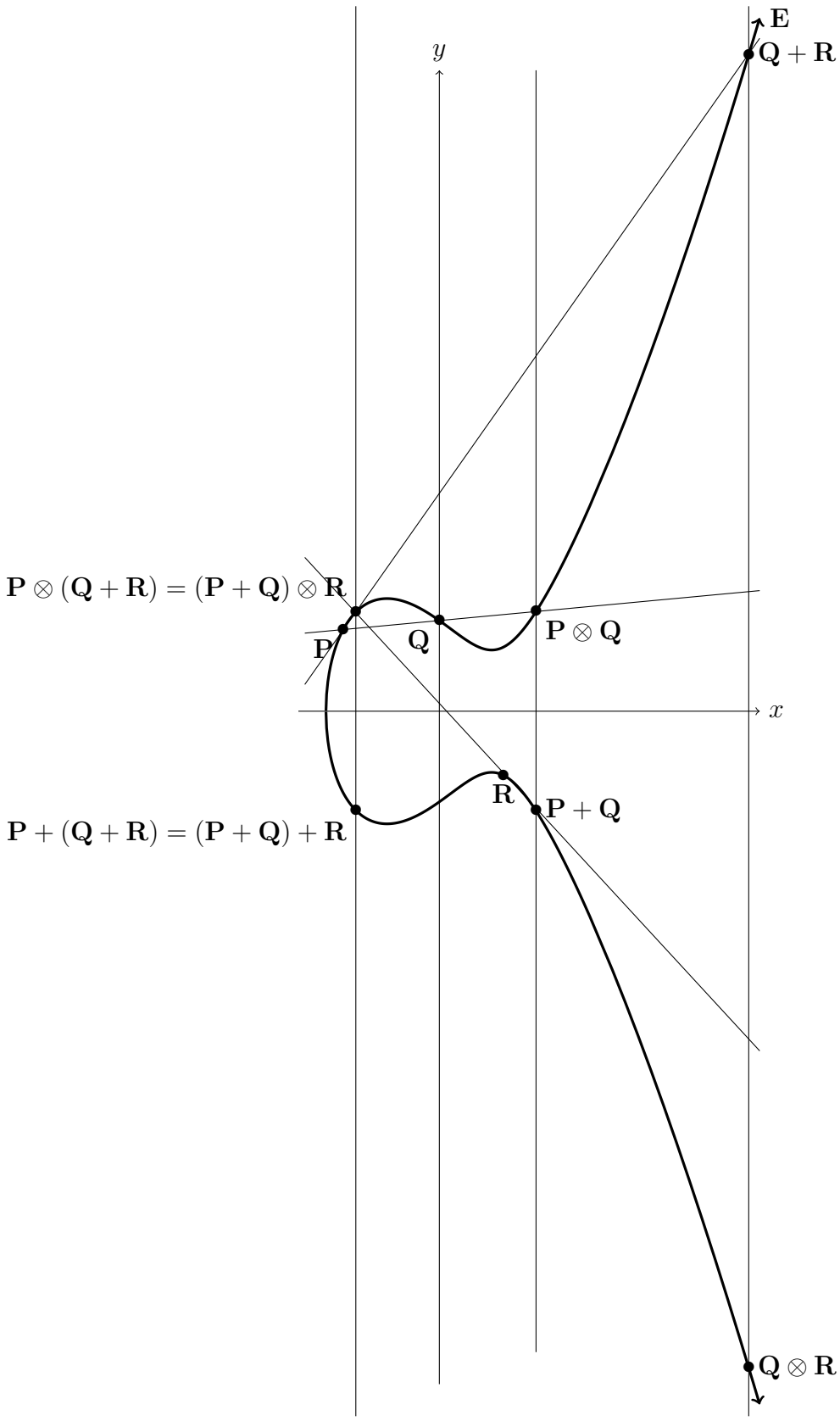


Figure 10: Associativity of + on $E(\mathbb{Q})$.

References

[1] Silverman, Joseph H., and John Torrence Tate. Rational Points on Elliptic Curves. New York: Springer-Verlag, 1992.

[2] Lang, Serge. Elliptic Functions. New York: Springer-Verlag, 1987.

[3] Silverman, Joseph H. The Arithmetic of Elliptic Curves. New York: Springer-Verlag, 1986.

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

[5] Shimura, Goro. *Class Fields Over Real Quadratic Fields and Hecke Operators.* Annals of Mathematics **95** (1972): 130–90.

[6] Shimura, Goro. Introduction to the Arithmetic Theory of Automorphic Functions. Tokyo: Iwanami Shoten, 1971.

[7] Shimura, G, "Class Fields Over Real Quadratic Fields and Hecke Operators", Seminar on Modern Methods in Number Theory, Institute of Statistical Mathematics, Tokyo, 1971.

[8] Dummit, David Steven., and Richard M. Foote. Abstract Algebra. Hoboken, NJ: Wiley, 2004.