Chapter III

The Geometry of Elliptic Curves

Elliptic curves, our principal object of study in this book, are curves of genus one having a specified base point. Our ultimate goal, as the title of the book indicates, is to study the arithmetic properties of these curves. In other words, we will be interested in analyzing their points defined over arithmetically interesting fields, such as finite fields, local (p-adic) fields, and global (number) fields. However, before doing so we are well advised to study the properties of these curves in the simpler situation of an algebraically closed field, i.e., to study their geometry. This reflects the general principle in Diophantine geometry that in attempting to study any significant problem, it is essential to have a thorough understanding of the geometry before one can hope to make progress on the number theory. It is the purpose of this chapter to make an intensive study of the geometry of elliptic curves over arbitrary algebraically closed fields. (The particular case of elliptic curves over the complex numbers is studied in more detail in Chapter VI.)

We start in the first two sections by looking at elliptic curves given by explicit polynomial equations called Weierstrass equations. Using these explicit equations, we show, among other things, that the set of points of an elliptic curve forms an abelian group, and that the group law is given by rational functions. Then, in Section 3, we use the Riemann–Roch theorem to study arbitrary elliptic curves and to show that every elliptic curve has a Weierstrass equation, so the results from the first two sections in fact apply generally. The remainder of the chapter studies, in various guises, the algebraic maps between elliptic curves. In particular, since the points of an elliptic curve form a group, for each integer m there is a multiplication-by-m map from the curve to itself. It would be difficult to overestimate the importance of these multiplication maps in any attempt to study the arithmetic of elliptic curves, which will explain why we devote so much space to them in this chapter.

J.H. Silverman, *The Arithmetic of Elliptic Curves, Second Edition*, Graduate Texts in Mathematics 106, DOI 10.1007/978-0-387-09494-6_III,

III.1 Weierstrass Equations

Our primary objects of study are *elliptic curves*, which are curves of genus one having a specified base point. As we will see in (III §3), every such curve can be written as the locus in $\mathbb{P}^2$ of a cubic equation with only one point, the base point, on the line at ∞. Then, after X and Y are scaled appropriately, an elliptic curve has an equation of the form

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

Here $O = [0, 1, 0]$ is the base point and $a_1, \dots, a_6 \in \bar{K}$. (It will become clear later why the coefficients are labeled in this way.) In this section and the next, we study the curves given by such *Weierstrass equations*, using explicit formulas as much as possible to replace the need for general theory.

To ease notation, we generally write the Weierstrass equation for our elliptic curve using non-homogeneous coordinates $x = X/Z$ and $y = Y/Z$,

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

always remembering that there is an extra point $O = [0, 1, 0]$ out at infinity. As usual, if $a_1, \dots, a_6 \in K$, then E is said to be *defined over* K.

If $\operatorname{char}(\bar{K}) \neq 2$, then we can simplify the equation by completing the square. Thus the substitution

$$y \longmapsto \frac{1}{2}(y - a_1x - a_3)$$

gives an equation of the form

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6,$$

where

$$b_2 = a_1^2 + 4a_2, \qquad b_4 = 2a_4 + a_1a_3, \qquad b_6 = a_3^2 + 4a_6.$$

We also define quantities

$$\begin{aligned}
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,\\
c_4 &= b_2^2 - 24b_4,\\
c_6 &= -b_2^3 + 36b_2b_4 - 216b_6,\\
\Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,\\
j &= c_4^3/\Delta,\\
\omega &= \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y}.
\end{aligned}$$

One easily verifies that they satisfy the relations

$$4b_8 = b_2b_6 - b_4^2 \qquad \text{and} \qquad 1728\Delta = c_4^3 - c_6^2.$$

If further $\operatorname{char}(\bar{K}) \neq 2, 3$, then the substitution

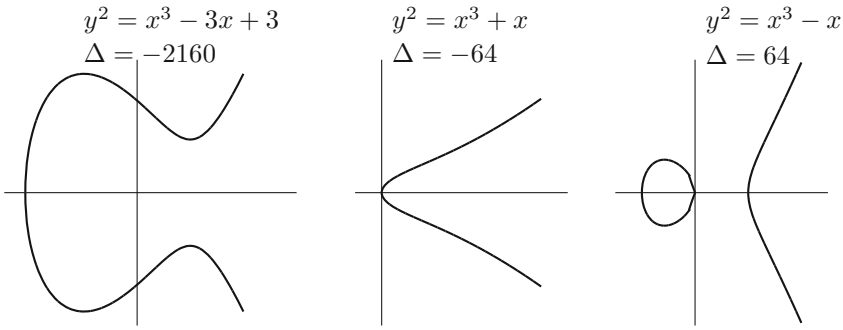
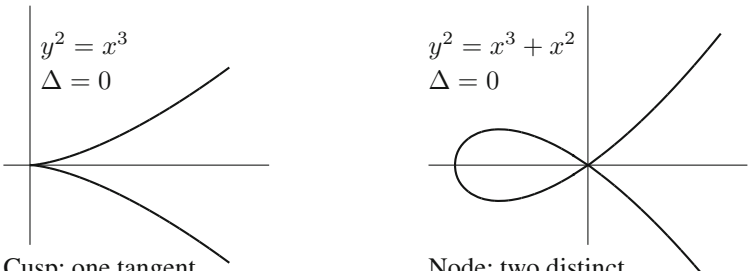


Figure 3.1: Three elliptic curves



Cusp: one tangent direction

Node: two distinct tangent directions

Figure 3.2: Two singular cubic curves.

$$(x, y) \longmapsto \left(\frac{x - 3b_2}{36}, \frac{y}{108} \right)$$

eliminates the x^2 term, yielding the simpler equation

$$E : y^2 = x^3 - 27c_4x - 54c_6.$$

Definition. The quantity Δ is the *discriminant* of the Weierstrass equation, the quantity j is the *j-invariant* of the elliptic curve, and ω is the *invariant differential* associated to the Weierstrass equation.

Example 1.1. It is easy to graph the real locus of a Weierstrass equation. Some representative examples are shown in Figure 3.1. If $\Delta = 0$, then we will see later (III.1.4) that the curve is singular. Two sorts of behavior can occur, as illustrated in Figure 3.2.

With these singular examples in mind, we consider the general situation. Let $P = (x_0, y_0)$ be a point satisfying a Weierstrass equation

$$f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0,$$

and assume that P is a singular point on the curve $f(x,y)=0$.Then from (I.1.5) we have

$$\frac{\partial f}{\partial x}(P)=\frac{\partial f}{\partial y}(P)=0.$$

It follows that there are $\alpha,\beta\in\bar{K}$ such that the Taylor series expansion of $f(x,y)$ at P has the form

$$\begin{aligned}f(x,y)-f(x_0,y_0)&\\ =\big((y-y_0)-\alpha(x-x_0)\big)\big((y-y_0)-\beta(x-x_0)\big)-(x-x_0)^3.&\end{aligned}$$

Definition. With notation as above, the singular point P is a *node* if $\alpha\neq\beta$. In this case, the lines

$$y-y_0=\alpha(x-x_0)\qquad\text{and}\qquad y-y_0=\beta(x-x_0)$$

are the *tangent lines* at P. Conversely, if $\alpha=\beta$, then we say that P is a *cusp*, in which case the *tangent line* at P is given by

$$y-y_0=\alpha(x-x_0).$$

To what extent is the Weierstrass equation for an elliptic curve unique? Assuming that the line at infinity, i.e., the line $Z=0$ in $\mathbb{P}^2$, is required to intersect E only at the one point $[0,1,0]$, we will see (III.3.1b) that the only change of variables fixing $[0,1,0]$ and preserving the Weierstrass form of the equation is

$$x=u^2x'+r\qquad\text{and}\qquad y=u^3y'+u^2sx'+t,$$

where $u,r,s,t\in\bar{K}$ and $u\neq0$. It is now a simple (but tedious) matter to make this substitution and compute the a_i' coefficients and associated quantities for the new equation. The results are compiled in Table 3.1.

It is now clear why the j-invariant has been so named; it is an invariant of the isomorphism class of the curve, and does not depend on the particular equation chosen. For algebraically closed fields, the converse is true, a fact that we establish later in this section (III.1.4b).

Remark 1.3. As we have seen, if the characteristic of K is different from 2 and 3, then any elliptic curve over K has a Weierstrass equation of a particularly simple kind. Thus any proof that involves extensive algebraic manipulation with Weierstrass equation, for example that of (III.1.4) later in this section, tends to be much shorter if K is so restricted. On the other hand, even if one is primarily interested in characteristic 0, e.g., $K=\mathbb{Q}$, an important tool is the process of reducing the coefficients of an equation modulo p for various primes p, including $p=2$ and $p=3$. So even for $K=\mathbb{Q}$, it is important to understand elliptic curves in all characteristics. Consequently, we adopt the following policy. All theorems will be stated for a general Weierstrass equation, but if it makes the proof substantially shorter, we will make the assumption that the characteristic of K is not 2 or 3 and give the proof in that case. Then, in the interest of completeness, we return to these theorems in Appendix A and give the proofs for general Weierstrass equations and arbitrary characteristic.

$ua_1' = a_1 + 2s$	
$u^2a_2' = a_2 - sa_1 + 3r - s^2$	
$u^3a_3' = a_3 + ra_1 + 2t$	
$u^4a_4' = a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st$	
$u^6a_6' = a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1$	
$u^2b_2' = b_2 + 12r$	
$u^4b_4' = b_4 + rb_2 + 6r^2$	
$u^6b_6' = b_6 + 2rb_4 + r^2b_2 + 4r^3$	
$u^8b_8' = b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4$	
$u^4c_4' = c_4$	
$u^6c_6' = c_6$	
$u^{12}\Delta' = \Delta$	
$j' = j$	
$u^{-1}\omega' = \omega$	

Table 3.1: Change-of-variable formulas for Weierstrass equations.

Assuming now that the characteristic of K is not 2 or 3, our elliptic curve(s) have Weierstrass equation(s) of the form

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

Associated to this equation are the quantities

$$\Delta = -16(4A^3 + 27B^2) \qquad \text{and} \qquad j = -1728\frac{(4A)^3}{\Delta}.$$

The only change of variables preserving this form of the equation is

$$x = u^2x' \qquad \text{and} \qquad y = u^3y' \qquad \text{for some } u \in \bar{K}^*;$$

and then

$$u^4A' = A, \qquad u^6B' = B, \qquad u^{12}\Delta' = \Delta.$$

Proposition 1.4. (a) *The curve given by a Weierstrass equation satisfies*:

(i) *It is nonsingular if and only if* $\Delta \neq 0$.
(ii) *It has a node if and only if* $\Delta = 0$ *and* $c_4 \neq 0$.
(iii) *It has a cusp if and only if* $\Delta = c_4 = 0$.

In cases (ii) *and* (iii)*, there is only the one singular point.*

(b) *Two elliptic curves are isomorphic over* $\bar{K}$ *if and only if they both have the same* j*-invariant.*

(c) *Let* $j_0 \in \bar{K}$*. There exists an elliptic curve defined over* $K(j_0)$ *whose* j*-invariant is equal to* j_0.

PROOF. Let E be given by the Weierstrass equation

$$E : f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0.$$

We start by showing that the point at infinity is never singular. Thus we look at the curve in $\mathbb{P}^2$ with homogeneous equation

$$\begin{aligned} F(X,Y,Z) &= Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 \\ &= 0 \end{aligned}$$

and at the point $O = [0,1,0]$. Since

$$\frac{\partial F}{\partial Z}(O) = 1 \neq 0,$$

we see that O is a nonsingular point of E.

Next suppose that E is singular, say at $P_0 = (x_0, y_0)$. The substitution

$$x = x' + x_0 \qquad y = y' + y_0$$

leaves Δ and c_4 invariant Table 3.1, so without loss of generality we may assume that E is singular at $(0,0)$. Then

$$a_6 = -f(0,0) = 0, \qquad a_4 = -\frac{\partial f}{\partial x}(0,0) = 0, \qquad a_3 = \frac{\partial f}{\partial y}(0,0) = 0,$$

so the equation for E takes the form

$$E : f(x,y) = y^2 + a_1xy - a_2x^2 - x^3 = 0.$$

This equation has associated quantities

$$c_4 = (a_1^2 + 4a_2)^2 \qquad \text{and} \qquad \Delta = 0.$$

By definition, E has a node (respectively cusp) at $(0,0)$ if the quadratic form $y^2 + a_1xy - a_2x^2$ has distinct (respectively equal) factors, which occurs if and only if the discriminant of this quadratic form satisfies

$$a_1^2 + 4a_2 \neq 0 \qquad (\text{respectively } a_1^2 + 4a_2 = 0).$$

This proves the "only if" part of (ii) and (iii).

To complete the proof of (i)–(iii), it remains to show that if E is nonsingular, then $\Delta \neq 0$. To simplify the computation, we assume that $\operatorname{char}(K) \neq 2$ and consider a Weierstrass equation of the form

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6.$$

(See (III.1.3) and (A.1.2a).) The curve E is singular if and only if there is a point $(x_0, y_0) \in E$ satisfying

$$2y_0 = 12x_0^2 + 2b_2x_0 + 2b_4 = 0.$$

In other words, the singular points are exactly the points of the form $(x_0, 0)$ such that x_0 is a double root of the cubic polynomial $4x^3 + b_2x^2 + 2b_4x + b_6$. This polynomial has a double root if and only if its discriminant, which equals 16Δ, vanishes. This completes the proof of (i)–(iii). Further, since a cubic polynomial cannot have two double roots, E has at most one singular point.

(b) If two elliptic curves are isomorphic, then the transformation formulas Table 3.1 show that they have the same j-invariant. For the converse, we will assume that $\operatorname{char}(K) \geq 5$ (see (III.1.3) and (A.1.2b)). Let E and E' be elliptic curves with the same j-invariant, say with Weierstrass equations

$$E : y^2 = x^3 + Ax + B,$$
$$E' : y'^2 = x'^3 + A'x' + B'.$$

Then the assumption that $j(E) = j(E')$ means that

$$\frac{(4A)^3}{4A^3 + 27B^2} = \frac{(4A')^3}{4A'^3 + 27B'^2},$$

which yields

$$A^3B'^2 = A'^3B^2.$$

We look for an isomorphism of the form $(x, y) = (u^2x', u^3y')$ and consider three cases:

Case 1. $A = 0$ ($j = 0$). Then $B \neq 0$, since $\Delta \neq 0$, so $A' = 0$, and we obtain an isomorphism using $u = (B/B')^{1/6}$.

Case 2. $B = 0$ ($j = 1728$). Then $A \neq 0$, so $B' = 0$, and we take $u = (A/A')^{1/4}$.

Case 3. $AB \neq 0$ ($j \neq 0, 1728$). Then $A'B' \neq 0$, since if one of them were 0, then both of them would be 0, contradicting $\Delta' \neq 0$. Taking $u = (A/A')^{1/4} = (B/B')^{1/6}$ gives the desired isomorphism.

(c) Assume that $j_0 \neq 0, 1728$ and consider the curve

$$E : y^2 + xy = x^3 - \frac{36}{j_0 - 1728}x - \frac{1}{j_0 - 1728}.$$

A simple calculations yields

$$\Delta = \frac{j_0^3}{(j_0 - 1728)^3} \qquad \text{and} \qquad j = j_0.$$

This gives the desired elliptic curve (in any characteristic) provided that $j_0 \neq 0, 1728$. To complete the list, we use the two curves

$$E : y^2 + y = x^3, \qquad \Delta = -27, \qquad j = 0,$$
$$E : y^2 = x^3 + x, \qquad \Delta = -64, \qquad j = 1728.$$

(Notice that in characteristic 2 or 3 we have $1728 = 0$, so even in these cases one of the two curves will be nonsingular and fill in the missing value of j.) □

Proposition 1.5. *Let E be an elliptic curve. Then the invariant differential ω associated to a Weierstrass equation for E is holomorphic and nonvanishing, i.e.,* $\operatorname{div}(\omega) = 0$.

PROOF. Let $P = (x_0, y_0) \in E$ and

$$E : F(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0,$$

so

$$\omega = \frac{d(x-x_0)}{F_y(x,y)} = -\frac{d(y-y_0)}{F_x(x,y)}.$$

Thus P cannot be a pole of ω, since otherwise $F_y(P) = F_x(P) = 0$, which would say that P is a singular point of E. The map

$$E \longrightarrow \mathbb{P}^1, \qquad [x,y,1] \longmapsto [x,1],$$

is of degree 2, so $\operatorname{ord}_P(x - x_0) \le 2$, and we have equality $\operatorname{ord}_P(x - x_0) = 2$ if and only if the quadratic polynomial $F(x_0, y)$ has a double root. In other words, either $\operatorname{ord}_P(x - x_0) = 1$, or else $\operatorname{ord}_P(x - x_0) = 2$ and $F_y(x_0, y_0) = 0$. Thus in both cases, we can use (II.4.3) to compute

$$\operatorname{ord}_P(\omega) = \operatorname{ord}_P(x - x_0) - \operatorname{ord}_P(F_y) - 1 = 0.$$

This shows that ω has no poles or zeros of the form (x_0, y_0), so it remains to check what happens at O.

Let t be a uniformizer at O. Since $\operatorname{ord}_O(x) = -2$ and $\operatorname{ord}_O(y) = -3$, we see that $x = t^{-2}f$ and $y = t^{-3}g$ for functions f and g satisfying $f(O) \ne 0, \infty$ and $g(O) \ne 0, \infty$. Now

$$\omega = \frac{dx}{F_y(x,y)} = \frac{-2t^{-3}f + t^{-2}f'}{2t^{-3}g + a_1t^{-2}f + a_3}\,dt = \frac{-2f + tf'}{2g + a_1tf + a_3t^3}\,dt.$$

Here we are writing $f' = df/dt$; cf. (II.4.3). In particular, (II.4.3b) tells us that f' is regular at O. Hence assuming that $\operatorname{char}(K) \ne 2$, the function

$$\frac{-2f + tf'}{2g + a_1tf + a_3t^3}$$

is regular and nonvanishing at O, and thus

$$\operatorname{ord}_O(\omega) = 0.$$

Finally, if $\operatorname{char}(K) = 2$, then the same result follows from a similar calculation using $\omega = -dy/F_x(x,y)$. We leave the details to the reader. □

Next we look at what happens when a Weierstrass equation is singular.

Proposition 1.6. *If a curve E given by a Weierstrass equation is singular, then there exists a rational map $\phi : E \to \mathbb{P}^1$ of degree one, i.e., the curve E is birational to $\mathbb{P}^1$.* (*Note that since E is singular, we cannot use* (II.2.4.1) *to conclude that $E \cong \mathbb{P}^1$.*)

PROOF. Making a linear change of variables, we may assume that the singular point is $(x, y) = (0, 0)$. Checking partial derivatives, we see that the Weierstrass equation has the form

$$E : y^2 + a_1xy = x^3 + a_2x^2.$$

Then the rational map

$$E \longrightarrow \mathbb{P}^1, \qquad (x, y) \to [x, y],$$

has degree one, since it has an inverse given by

$$\mathbb{P}^1 \longrightarrow E, \qquad [1, t] \longmapsto (t^2 + a_1t - a_2, t^3 + a_1t^2 - a_2t).$$

(To derive this formula, let $t = y/x$ and note that dividing the Weierstrass equation of E by x^2 yields $t^2 + a_1t = x + a_2$. This shows that both x and $y = xt$ are in $\bar{K}(t)$.) □

Legendre Form

There is another form of Weierstrass equation that is sometimes convenient.

Definition. A Weierstrass equation is in *Legendre form* if it can be written as

$$y^2 = x(x - 1)(x - \lambda).$$

Proposition 1.7. *Assume that* $\mathrm{char}(K) \neq 2$.
(a) *Every elliptic curve is isomorphic (over* $\bar{K}$*) to an elliptic curve in Legendre form*

$$E_\lambda : y^2 = x(x - 1)(x - \lambda)$$

for some $\lambda \in \bar{K}$ *with* $\lambda \neq 0, 1$.
(b) *The* j*-invariant of* E_λ *is*

$$j(E_\lambda) = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}.$$

(c) *The association*

$$\bar{K} \smallsetminus \{0, 1\} \longrightarrow \bar{K}, \qquad \lambda \longmapsto j(E_\lambda),$$

is surjective and exactly six-to-one except above $j = 0$ *and* $j = 1728$*, where it is two-to-one and three-to-one, respectively (unless* $\mathrm{char}(K) = 3$*, in which case it is one-to-one above* $j = 0 = 1728$*).*

PROOF. (a) Since $\mathrm{char}(K) \neq 2$, we know that E has a Weierstrass equation of the form

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6.$$

Replacing (x, y) by $(x, 2y)$ and factoring the cubic yields an equation of the form

$$y^2 = (x - e_1)(x - e_2)(x - e_3)$$

for some $e_1, e_2, e_3 \in \bar{K}$. Further, since

$$\Delta = 16(e_1 - e_2)^2(e_1 - e_3)^2(e_2 - e_3)^2 \neq 0,$$

we see that the e_i's are distinct. Now the substitution

$$x = (e_2 - e_1)x' + e_1, \qquad y = (e_2 - e_1)^{3/2}y'$$

gives an equation in Legendre form with

$$\lambda = \frac{e_3 - e_1}{e_2 - e_1} \in \bar{K}, \qquad \lambda \neq 0, 1.$$

(b) Calculation.
(c) One can work directly from the formula for $j(E_\lambda)$ in (b), an approach that we leave to the reader. Instead, we use the fact that the j-invariant classifies an elliptic curve up to isomorphism (III.1.4b). Thus suppose that $j(E_\lambda) = j(E_\mu)$. Then $E_\lambda \cong E_\mu$, so their Weierstrass equations (in Legendre form) are related by a change of variables

$$x = u^2x' + r, \qquad y = u^3y'.$$

Equating

$$x(x-1)(x-\mu) = \left(x + \frac{r}{u^2}\right)\left(x + \frac{r-1}{u^2}\right)\left(x + \frac{r-\lambda}{u^2}\right),$$

there are six ways of assigning the linear terms to one another, and one easily checks that these lead to six possible values for μ in terms of λ,

$$\mu \in \left\{\lambda, \frac{1}{\lambda}, 1-\lambda, \frac{1}{1-\lambda}, \frac{\lambda}{\lambda-1}, \frac{\lambda-1}{\lambda}\right\}.$$

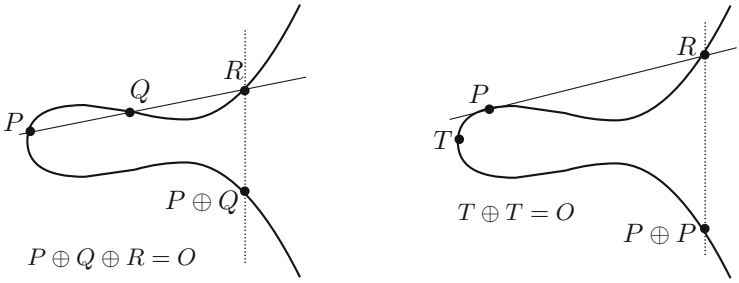
Hence $\lambda \mapsto j(E_\lambda)$ is exactly six-to-one unless two or more of these values for μ coincide. Equating them by pairs shows that this occurs if and only if

$$\lambda \in \left\{-1, 2, \frac{1}{2}\right\} \Longrightarrow \text{association is three-to-one}$$

or

$$\lambda^2 - \lambda + 1 = 0 \Longrightarrow \text{association is two-to-one.}$$

These λ values correspond, respectively, to $j = 1728$ and $j = 0$. Finally, if K has characteristic 3, then these λ values coincide and the equation $j(\lambda) = 0 = 1728$ has the unique solution $\lambda = -1$. □



Addition of distinct points Adding a point to itself

Figure 3.3: The composition law.

III.2 The Group Law

Let E be an elliptic curve given by a Weierstrass equation. Thus $E \subset \mathbb{P}^2$ consists of the points $P = (x, y)$ satisfying the Weierstrass equation, together with the point $O = [0, 1, 0]$ at infinity. Let $L \subset \mathbb{P}^2$ be a line. Then, since the equation has degree three, the line L intersects E at exactly three points, say P, Q, R. Of course, if L is tangent to E, then P, Q, R need not be distinct. The fact that $L \cap E$, taken with multiplicities, consists of exactly three points is a special case of Bézout's theorem [111, I.7.8]. However, since we give explicit formulas later in this section, there is no need to use a general theorem.

We define a composition law $\oplus$ on E by the following rule:

Composition Law 2.1. *Let $P, Q \in E$, let L be the line through P and Q (if $P = Q$, let L be the tangent line to E at P), and let R be the third point of intersection of L with E. Let L' be the line through R and O. Then L' intersects E at R, O, and a third point. We denote that third point by $P \oplus Q$.*

Various instances of the composition law (III.2.1) are illustrated in Figure 3.3. We now justify the use of the symbol $\oplus$.

Proposition 2.2. *The composition law* (III.2.1) *has the following properties*:
(a) *If a line L intersects E at the* (*not necessarily distinct*) *points P, Q, R, then*

$$(P \oplus Q) \oplus R = O.$$

(b) *$P \oplus O = P$ for all $P \in E$.*
(c) *$P \oplus Q = Q \oplus P$ for all $P, Q \in E$.*
(d) *Let $P \in E$. There is a point of E, denoted by $\ominus P$, satisfying*

$$P \oplus (\ominus P) = O.$$

(e) *Let $P, Q, R \in E$. Then*

$$(P \oplus Q) \oplus R = P \oplus (Q \oplus R).$$

In other words, the composition law (III.2.1) *makes E into an abelian group with identity element O. Further:*
(f) *Suppose that E is defined over K. Then*

$$E(K) = \big\{(x,y) \in K^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\big\} \cup \{O\}$$

is a subgroup of E.

PROOF. All of this is easy except for the associativity (e).
(a) This is obvious from (III.2.1), or look at Figure 3.3 and note that the tangent line to E at O intersects E with multiplicity 3 at O.
(b) Taking $Q = O$ in (III.2.1), we see that the lines L and L' coincide. The former intersects E at P, O, R and the latter at $R, O, P \oplus O$, so $P \oplus O = P$.
(c) This is also clear, since the construction of $P \oplus Q$ in (III.2.1) is symmetric in P and Q.
(d) Let the line through P and O also intersect E at R. Then using (a) and (b), we find that

$$O = (P \oplus O) \oplus R = P \oplus R.$$

(e) Using the explicit formulas given later in this section (III.2.3), one can laboriously verify the associative law case by case. We leave this task to the reader. A more enlightening proof using the Riemann–Roch theorem is given in the next section (III.3.4e). For a geometric proof, see [95].
(f) If P and Q have coordinates in K, then the equation of the line connecting them has coefficients in K. If, further, E is defined over K, then the third point of intersection has coordinates given by a rational combination of the coordinates of coefficients of the line and of E, so will be in K. (If this is not clear, see (III.2.3) in this section for explicit formulas.) □

Notation. From here on, we drop the special symbols $\oplus$ and $\ominus$ and simply write $+$ and $-$ for the group operation on an elliptic curve E. For $m \in \mathbb{Z}$ and $P \in E$, we let

$$[m]P = \overbrace{P + \cdots + P}^{m \text{ terms if } m > 0}, \qquad [m]P = \overbrace{-P - \cdots - P}^{|m| \text{ terms if } m < 0}, \qquad [0]P = O.$$

As promised, we now derive explicit formulas for the group operations on E. Let E be an elliptic curve given by a Weierstrass equation

$$F(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0,$$

and let $P_0 = (x_0, y_0) \in E$. Following the proof of (III.2.2d), in order to calculate $-P_0$, we take the line L through P_0 and O and find its third point of intersection with E. The line L is given by

$$L : x - x_0 = 0.$$

Substituting this into the equation for E, we see that the quadratic polynomial $F(x_0, y)$ has roots y_0 and y_0', where $-P = (x_0, y_0')$. Writing out

$$F(x_0, y) = c(y - y_0)(y - y_0')$$

and equating the coefficients of y^2 gives $c = 1$, and similarly equating the coefficients of y gives $y_0' = -y_0 - a_1x_0 - a_3$. This yields

$$-P_0 = -(x_0, y_0) = (x_0, -y_0 - a_1x_0 - a_3).$$

Next we derive a formula for the addition law. Let

$$P_1 = (x_1, y_1) \quad \text{and} \quad P_2 = (x_2, y_2)$$

be points of E. If $x_1 = x_2$ and $y_1 + y_2 + a_1x_2 + a_3 = 0$, then we have already shown that $P_1 + P_2 = O$. Otherwise the line L through P_1 and P_2 (or the tangent line to E if $P_1 = P_2$) has an equation of the form

$$L : y = \lambda x + \nu;$$

formulas for λ and ν are given below. Substituting the equation of L into the equation of E, we see that $F(x, \lambda x + \nu)$ has roots x_1, x_2, x_3, where $P_3 = (x_3, y_3)$ is the third point of $L \cap E$. From (III.2.2a) we have

$$P_1 + P_2 + P_3 = O.$$

We write out

$$F(x, \lambda x + \nu) = c(x - x_1)(x - x_2)(x - x_3)$$

and equate coefficients. The coefficient of x^3 gives $c = -1$, and then the coefficient of x^2 yields

$$x_1 + x_2 + x_3 = \lambda^2 + a_1\lambda - a_2.$$

This gives a formula for x_3, and substituting into the equation of L gives the value of $y_3 = \lambda x_3 + \nu$. Finally, to find $P_1 + P_2 = -P_3$, we apply the negation formula to P_3. All of this is summarized in the following algorithm.

Group Law Algorithm 2.3. *Let E be an elliptic curve given by a Weierstrass equation*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

(a) *Let $P_0 = (x_0, y_0)$. Then*

$$-P_0 = (x_0, -y_0 - a_1x_0 - a_3).$$

Next let

$$P_1 + P_2 = P_3 \qquad \textit{with} \qquad P_i = (x_i, y_i) \in E \quad \textit{for } i = 1, 2, 3.$$

(b) *If $x_1 = x_2$ and $y_1 + y_2 + a_1x_2 + a_3 = 0$, then*

$$P_1 + P_2 = O.$$

Otherwise, define λ and ν by the following formulas:

	λ	ν
$x_1 \neq x_2$	$\dfrac{y_2 - y_1}{x_2 - x_1}$	$\dfrac{y_1x_2 - y_2x_1}{x_2 - x_1}$
$x_1 = x_2$	$\dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}$	$\dfrac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}$

Then $y = \lambda x + \nu$ is the line through P_1 and P_2, or tangent to E if $P_1 = P_2$.

(c) *With notation as in* (b), *$P_3 = P_1 + P_2$ has coordinates*

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2,$$
$$y_3 = -(\lambda + a_1)x_3 - \nu - a_3.$$

(d) *As special cases of* (c), *we have for $P_1 \neq \pm P_2$,*

$$x(P_1 + P_2) = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 + a_1\left(\frac{y_2 - y_1}{x_2 - x_1}\right) - a_2 - x_1 - x_2,$$

and the duplication formula *for $P = (x, y) \in E$,*

$$x\big([2]P\big) = \frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6},$$

where b_2, b_4, b_6, b_8 are the polynomials in the a_i's given in (III §1). (*See also Exercise 3.25.*)

Corollary 2.3.1. *With notation as in* (III.2.3), *a function $f \in \bar{K}(E) = \bar{K}(x, y)$ is said to be* even *if $f(P) = f(-P)$ for all $P \in E$. Then*

$$f \text{ is even} \qquad \text{if and only if} \qquad f \in \bar{K}(x).$$

PROOF. From (III.2.3), if $P = (x_0, y_0)$, then $-P = (x_0, -y_0 - a_1x_0 - a_3)$. It follows immediately that every element of $\bar{K}(x)$ is even. Suppose now that $f \in \bar{K}(x, y)$ is even. Using the Weierstrass equation for E, we can write f in the form

$$f(x, y) = g(x) + h(x)y \qquad \text{for some } g, h \in \bar{K}(x).$$

Then the assumed evenness of f implies that

$$f(x, y) = f(x, -y - a_1x - a_3),$$
$$g(x) + h(x)y = g(x) + h(x)(-y - a_1x - a_3),$$
$$(2y + a_1x + a_3)h(x) = 0.$$

This holds for all $(x, y) \in E$, so either h is identically 0, or else $2 = a_1 = a_3 = 0$. The latter implies that the discriminant satisfies $\Delta = 0$, contradicting our assumption that the Weierstrass equation is nonsingular (III.1.4a). Hence $h = 0$, and so $f(x, y) = g(x) \in \bar{K}(x)$. □

Example 2.4. Let $E/\mathbb{Q}$ be the elliptic curve

$$E : y^2 = x^3 + 17.$$

A brief inspection reveals some points with integer coordinates,

$$P_1 = (-2, 3), \quad P_2 = (-1, 4), \quad P_3 = (2, 5), \quad P_4 = (4, 9), \quad P_5 = (8, 23),$$

and a short computer search gives some others,

$$P_6 = (43, 282), \quad P_7 = (52, 375), \quad P_8 = (5234, 378661).$$

Using the addition formula, one easily verifies relations such as

$$P_5 = [-2]P_1, \qquad P_4 = P_1 - P_3, \qquad [3]P_1 - P_3 = P_7.$$

Of course, there also are lots of points with nonintegral rational coordinates, for example

$$[2]P_2 = \left(\frac{137}{64}, -\frac{2651}{512}\right), \qquad P_2 + P_3 = \left(-\frac{8}{9}, -\frac{109}{27}\right).$$

Now it is true, but not so easy to prove, that every rational point $P \in E(\mathbb{Q})$ can be written in the form

$$P = [m]P_1 + [n]P_3 \qquad \text{for some } m, n \in \mathbb{Z},$$

and with this identification, the group $E(\mathbb{Q})$ is isomorphic to $\mathbb{Z} \times \mathbb{Z}$. Further, there are only 16 integral points $P = (x, y) \in E$, i.e., points with $x, y \in \mathbb{Z}$, namely $\{\pm P_1, \ldots, \pm P_8\}$. (See [190].) These facts illustrate two fundamental theorems in the arithmetic of elliptic curves, namely that the group of rational points on an elliptic curve is finitely generated (the Mordell–Weil theorem, proven in Chapter VIII) and that the set of integral points on an elliptic curve is finite (Siegel's theorem, proven in Chapter IX).

Singular Weierstrass Equations

Suppose that a given Weierstrass equation has discriminant $\Delta = 0$, so (III.1.4a) tells us that it has a singular point. To what extent does our analysis of the composition law fail in this case? As we will see, everything is fine provided that we discard the singular point; and in fact, the resulting group has a particularly simple structure.

The reason that we will be interested in this situation is best illustrated by an example. Consider again the elliptic curve from (III.2.4),

$$E : y^2 = x^3 + 17.$$

This is an elliptic curve defined over $\mathbb{Q}$ with discriminant $\Delta = -2^4 3^3 17$. It is often useful to reduce the coefficients of E modulo p for various primes p and to consider E as a curve defined over the finite field $\mathbb{F}_p$. For almost all primes, namely

those for which $\Delta \not\equiv 0 \pmod{p}$, the "reduced" curve is nonsingular, and hence is an elliptic curve defined over $\mathbb{F}_p$. However, for primes p that divide Δ, so in this example for $p \in \{2, 3, 17\}$, the "reduced" curve has a singular point, so it is no longer an elliptic curve. Thus even when dealing with nonsingular elliptic curves, say defined over $\mathbb{Q}$, we find singular curves naturally appearing. We will return to this reduction process in more detail in Chapter VII.

Definition. Let E be a (possibly singular) curve given by a Weierstrass equation. The *nonsingular part of* E, denoted by E_{ns}, is the set of nonsingular points of E. Similarly, if E is defined over K, then $E_{\text{ns}}(K)$ is the set of nonsingular points of $E(K)$.

We recall from (III.1.4a) that if E is singular, then there are two possibilities for the singularity, namely a node or a cusp, determined by whether $c_4 \neq 0$ or $c_4 = 0$, respectively.

Proposition 2.5. *Let E be a curve given by a Weierstrass equation with $\Delta = 0$, so E has a singular point S. Then the composition law* (III.2.1) *makes E_{ns} into an abelian group.*

(a) *Suppose that E has a node, so $c_4 \neq 0$, and let*

$$y = \alpha_1 x + \beta_1 \quad \textit{and} \quad y = \alpha_2 x + \beta_2$$

be the distinct tangent lines to E at S. Then the map

$$E_{\text{ns}} \longrightarrow \bar{K}^*, \qquad (x, y) \longmapsto \frac{y - \alpha_1 x - \beta_1}{y - \alpha_2 x - \beta_2}$$

is an isomorphism of abelian groups.

(b) *Suppose that E has a cusp, so $c_4 = 0$, and let*

$$y = \alpha x + \beta$$

be the tangent line to E at S. Then the map

$$E_{\text{ns}} \longrightarrow \bar{K}^+, \qquad (x, y) \longmapsto \frac{x - x(S)}{y - \alpha x - \beta}$$

is an isomorphism of abelian groups.

Remark 2.6. For a group-theoretic description of $E_{\text{ns}}(K)$ when K is not algebraically closed, see Exercise 3.5.

PROOF. We first observe that E_{ns} is closed under the composition law (III.2.1), since if a line L intersects E_{ns} at two (not necessarily distinct) points, then L cannot contain the point S. This is true because S is a singular point of E, so S has multiplicity at least two in the intersection $E \cap L$; see Exercise 3.28. Thus if L also contains S, then $E \cap L$ would consist of four points (counted with multiplicity), contradicting Bézout's theorem [111, I.7.8].

We will verify that the maps in (a) and (b) are set bijections with the property that if a line L not hitting S intersects E_{ns} in three not necessarily distinct points, then the images of these three points in $\bar{K}^*$ (respectively $\bar{K}^+$) multiply to 1 (respectively sum to 0). Using this property, we will prove that the composition law (III.2.1) makes E_{ns} into an abelian group and that the maps in (a) and (b) are group isomorphisms.

Since the composition law (III.2.1) and the maps (a) and (b) are defined in terms of lines in $\mathbb{P}^2$, it suffices to prove the theorem after making a linear change of variables. We start by moving the singular point to $(0,0)$, yielding the Weierstrass equation

$$y^2 + a_1xy = x^3 + a_2x^2.$$

Let $s \in \bar{K}$ be a root of $s^2 + a_1s - a_2 = 0$. Replacing y by $y + sx$ eliminates the x^2 term, giving the following equation for E, which we now write using homogeneous coordinates:

$$E : Y^2Z + AXYZ - X^3 = 0.$$

Note that E has a node if $A \neq 0$ and a cusp if $A = 0$.

(a) The tangent lines to E at $S = [0,0,1]$ are $Y = 0$ and $Y + AX = 0$, so we are looking at the map

$$E_{\text{ns}} \longrightarrow \bar{K}^*, \qquad [X,Y,Z] \longmapsto 1 + \frac{AX}{Y}.$$

It is convenient to make one more variable change, so we let

$$X = A^2X' - A^2Y', \qquad Y = A^3Y', \qquad Z = Z'.$$

Dropping the primes, this gives the equation

$$E : XYZ - (X - Y)^3 = 0.$$

We now dehomogenize by setting $Y = 1$, so $x = X/Y$ and $z = Z/Y$, which yields the equation

$$E : xz - (x-1)^3 = 0$$

and the map

$$E_{\text{ns}} \longrightarrow \bar{K}^*, \qquad (x,z) \longmapsto x.$$

(Notice that in this new coordinate system, the singular point is now a point at infinity.) The inverse map is

$$\bar{K}^* \longrightarrow E_{\text{ns}}, \qquad t \longmapsto \left(t, \frac{(t-1)^3}{t}\right),$$

so we have a bijection of sets $\bar{K}^* \xleftrightarrow{\sim} E_{\text{ns}}$. It remains to show that if a line, not going through $[0,0,1]$, intersects E at the three points (x_1,z_1), (x_2,z_2), and (x_3,z_3), then $x_1x_2x_3 = 1$. (See Figure 3.4.) Any such line has the form $z = ax + b$, so the three x-coordinates x_1, x_2, and x_3 are the roots of the cubic polynomial

$$x(ax+b) - (x-1)^3 = -x^3 + (a+3)x^2 + (b-3)x + 1.$$

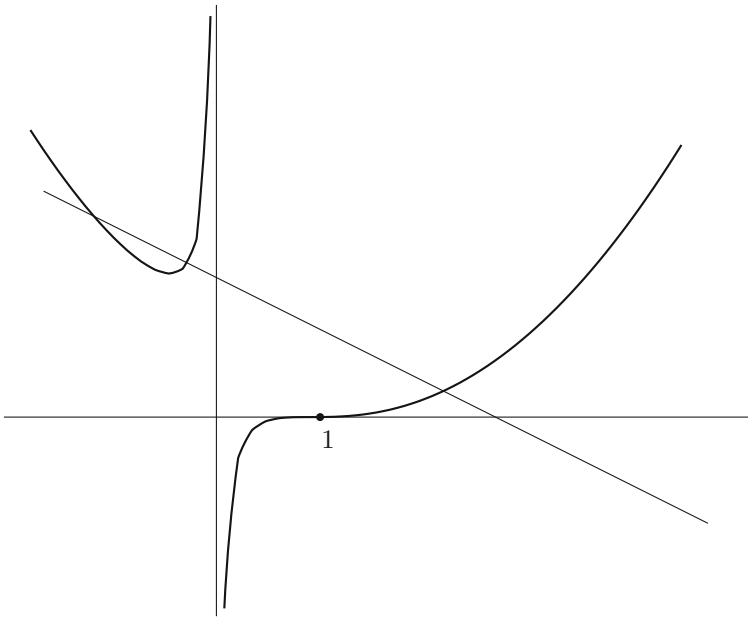


Figure 3.4: The curve $xz - (x-1)^3 = 0$.

Looking at the constant term, we see that $x_1x_2x_3 = 1$, as desired.
(b) In this case $A = 0$ and the tangent line to E at $S = [0, 0, 1]$ is $Y = 0$, so we are looking at the map

$$E_{\text{ns}} \longrightarrow \bar{K}^+, \qquad [X, Y, Z] \longmapsto X/Y.$$

Again dehomogenizing by setting $Y = 1$, we obtain

$$E : z - x^3 = 0,$$
$$E_{\text{ns}} \longrightarrow \bar{K}^+, \qquad (x, z) \longmapsto x.$$

The inverse map is $t \mapsto (t, t^3)$. Finally, if the line $z = ax + b$ intersects E at the three points (x_1, z_1), (x_2, z_2), and (x_3, z_3), then the absence of an x^2-term in

$$(ax + b) - x^3$$

implies that $x_1 + x_2 + x_3 = 0$. □

III.3 Elliptic Curves

Let E be a smooth curve of genus one. For example, the nonsingular Weierstrass equations studied in (III §1) and (III §2) define curves of this sort. As we have seen,

such Weierstrass curves can be given the structure of an abelian group. In order to make a set into a group, clearly an initial requirement is to choose a distinguished (identity) element. This leads to the following definition.

Definition. An *elliptic curve* is a pair (E, O), where E is a nonsingular curve of genus one and $O \in E$. (We generally denote the elliptic curve by E, the point O being understood.) The elliptic curve E is *defined over* K, written E/K, if E is defined over K as a curve and $O \in E(K)$.

In order to connect this definition with the material in (III §1) and (III §2), we begin by using the Riemann–Roch theorem to show that every elliptic curve can be written as a plane cubic, and conversely, every smooth Weierstrass plane cubic curve is an elliptic curve.

Proposition 3.1. *Let E be an elliptic curve defined over K.*
(a) *There exist functions $x, y \in K(E)$ such that the map*

$$\phi : E \longrightarrow \mathbb{P}^2, \qquad \phi = [x, y, 1],$$

gives an isomorphism of E/K onto a curve given by a Weierstrass equation

$$C : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

with coefficients $a_1, \ldots, a_6 \in K$ and satisfying $\phi(O) = [0, 1, 0]$. The functions x and y are called Weierstrass coordinates *for the elliptic curve E.*
(b) *Any two Weierstrass equations for E as in* (a) *are related by a linear change of variables of the form*

$$X = u^2X' + r, \qquad Y = u^3Y' + su^2X' + t,$$

with $u \in K^*$ and $r, s, t \in K$.
(c) *Conversely, every smooth cubic curve C given by a Weierstrass equation as in* (a) *is an elliptic curve defined over K with base point $O = [0, 1, 0]$.*

PROOF. (a) We look at the vector spaces $\mathcal{L}\big(n(O)\big)$ for $n = 1, 2, \ldots$. By the Riemann–Roch theorem, more specifically from (II.5.5c) with $g = 1$, we have

$$\ell\big(n(O)\big) = \dim \mathcal{L}\big(n(O)\big) = n \qquad \text{for all } n \geq 1.$$

Thus we can choose functions $x, y \in K(E)$ as in (II.5.8) so that $\{1, x\}$ is a basis for $\mathcal{L}\big(2(O)\big)$ and so that $\{1, x, y\}$ is a basis for $\mathcal{L}\big(3(O)\big)$. Note that x must have a pole of exact order 2 at O, and similarly y must have a pole of exact order 3 at O.

Now we observe that $\mathcal{L}\big(6(O)\big)$ has dimension 6, but it contains the seven functions

$$1, x, y, x^2, xy, y^2, x^3.$$

It follows that there is a linear relation

$$A_1 + A_2x + A_3y + A_4x^2 + A_5xy + A_6y^2 + A_7x^3 = 0,$$

where by (II.5.8) we may take $A_1, \ldots, A_7 \in K$. Note that $A_6 A_7 \neq 0$, since otherwise every term would have a pole at O of a different order, and so all of the A_j's would vanish. Replacing x and y by $-A_6 A_7 x$ and $A_6 A_7^2 y$, respectively, and dividing by $A_6^3 A_7^4$, we get a cubic equation in Weierstrass form. This gives a map

$$\phi : E \longrightarrow \mathbb{P}^2, \qquad \phi = [x, y, 1],$$

whose image lies in the locus C described by a Weierstrass equation. Note that $\phi : E \to C$ is a morphism from (II.2.1), and that it is surjective from (II.2.3). Further, we have $\phi(O) = [0, 1, 0]$, since y has a higher-order pole than x at the point O.

The next step is to show that the map $\phi : E \to C \subset \mathbb{P}^2$ has degree-one, or equivalently, to show that $K(E) = K(x, y)$. Consider the map $[x, 1] : E \to \mathbb{P}^1$. Since x has a double pole at O and no other poles, (II.2.6a) says that this map has degree 2. Thus $\big[K(E) : K(x)\big] = 2$. Similarly, the map $[y, 1] : E \to \mathbb{P}^1$ has degree 3, so $\big[K(E) : K(y)\big] = 3$. Therefore $\big[K(E) : K(x, y)\big]$ divides both 2 and 3, so it must equal 1.

Next we show that C is smooth. Suppose that C is singular. Then from (III.1.6), there is a rational map $\psi : C \to \mathbb{P}^1$ of degree one. It follows that the composition $\psi \circ \phi : E \to \mathbb{P}^1$ is a map of degree one between smooth curves, so from (II.2.4.1), it is an isomorphism. This contradicts the fact that E has genus one and $\mathbb{P}^1$ has genus zero (II.5.6). Therefore C is smooth, and now another application of (II.2.4.1) shows that the degree one map $\phi : E \to C$ is an isomorphism.

(b) Let $\{x, y\}$ and $\{x', y'\}$ be two sets of Weierstrass coordinate functions on E. Then x and x' have poles of order 2 at O, and y and y' have poles of order 3 at O. Hence $\{1, x\}$ and $\{1, x'\}$ are both bases for $\mathcal{L}\big(2(O)\big)$, and similarly $\{1, x, y\}$ and $\{1, x', y'\}$ are both bases for $\mathcal{L}\big(3(O)\big)$. Thus there are constants

$$u_1, u_2 \in K^* \quad \text{and} \quad r, s_2, t \in K$$

such that

$$x = u_1 x' + r \quad \text{and} \quad y = u_2 y' + s_2 x' + t.$$

Since both (x, y) and (x', y') satisfy Weierstrass equations in which the Y^2 and X^3 terms have coefficient 1, we have $u_1^3 = u_2^2$. Letting $u = u_2/u_1$ and $s = s_2/u^2$ puts the change of variables formula into the desired form.

(c) Let E be given by a nonsingular Weierstrass equation. We have seen (III.1.5) that the differential

$$\omega = \frac{dx}{2y + a_1 x + a_3} \in \Omega_E$$

has neither zeros nor poles, so $\operatorname{div}(\omega) = 0$. The Riemann–Roch theorem (II.5.5b) then tells us that

$$2\,\mathrm{genus}(E) - 2 = \deg \operatorname{div}(\omega) = 0,$$

so E has genus one, and taking $[0, 1, 0]$ as the base point makes E into an elliptic curve. (For an alternative proof of (c) using the Hurwitz genus formula, see Exercise 2.7.) □

Corollary 3.1.1. *Let E/K be an elliptic curve with Weierstrass coordinate functions x and y. Then*

$$K(E) = K(x,y) \qquad \textit{and} \qquad \bigl[K(E) : K(x)\bigr] = 2.$$

PROOF. These two facts were proven during the course of proving (III.3.1a). □

Remark 3.2. Note that (III.3.1b) does *not* imply that if two Weierstrass equations have coefficients in a given field K, then every change of variables mapping one to the other has coefficients in K. A simple example is the equation

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

It has coefficients in $\mathbb{Q}$, yet it is mapped to itself by the substitution

$$x = -x', \qquad y = \sqrt{-1}\,y'.$$

We next use the Riemann–Roch theorem to describe a group law on the points of an elliptic curve E. Of course, this will turn out to be the group law described by (III.2.1) when E is given by a Weierstrass equation. We start with a simple lemma that serves to distinguish $\mathbb{P}^1$ from curves of genus one; see Exercise 2.5 for a generalization.

Lemma 3.3. *Let C be a curve of genus one and let $P, Q \in C$. Then*

$$(P) \sim (Q) \qquad \textit{if and only if} \qquad P = Q.$$

PROOF. Suppose that $(P) \sim (Q)$ and choose $f \in \bar{K}(C)^*$ such that

$$\operatorname{div}(f) = (P) - (Q).$$

Then $f \in \mathcal{L}\bigl((Q)\bigr)$. The Riemann–Roch theorem (II.5.5c) tells us that

$$\dim \mathcal{L}\bigl((Q)\bigr) = 1.$$

But $\mathcal{L}\bigl((Q)\bigr)$ certainly contains the constant functions; hence $f \in \bar{K}$ and $P = Q$. □

Proposition 3.4. *Let (E, O) be an elliptic curve.*

(a) *For every degree-0 divisor $D \in \operatorname{Div}^0(E)$ there exists a unique point $P \in E$ satisfying*

$$D \sim (P) - (O).$$

Define

$$\sigma : \operatorname{Div}^0(E) \longrightarrow E$$

to be the map that sends D to its associated P.

(b) *The map σ is surjective.*

(c) *Let $D_1, D_2 \in \mathrm{Div}^0(E)$. Then*

$$\sigma(D_1) = \sigma(D_2) \qquad \textit{if and only if} \qquad D_1 \sim D_2.$$

Thus σ induces a bijection of sets (which we also denote by σ),

$$\sigma : \mathrm{Pic}^0(E) \xrightarrow{\sim} E.$$

(d) *The inverse to σ is the map*

$$\kappa : E \xrightarrow{\sim} \mathrm{Pic}^0(E), \qquad P \longmapsto \big(\textit{divisor class of } (P) - (O)\big).$$

(e) *If E is given by a Weierstrass equation, then the "geometric group law" on E described by* (III.2.1) *and the "algebraic group law" induced from $\mathrm{Pic}^0(E)$ using σ are the same.*

PROOF. (a) Since E has genus one, the Riemann–Roch theorem (II.5.5c) says that

$$\dim \mathcal{L}\big(D + (O)\big) = 1.$$

Let $f \in \bar{K}(E)$ be a nonzero element of $\mathcal{L}\big(D + (O)\big)$, so f is a basis for this one-dimensional vector space. Since

$$\mathrm{div}(f) \ge -D - (O) \qquad \text{and} \qquad \deg(\mathrm{div}(f)) = 0,$$

it follows that

$$\mathrm{div}(f) = -D - (O) + (P)$$

for some $P \in E$. Hence

$$D \sim (P) - (O),$$

which gives the existence of a point with the desired property.

Next suppose that $P' \in E$ has the same property. Then

$$(P) \sim D + (O) \sim (P'),$$

so (III.3.3) tells us that $P = P'$. Hence P is unique.

(b) For any $P \in E$, we have

$$\sigma\big((P) - (O)\big) = P.$$

(c) Let $D_1, D_2 \in \mathrm{Div}^0(E)$, and set $P_i = \sigma(D_i)$ for $i = 1, 2$. Then from the definition of σ we have

$$(P_1) - (P_2) \sim D_1 - D_2.$$

Thus if $P_1 = P_2$, then $D_1 \sim D_2$; and conversely, if $D_1 \sim D_2$, then $(P_1) \sim (P_2)$, so $P_1 = P_2$ from (III.3.3).

(d) Clear.

(e) Let E be given by a Weierstrass equation and let $P, Q, \in E$. It suffices to show that

$$\kappa(P+Q) = \kappa(P) + \kappa(Q).$$

(N.B. The first $+$ is addition on E using (III.2.1), while the second $+$ is addition of divisor classes in $\mathrm{Pic}^0(E)$.)

Let

$$f(X,Y,Z) = \alpha X + \beta Y + \gamma Z = 0$$

give the line L in $\mathbb{P}^2$ going through P and Q, let R be the third point of intersection of L with E, and let

$$f'(X,Y,Z) = \alpha' X + \beta' Y + \gamma' Z = 0$$

be the line L' through R and O. Then from the definition of addition on E (III.2.1) and the fact that the line $Z = 0$ intersects E at O with multiplicity 3, we have

$$\begin{aligned} \mathrm{div}(f/Z) &= (P) + (Q) + (R) - 3(O), \\ \mathrm{div}(f'/Z) &= (R) + (P+Q) - 2(O). \end{aligned}$$

Hence

$$(P+Q) - (P) - (Q) + (O) = \mathrm{div}(f'/f) \sim 0,$$

so

$$\kappa(P+Q) - \kappa(P) - \kappa(Q) = 0.$$

This proves that κ is a group homomorphism. □

Corollary 3.5. *Let E be an elliptic curve and let $D = \sum n_P(P) \in \mathrm{Div}(E)$. Then D is a principal divisor if and only if*

$$\sum_{P\in E} n_P = 0 \qquad \textit{and} \qquad \sum_{P\in E} [n_P]P = O.$$

(*Note that the first sum is of integers, while the second is addition on E.*)

PROOF. From (II.3.1b), every principal divisor has degree 0. Next let $D \in \mathrm{Div}^0(E)$. We use (III.3.4a,e) to deduce that

$$D \sim 0 \iff \sigma(D) = O \iff \sum_{P\in E} [n_P]\sigma\big((P)-(O)\big) = O.$$

This is the desired result, since $\sigma\big((P)-(O)\big) = P$. □

Remark 3.5.1. If we combine (III.3.4) and (II.3.4), we see that every elliptic curve E/K fits into an exact sequence

$$1 \longrightarrow \bar{K}^* \longrightarrow \bar{K}(E)^* \xrightarrow{\mathrm{div}} \mathrm{Div}^0(E) \xrightarrow{\ \sigma\ } E \longrightarrow 0,$$

where σ is the operation "sum the points in the divisor using the group law on E." Further, Exercise 2.13b implies that the sequence remains exact if we take $G_{\bar{K}/K}$-invariants,

$$1 \longrightarrow K^* \longrightarrow K(E)^* \xrightarrow{\text{div}} \text{Div}^0_K(E) \xrightarrow{\sigma} E(K) \longrightarrow 0.$$

(See also (X.3.8).)

We now prove the fundamental fact that the addition law on an elliptic curve is a *morphism*. Addition is a map $E \times E \to E$ and the variety $E \times E$ has dimension 2, so we cannot use (II.2.1) directly; but (II.2.1) will play a crucial role in the proof. One can also give a proof using explicit equations, but the algebra is somewhat lengthy; see (III.3.6.1).

Theorem 3.6. *Let E/K be an elliptic curve. Then the equations* (III.2.3) *giving the group law on E define morphisms*

$$\begin{aligned} +\,:\, E \times E &\longrightarrow E, \\ (P_1, P_2) &\longmapsto P_1 + P_2, \end{aligned} \qquad \textit{and} \qquad \begin{aligned} -\,:\, E &\longrightarrow E, \\ P &\longmapsto -P. \end{aligned}$$

PROOF. First, the negation map

$$(x, y) \longmapsto (x, -y - a_1 x - a_3)$$

is clearly a rational map $E \to E$. Since E is smooth, it follows from (II.2.1) that negation is a morphism.

Next we fix a point $Q \neq O$ on E and consider the *translation-by-Q map*

$$\tau : E \longrightarrow E, \qquad \tau(P) = P + Q.$$

From the addition formula given in (III.2.3c), this is clearly a rational map; and thus, again using (II.2.1), it is a morphism. In fact, since τ has an inverse, namely $P \mapsto P - Q$, it is an isomorphism.

Finally, consider the general addition map $+ : E \times E \to E$. From (III.2.3c) we see that it is a morphism except possibly at pairs of points having one of the following forms,

$$(P, P), \quad (P, -P), \quad (P, O), \quad (O, P),$$

since for pairs of points not of this form, the rational functions

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \qquad \text{and} \qquad \nu = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}$$

on $E \times E$ are well-defined.

To deal with the four exceptional cases, we could work directly with the definition of morphism; see (III.3.6.1). However, we prefer to let the group law assist us. Thus let τ_1 and τ_2 be translation maps as above for points Q_1 and Q_2, respectively. Consider the composition of maps

$$\phi : E \times E \xrightarrow{\tau_1 \times \tau_2} E \times E \xrightarrow{+} E \xrightarrow{\tau_1^{-1}} E \xrightarrow{\tau_2^{-1}} E.$$

Since the group law on E is associative and commutative (III.2.2), the net effect of the above maps is as follows:

$$\begin{aligned}(P_1, P_2) &\xrightarrow{\tau_1 \times \tau_2} (P_1 + Q_1, P_2 + Q_2)\\ &\xrightarrow{+} P_1 + Q_1 + P_2 + Q_2\\ &\xrightarrow{\tau_1^{-1}} P_1 + P_2 + Q_2\\ &\xrightarrow{\tau_2^{-1}} P_1 + P_2.\end{aligned}$$

Thus the rational map ϕ agrees with the addition map wherever they are both defined.

Further, since the τ_i's are isomorphisms, it follows from the above discussion that ϕ is a morphism except possibly at pairs of points of the form

$$(P - Q_1, P - Q_2), \quad (P - Q_1, -P - Q_2), \quad (P - Q_1, -Q_2), \quad (-Q_1, P - Q_2).$$

But Q_1 and Q_2 are arbitrary points. Hence by varying Q_1 and Q_2, we can find a finite set of rational maps

$$\phi_1, \phi_2, \ldots, \phi_n : E \times E \longrightarrow E$$

with the following properties:

(i) ϕ_1 is the addition map given in (III.2.3c).

(ii) For each $(P_1, P_2) \in E \times E$, some ϕ_i is defined at (P_1, P_2).

(iii) If ϕ_i and ϕ_j are both defined at (P_1, P_2), then $\phi_i(P_1, P_2) = \phi_j(P_1, P_2)$.

It follows that addition is defined on all of $E \times E$, so it is a morphism. □

Remark 3.6.1. During the course of proving (III.3.6), we noted that the formulas in (III.2.3c) make it clear that the addition map $+ : E \times E \to E$ is a morphism except possibly at pairs of points of the form $(P, \pm P)$, (P, O), or (O, P). Rather than using translation maps to circumvent this difficulty, one can work directly with the definition of morphism using explicit equations. It turns out that this involves consideration of quite a few cases; we do one to illustrate the method.

Thus let $(x_1, y_1; x_2, y_2)$ be Weierstrass coordinates on $E \times E$. We will show explicitly that addition is a morphism at points of the form (P, P) with $P \neq O$ and $[2]P \neq O$. Note that addition is defined in general by the formulas given in (III.2.3c):

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \qquad \nu = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1} = y_1 - \lambda x_1,$$
$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2, \qquad y_3 = -(\lambda + a_1)x_3 - \nu - a_3.$$

Here we view λ, ν, x_3, y_3 as functions on $E \times E$, and addition is given by the map $[x_3, y_3, 1] : E \times E \to E$. Thus to show that addition is a morphism at (P, P), it suffices to show that λ is a morphism at (P, P). By assumption, both pairs of functions (x_1, y_1) and (x_2, y_2) satisfy the same Weierstrass equation. Subtracting one equation from the other and factoring yields

$$(y_1 - y_2)(y_1 + y_2 + a_1x_1 + a_3)$$
$$= (x_1 - x_2)(x_1^2 + x_1x_2 + x_2^2 + a_2x_1 + a_2x_2 + a_4 - a_1y_2).$$

Thus λ, considered as a function on $E \times E$, may also be written as

$$\lambda(P_1, P_2) = \frac{x_1^2 + x_1x_2 + x_2^2 + a_2x_1 + a_2x_2 + a_4 - a_1y_2}{y_1 + y_2 + a_1x_1 + a_3}.$$

Therefore, letting $P = (x, y)$, we have

$$\lambda(P, P) = \frac{3x^2 + 2a_2x + a_4 - a_1y}{2y + a_1x + a_3}.$$

Hence λ is a morphism at (P, P) provided that $2y(P) + a_1x(P) + a_3 \neq 0$, and we have excluded this case by our assumption that $[2]P \neq O$. We leave it as an exercise for the reader to deal similarly with the other cases.

III.4 Isogenies

Having examined in some detail the geometry of individual elliptic curves, we turn now to the study of the maps between curves. Since an elliptic curve has a distinguished zero point, it is natural to single out the maps that respect this property.

Definition. Let E_1 and E_2 be elliptic curves. An *isogeny* from E_1 to E_2 is a morphism

$$\phi : E_1 \longrightarrow E_2 \quad \text{satisfying} \quad \phi(O) = O.$$

Two elliptic curves E_1 and E_2 are *isogenous* if there is an isogeny from E_1 to E_2 with $\phi(E_1) \neq \{O\}$. We will see later (III.6.1) that this is an equivalence relation.

It follows from (II.2.3) that an isogeny satisfies either

$$\phi(E_1) = \{O\} \qquad \text{or} \qquad \phi(E_1) = E_2.$$

Thus except for the zero isogeny defined by $[0](P) = O$ for all $P \in E_1$, every other isogeny is a finite map of curves. Hence we obtain the usual injection of function fields (II §2),

$$\phi^* : \bar{K}(E_2) \longrightarrow \bar{K}(E_1).$$

The degree of ϕ, which is denoted by $\deg \phi$, is the degree of the finite extension $\bar{K}(E_1)/\phi^*\bar{K}(E_2)$, and similarly for the separable and inseparable degrees, denoted respectively by $\deg_s \phi$ and $\deg_i \phi$. We also refer to the map ϕ as being separable, inseparable, or purely inseparable according to the corresponding property of the field extension. Further, by convention we set

$$\deg[0] = 0.$$

This convention ensures that we have

$$\deg(\psi\circ\phi)=\deg(\psi)\deg(\phi) \quad \text{for all chains of isogenies} \quad E_1 \xrightarrow{\phi} E_2 \xrightarrow{\psi} E_3.$$

Elliptic curves are abelian groups, so the maps between them form groups. We denote the set of isogenies from E_1 to E_2 by

$$\operatorname{Hom}(E_1,E_2)=\{\text{isogenies } E_1\to E_2\}.$$

The sum of two isogenies is defined by

$$(\phi+\psi)(P)=\phi(P)+\psi(P),$$

and (III.3.6) implies that $\phi+\psi$ is a morphism, so it is an isogeny. Hence $\operatorname{Hom}(E_1,E_2)$ is a group.

If $E_1=E_2$, then we can also compose isogenies. Thus if E is an elliptic curve, we let

$$\operatorname{End}(E)=\operatorname{Hom}(E,E)$$

be the ring whose addition law is as given above and whose multiplication is composition,

$$(\phi\psi)(P)=\phi\big(\psi(P)\big).$$

(It is not obvious that the distributive law holds, but we will prove it later in this section; see (III.4.8).) The ring $\operatorname{End}(E)$ is called the *endomorphism ring of* E. The invertible elements of $\operatorname{End}(E)$ form the *automorphism group of* E, which is denoted by $\operatorname{Aut}(E)$. The endomorphism ring of an elliptic curve E is an important invariant of E that we will study in some detail throughout the rest of this chapter.

Of course, if E_1, E_2, and E are defined over a field K, then we can restrict attention to those isogenies that are defined over K. The corresponding groups of isogenies are denoted with the usual subscripts; thus

$$\operatorname{Hom}_K(E_1,E_2), \qquad \operatorname{End}_K(E), \qquad \operatorname{Aut}_K(E).$$

We have already seen an example (III.3.2) showing that $\operatorname{Aut}(E)$ may be strictly larger than $\operatorname{Aut}_K(E)$.

Example 4.1. For each $m\in\mathbb{Z}$ we define the *multiplication-by-m isogeny*

$$[m]: E\longrightarrow E$$

in the natural way. Thus if $m>0$, then

$$[m](P)=\underbrace{P+P+\cdots+P}_{m \text{ terms}}.$$

For $m<0$, we set $[m](P)=[-m](-P)$, and we have already defined $[0](P)=O$. Using (III.3.6), an easy induction shows that $[m]$ is a morphism, hence an isogeny, since it clearly sends O to O.

Notice that if E is defined over K, then $[m]$ is defined over K. We start our analysis of the group of isogenies by showing that if $m\neq 0$, then the multiplication-by-m map is nonconstant.

Proposition 4.2. (a) *Let E/K be an elliptic curve and let $m \in \mathbb{Z}$ with $m \neq 0$. Then the multiplication-by-m map*

$$[m] : E \longrightarrow E$$

is nonconstant.

(b) *Let E_1 and E_2 be elliptic curves. Then the group of isogenies*

$$\mathrm{Hom}(E_1, E_2)$$

is a torsion-free $\mathbb{Z}$-module.

(c) *Let E be an elliptic curve. Then the endomorphism ring $\mathrm{End}(E)$ is a (not necessarily commutative) ring of characteristic 0 with no zero divisors.*

PROOF. (a) We start by showing that $[2] \neq [0]$. The duplication formula (III.2.3d) says that if a point $P = (x, y) \in E$ has order 2, then it must satisfy

$$4x^3 + b_2x^2 + 2b_4x + b_6 = 0.$$

If $\mathrm{char}(K) \neq 2$, this shows immediately that there are only finitely many such points. Further, even for $\mathrm{char}(K) = 2$, the only way to have $[2] = [0]$ is for the cubic polynomial to be identically 0, which means that $b_2 = b_6 = 0$, which in turn implies that $\Delta = 0$. Hence in all cases we have $[2] \neq [0]$. Now, using the fact that $[mn] = [m] \circ [n]$, we are reduced to considering the case that m is odd.

Assume now that $\mathrm{char}(K) \neq 2$. Then, using long division, it is easy to verify that the polynomial

$$4x^3 + b_2x^2 + 2b_4x + b_6$$

does not divide the polynomial

$$x^4 - b_4x^2 - 2b_6x - b_8.$$

More precisely, if the first polynomial divides the second, then $\Delta = 0$; see Exercise 3.1. Hence we can find an $x_0 \in \bar{K}$ such that the first polynomial vanishes to higher order at x_0 than does the second. Choosing $y_0 \in \bar{K}$ so that $P_0 = (x_0, y_0) \in E$, the doubling formula implies that $[2]P_0 = O$. In other words, we have shown that E has a nontrivial point P_0 of order 2. Then for odd integers m we have

$$[m]P_0 = P_0 \neq O,$$

so clearly $[m] \neq [0]$.

Finally, if $\mathrm{char}(K) = 2$, then one can proceed as above using the "triplication formula" (Exercise 3.2) to produce a point of order 3. We leave this approach to the reader, since later in this chapter we prove a result (III.5.4) that includes the case of $\mathrm{char}(K) = 2$ and m odd.

(b) This follows immediately from (a). Suppose that $\phi \in \mathrm{Hom}(E_1, E_2)$ and $m \in \mathbb{Z}$ satisfy

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

Taking degrees gives

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

so either $m = 0$, or else (a) implies that $\deg[m] \ge 1$, in which case we must have $\phi = [0]$.
(c) From (b), the endomorphism ring $\mathrm{End}(E)$ has characteristic 0. Suppose that $\phi, \psi \in \mathrm{End}(E)$ satisfy $\phi \circ \psi = [0]$. Then

$$(\deg\phi)(\deg\psi) = \deg(\phi\circ\psi) = 0.$$

It follows that either $\phi = [0]$ or $\psi = [0]$. Therefore $\mathrm{End}(E)$ has no zero divisors. □

Definition. Let E be an elliptic curve and let $m \in \mathbb{Z}$ with $m \ge 1$. The *m-torsion subgroup of E*, denoted by $E[m]$, is the set of points of E of order m,

$$E[m] = \big\{P \in E : [m]P = O\big\}.$$

The *torsion subgroup of E*, denoted by E_{tors}, is the set of points of finite order,

$$E_{\text{tors}} = \bigcup_{m=1}^{\infty} E[m].$$

If E is defined over K, then $E_{\text{tors}}(K)$ denotes the points of finite order in $E(K)$.

The most important fact about the multiplication-by-m map is that it has degree m^2, from which one can deduce the structure of the finite group $E[m]$. We do not prove this result here, because it is an immediate corollary of the material on dual isogenies covered in (III §6). However, the reader should be aware that there are completely elementary, but rather messy, proofs that $\deg[m] = m^2$ using explicit formulas and induction. (See exercises 3.7, 3.8, and 3.9 for various approaches.)

Remark 4.3. Suppose that $\mathrm{char}(K) = 0$. Then the map

$$[\ ] : \mathbb{Z} \longrightarrow \mathrm{End}(E)$$

is usually the whole story, i.e., $\mathrm{End}(E) \cong \mathbb{Z}$. If $\mathrm{End}(E)$ is strictly larger than $\mathbb{Z}$, then we say that E has *complex multiplication*, or CM for short. Elliptic curves with complex multiplication have many special properties; see (C §11) for a brief dicussion. On the other hand, if K is a finite field, then $\mathrm{End}(E)$ is always larger than $\mathbb{Z}$; see (V §3).

Example 4.4. Assume that $\mathrm{char}(K) \ne 2$ and let $i \in \bar{K}$ be a primitive fourth root of unity, i.e., $i^2 = -1$. Then, as noted in (III.3.2), the elliptic curve E/K given by the equation

$$E : y^2 = x^3 - x$$

has endomorphism ring $\mathrm{End}(E)$ strictly larger than $\mathbb{Z}$, since it contains a map, which we denote by $[i]$, given by

$$[i] : (x, y) \longmapsto (-x, iy).$$

Thus E has complex multiplication. Clearly $[i]$ is defined over K if and only if $i \in K$. Hence even if E is defined over K, it may happen that $\mathrm{End}_K(E)$ is strictly smaller than $\mathrm{End}(E)$.

Continuing with this example, we observe that

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

so $[i] \circ [i] = [-1]$. There is thus a ring homomorphism

$$\mathbb{Z}[i] \longrightarrow \mathrm{End}(E), \qquad m + ni \longmapsto [m] + [n] \circ [i].$$

If $\mathrm{char}(K) = 0$, this map is an isomorphism, $\mathbb{Z}[i] \cong \mathrm{End}(E)$, in which case

$$\mathrm{Aut}(E) \cong \mathbb{Z}[i]^* = \{\pm 1, \pm i\}$$

is a cyclic group of order 4.

Example 4.5. Again assume that $\mathrm{char}(K) \neq 2$ and let $a, b \in K$ satisfy $b \neq 0$ and $r = a^2 - 4b \neq 0$. Consider the two elliptic curves

$$E_1 : y^2 = x^3 + ax^2 + bx,$$
$$E_2 : Y^2 = X^3 - 2aX^2 + rX.$$

There are isogenies of degree 2 connecting these curves,

$$\begin{aligned} &\phi : E_1 \longrightarrow E_2, \\ &(x,y) \longmapsto \left(\frac{y^2}{x^2}, \frac{y(b-x^2)}{x^2} \right), \end{aligned} \qquad \begin{aligned} &\hat{\phi} : E_2 \longrightarrow E_1, \\ &(X,Y) \longmapsto \left(\frac{Y^2}{4X^2}, \frac{Y(r-X^2)}{8X^2} \right). \end{aligned}$$

A direct computation shows that $\hat{\phi} \circ \phi = [2]$ on E_1 and $\phi \circ \hat{\phi} = [2]$ on E_2. The maps ϕ and $\hat{\phi}$ are examples of *dual isogenies*, which we discuss further in (III §6).

Example 4.6. Let K be a field of characteristic $p > 0$, let $q = p^r$, and let E/K be an elliptic curve given by a Weierstrass equation. We recall from (II §2) that the curve $E^{(q)}/K$ is defined by raising the coefficients of the equation for E to the q^{th} power, and the Frobenius morphism ϕ_q is defined by

$$\phi_q : E \longrightarrow E^{(q)}, \qquad (x,y) \longmapsto (x^q, y^q).$$

Since $E^{(q)}$ is the zero locus of a Weierstrass equation, it will be an elliptic curve provided that its equation is nonsingular. Writing everything out in terms of Weierstrass coefficients and using the fact that the q^{th}-power map $K \to K$ is a homomorphism, it is clear that

$$\Delta(E^{(q)}) = \Delta(E)^q \qquad \text{and} \qquad j(E^{(q)}) = j(E)^q.$$

In particular, the equation for $E^{(q)}$ is nonsingular.

Now suppose that $K = \mathbb{F}_q$ is a finite field with q elements. Then the q^{th}-power map on K is the identity, so $E^{(q)} = E$ and ϕ_q is an endomorphism of E, called the *Frobenius endomorphism*. The set of points fixed by ϕ_q is exactly the finite group $E(\mathbb{F}_q)$. This fact lies at the heart of Hasse's proof of an estimate for $\#E(\mathbb{F}_q)$; see (V §1).

Example 4.7. Let E/K be an elliptic curve and let $Q \in E$. Then we can define a *translation-by-Q map*

$$\tau_Q : E \longrightarrow E, \qquad P \longmapsto P + Q.$$

The map τ_Q is clearly an isomorphism, since τ_{-Q} provides an inverse. Of course, it is not an isogeny unless $Q = O$.

Now consider an arbitrary morphism

$$F : E_1 \longrightarrow E_2$$

of elliptic curves. The composition

$$\phi = \tau_{-F(O)} \circ F$$

is an isogeny, since $\phi(O) = O$. This proves that any morphism F between elliptic curves can be written as

$$F = \tau_{F(O)} \circ \phi,$$

the composition of an isogeny and a translation.

An isogeny is a map between elliptic curves that sends O to O. Since an elliptic curve is a group, it might seem more natural to focus on those isogenies that are group homomorphisms. However, as we now show, it turns out that every isogeny is automatically a homomorphism.

Theorem 4.8. *Let*

$$\phi : E_1 \longrightarrow E_2$$

be an isogeny. Then

$$\phi(P + Q) = \phi(P) + \phi(Q) \qquad \textit{for all } P, Q \in E_1.$$

PROOF. If $\phi(P) = O$ for all $P \in E$, there is nothing to prove. Otherwise, ϕ is a finite map, so by (II.3.7), it induces a homomorphism

$$\phi_* : \mathrm{Pic}^0(E_1) \longrightarrow \mathrm{Pic}^0(E_2)$$

defined by

$$\phi_*\big(\text{class of } \sum n_i(P_i)\big) = \text{class of } \sum n_i(\phi P_i).$$

On the other hand, from (III.3.4) we have *group isomorphisms*

$$\kappa_i : E_i \longrightarrow \mathrm{Pic}^0(E_i), \qquad P \longmapsto \text{class of } (P) - (O).$$

Then, since $\phi(O) = O$, we obtain the following commutative diagram:

$$\begin{array}{ccc} E_1 & \xrightarrow[\kappa_1]{\cong} & \mathrm{Pic}^0(E_1) \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\phi_*} \\ E_2 & \xrightarrow[\kappa_2]{\cong} & \mathrm{Pic}^0(E_2). \end{array}$$

Since κ_1, κ_2, and ϕ_* are all group homomorphisms and κ_2 is injective, it follows that ϕ is also a homomorphism. □

Corollary 4.9. *Let $\phi : E_1 \to E_2$ be a nonzero isogeny. Then*

$$\ker \phi = \phi^{-1}(O)$$

is a finite group.

PROOF. It is a subgroup of E_1 from (III.4.8), and it is finite (of order at most $\deg \phi$) from (II.2.6a). □

The next three results, (III.4.10), (III.4.11), and (III.4.12), encompass the basic Galois theory of elliptic function fields.

Theorem 4.10. *Let $\phi : E_1 \to E_2$ be a nonzero isogeny.*

(a) *For every $Q \in E_2$,*

$$\#\phi^{-1}(Q) = \deg_s \phi.$$

Further, for every $P \in E_1$,

$$e_\phi(P) = \deg_i \phi.$$

(b) *The map*

$$\ker \phi \longrightarrow \operatorname{Aut}\bigl(\bar{K}(E_1)/\phi^*\bar{K}(E_2)\bigr), \qquad T \longmapsto \tau_T^*,$$

is an isomorphism. (Here τ_T is the translation-by-T map (III.4.7) *and τ_T^* is the automorphism that τ_T induces on $\bar{K}(E_1)$.)*

(c) *Suppose that ϕ is separable. Then ϕ is unramified,*

$$\#\ker \phi = \deg \phi,$$

and $\bar{K}(E_1)$ is a Galois extension of $\phi^*\bar{K}(E_2)$.

PROOF. (a) From (II.2.6b) we know that

$$\#\phi^{-1}(Q) = \deg_s \phi \qquad \text{for all but finitely many } Q \in E_2.$$

But for any $Q, Q' \in E_2$, if we choose some $R \in E_1$ with $\phi(R) = Q' - Q$, then the fact that ϕ is a homomorphism implies that there is a one-to-one correspondence

$$\phi^{-1}(Q) \longrightarrow \phi^{-1}(Q'), \qquad P \longmapsto P + R.$$

Hence

$$\#\phi^{-1}(Q) = \deg_s \phi \qquad \text{for all } Q \in E_2,$$

which proves the first assertion.

Now let $P, P' \in E_1$ with $\phi(P) = \phi(P') = Q$, and let $R = P' - P$. Then $\phi(R) = O$, so $\phi \circ \tau_R = \phi$. Therefore, using (II.2.6c) and the fact that τ_R is an isomorphism,

$$e_\phi(P) = e_{\phi\circ\tau_R}(P) = e_\phi\bigl(\tau_R(P)\bigr)e_{\tau_R}(P) = e_\phi(P').$$

Hence every point in $\phi^{-1}(Q)$ has the same ramification index. We compute

$$\begin{aligned}(\deg_s \phi)(\deg_i \phi) = \deg \phi &= \sum_{P\in\phi^{-1}(Q)} e_\phi(P) && \text{from (II.2.6a),}\\ &= \bigl(\#\phi^{-1}(Q)\bigr)e_\phi(P) && \text{for any } P\in\phi^{-1}(Q),\\ &= (\deg_s \phi)e_\phi(P) && \text{from above.}\end{aligned}$$

Canceling $\deg_s \phi$ gives the second assertion.
(b) First, if $T \in \ker\phi$ and $f \in \bar{K}(E_2)$, then

$$\tau_T^*(\phi^* f) = (\phi\circ\tau_T)^* f = \phi^* f,$$

since $\phi\circ\tau_T = \phi$. Hence as an automorphism of $\bar{K}(E_1)$, the map τ_T^* fixes $\phi^*\bar{K}(E_2)$, so the map in (b) is well-defined. Next, since

$$\tau_S \circ \tau_T = \tau_{S+T} = \tau_T \circ \tau_S,$$

the map in (b) is a homomorphism. Finally, from (a) we have

$$\#\ker\phi = \deg_s \phi,$$

while a basic result from Galois theory says that

$$\#\operatorname{Aut}\bigl(\bar{K}(E_1)/\phi^*\bar{K}(E_2)\bigr) \le \deg_s \phi.$$

Hence to prove that the map $T \to \tau_T^*$ is an isomorphism, it suffices to show that it is injective. But if τ_T^* fixes $\bar{K}(E_1)$, then in particular every function on E_1 takes the same value at T and O. This clearly implies that $T = O$, since for example, the coordinate function x has a pole at O and no other poles.
(c) If ϕ is separable, then from (a) we see that

$$\#\phi^{-1}(Q) = \deg\phi \qquad \text{for all } Q\in E_2.$$

Hence ϕ is unramified (II.2.7), and putting $Q = O$ gives

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

Then from (b) we find that

$$\#\operatorname{Aut}\bigl(\bar{K}(E_1)/\phi^*\bar{K}(E_2)\bigr) = \bigl[\bar{K}(E_1) : \phi^*\bar{K}(E_2)\bigr],$$

so $\bar{K}(E_1)/\phi^*\bar{K}(E_2)$ is a Galois extension. □

Corollary 4.11. *Let*

$$\phi : E_1 \longrightarrow E_2 \qquad \textit{and} \qquad \psi : E_1 \longrightarrow E_3$$

be nonconstant isogenies, and assume that ϕ is separable. If

$$\ker\phi \subset \ker\psi,$$

then there is a unique isogeny

$$\lambda : E_2 \longrightarrow E_3$$

satisfying $\psi = \lambda \circ \phi$.

PROOF. Since ϕ is separable, (III.4.10c) says that $\bar{K}(E_1)$ is a Galois extension of $\phi^*\bar{K}(E_2)$. Then the inclusion $\ker\phi \subset \ker\psi$ and the identification (III.4.10b) imply that every element of $\mathrm{Gal}\big(\bar{K}(E_1)/\phi^*\bar{K}(E_2)\big)$ fixes $\psi^*\bar{K}(E_3)$. Hence by Galois theory, there are field inclusions

$$\psi^*\bar{K}(E_3) \subset \phi^*\bar{K}(E_2) \subset \bar{K}(E_1).$$

Now (II.2.4b) gives a map

$$\lambda : E_2 \longrightarrow E_3$$

satisfying

$$\phi^*\big(\lambda^*\bar{K}(E_3)\big) = \psi^*\bar{K}(E_3),$$

and this in turn implies that

$$\lambda \circ \phi = \psi.$$

Finally, λ is an isogeny, since

$$\lambda(O) = \lambda\big(\phi(O)\big) = \psi(O) = O. \qquad \square$$

Proposition 4.12. *Let E be an elliptic curve and let Φ be a finite subgroup of E. There are a unique elliptic curve E' and a separable isogeny*

$$\phi : E \longrightarrow E' \qquad \textit{satisfying} \qquad \ker\phi = \Phi.$$

Remark 4.13.1. The elliptic curve whose existence is asserted in this corollary is often denoted by the quotient E/Φ. This notation clearly indicates the group structure, but there is no a priori reason why this quotient group should correspond to the points of an elliptic curve, nor why the natural group homomorphism $E \to E/\Phi$ should be a morphism. In general, it turns out that the quotient of any variety by a finite group of automorphisms is again a variety (see [186, §7]). The case of curves is done in Exercise 3.13.

Remark 4.13.2. Suppose that E is defined over K and that Φ is $G_{\bar{K}/K}$-invariant. In other words, if $T \in \Phi$, then $T^\sigma \in \Phi$ for all $\sigma \in G_{\bar{K}/K}$. Then the curve E' and isogeny ϕ described in (III.4.12) can be defined over K; see Exercise 3.13e.

Remark 4.13.3. For a given curve E and subgroup Φ, Velu [297] describes how to explicitly write down equations for the curve $E' = E/\Phi$ and isogeny $\phi : E \to E'$.

PROOF OF (III.4.12). As in (III.4.10b), each point $T \in \Phi$ gives rise to an automorphism τ_T^* of $\bar{K}(E)$. Let $\bar{K}(E)^\Phi$ be the subfield of $\bar{K}(E)$ fixed by every element of Φ. Then Galois theory tells us that $\bar{K}(E)$ is a Galois extension of $\bar{K}(E)^\Phi$ with Galois group isomorphic to Φ.

The field $\bar{K}(E)^\Phi$ has transcendence degree one over $\bar{K}$, so from (II.2.4c) there are a unique smooth curve $C/\bar{K}$ and a finite morphism

$$\phi : E \longrightarrow C \qquad \text{satisfying} \qquad \phi^*\bar{K}(C) = \bar{K}(E)^\Phi.$$

We next show that ϕ is unramified. Let $P \in E$ and $T \in \Phi$. Then for *every* function $f \in \bar{K}(C)$,

$$f\big(\phi(P+T)\big) = (\tau_T^* \circ \phi^*)f\big(P\big) = (\phi^* f)(P) = f\big(\phi(P)\big),$$

where the middle equality uses the fact that τ_T^* fixes every element of $\phi^*\bar{K}(C)$. It follows that $\phi(P+T) = \phi(P)$. Now let $Q \in C$ and choose any point $P \in E$ with $\phi(P) = Q$. Then

$$\phi^{-1}(Q) \supset \{P + T : T \in \Phi\}.$$

However, we also know from (II.2.6(a)) that

$$\#\phi^{-1}(Q) \le \deg \phi = \#\Phi,$$

with equality if and only if ϕ is unramified at all points in the inverse image $\phi^{-1}(Q)$. Since the points $P+T$ are distinct as T ranges over the elements of Φ, we conclude that ϕ is unramified at all points in $\phi^{-1}(Q)$; and since Q was arbitrary, the map ϕ is unramified.

Finally, we apply the Hurwitz genus formula (II.5.9) to ϕ. Since ϕ is unramified, the formula reads

$$2\,\mathrm{genus}(E) - 2 = (\deg\phi)(2\,\mathrm{genus}(C) - 2).$$

From this we conclude that C also has genus one, and hence C becomes an elliptic curve and ϕ becomes an isogeny if we take $\phi(O)$ to be the "zero point" on C. □

III.5 The Invariant Differential

Let E/K be an elliptic curve given by the usual Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

We have seen (III.1.5) that the differential

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

has neither zeros nor poles. We now justify its name of *invariant differential* by proving that it is invariant under translation.

Proposition 5.1. *Let E and ω be as above, let $Q \in E$, and let $\tau_Q : E \to E$ be the translation-by-Q map* (III.4.7)*. Then*

$$\tau_Q^*\omega = \omega.$$

PROOF. One can prove this proposition by a straightforward, but messy and unenlightening, calculation as follows. Write $x(P+Q)$ and $y(P+Q)$ in terms of $x(P)$, $x(Q)$, $y(P)$, and $y(Q)$ using the addition formula (III.2.3c). Then use standard differentiation rules to calculate $dx(P+Q)$ as a rational function times $dx(P)$, treating $x(Q)$ and $y(Q)$ as constants. In this way one can directly verify that for a fixed value of Q,

$$\frac{dx(P+Q)}{2y(P+Q)+a_1x(P+Q)+a_3} = \frac{dx(P)}{2y(P)+a_1x(P)+a_3}.$$

We leave the details of this calculation to the reader and instead give a more illuminating proof.

Since Ω_E is a one-dimensional $\bar{K}(E)$-vector space (II.4.2), there is function $a_Q \in \bar{K}(E)^*$, depending a priori on Q, such that

$$\tau_Q^*\omega = a_Q\omega.$$

(Note that $a_Q \neq 0$, because τ_Q is an isomorphism.) We compute

$$\begin{aligned}\operatorname{div}(a_Q) &= \operatorname{div}(\tau_Q^*\omega) - \operatorname{div}(\omega)\\ &= \tau_Q^* \operatorname{div}(\omega) - \operatorname{div}(\omega)\\ &= 0 \qquad \text{since } \operatorname{div}(\omega) = 0 \text{ from (III.1.5).}\end{aligned}$$

Hence a_Q is a function on E having neither zeros nor poles, so (II.1.2) tells us that it is constant, i.e., $a_Q \in \bar{K}^*$.

Next consider the map

$$f : E \longrightarrow \mathbb{P}^1, \qquad Q \longmapsto [a_Q, 1].$$

From the calculation sketched earlier, even without doing it explicitly, it is clear that a_Q can be expressed as a rational function of $x(Q)$ and $y(Q)$. Hence f is a rational map from E to $\mathbb{P}^1$, and it is not surjective, since it misses both $[0,1]$ and $[1,0]$. We conclude from (II.2.1) and (II.2.3) that f is constant. Thus a_Q does not depend on Q, and we find its value by noting that

$$a_Q = a_O = 1 \qquad \text{for all } Q \in E.$$

This completes the proof that $\tau_Q^*\omega = \omega$. □

Differential calculus is, in essence, a linearization tool. It will thus come as no surprise to learn that the enormous utility of the invariant differential on an elliptic curve lies in its ability to linearize the otherwise quite complicated addition law on the curve.

Theorem 5.2. *Let E and E' be elliptic curves, let ω be an invariant differential on E, and let*

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

be isogenies. Then

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

N.B. The two plus signs in this equation represent completely different operations. The first is addition in $\mathrm{Hom}(E', E)$, which is essentially addition using the group law on E. The second is the usual addition in the vector space of differentials $\Omega_{E'}$.

PROOF. If $\phi = [0]$ or $\psi = [0]$, the result is clear. Next, if $\phi + \psi = [0]$, then using the fact that

$$\psi^* = (-\phi)^* = \phi^* \circ [-1]^*,$$

it suffices to check that

$$[-1]^*\omega = -\omega.$$

The negation formula

$$[-1](x, y) = (x, -y - a_1x - a_3)$$

allows us to calculate

$$\begin{aligned}[-1]^* \left(\frac{dx}{2y + a_1x + a_3} \right) &= \frac{dx}{2(-y - a_1x - a_3) + a_1x + a_3} \\ &= -\frac{dx}{2y + a_1x + a_3},\end{aligned}$$

which is the desired result. We now assume that ϕ, ψ, and $\phi + \psi$ are all nonzero.

Let (x_1, y_1) and (x_2, y_2) be "independent" Weierstrass coordinates on E. By this we mean that they satisfy the given Weierstrass equation for E, but satisfy no other algebraic relations. More formally,

$$\big([x_1, y_1, 1], [x_2, y_2, 1]\big)$$

give coordinates for $E \times E$ sitting inside $\mathbb{P}^2 \times \mathbb{P}^2$. (Alternatively, (x_1, y_1) and (x_2, y_2) are "independent generic points of E" in the sense of Weil; see [41, page 213].)

Let

$$(x_3, y_3) = (x_1, y_1) + (x_2, y_2),$$

so x_3 and y_3 are rational combinations of x_1, x_2, y_1, y_2 given by the addition formula (III.2.3c) on E. Further, for any (x, y), let $\omega(x, y)$ denote the corresponding invariant differential,

$$\omega(x, y) = \frac{dx}{2y + a_1x + a_3}.$$

Then, using the addition formula (III.2.3c) and standard rules for differentiation, we can express $\omega(x_3, y_3)$ in terms of $\omega(x_1, y_1)$ and $\omega(x_2, y_2)$. This yields

$$\omega(x_3, y_3) = f(x_1, y_1, x_2, y_2)\omega(x_1, y_1) + g(x_1, y_1, x_2, y_2)\omega(x_2, y_2),$$

where f and g are rational functions of the indicated variables. In doing this calculation, remember that since x_i and y_i satisfy the given Weierstrass equation, the differentials dx_i and dy_i are related by

$$(2y_i + a_1x_i + a_3)\,dy_i = (3x_i^2 + 2a_2x_i + a_4 - a_1y_i)\,dx_i.$$

In this way, $\omega(x_3, y_3)$ can be expressed as a $\bar{K}(x_1, y_1, x_2, y_2)$-linear combination of dx_1 and dx_2.

We claim that both f and g are identically 1. Clearly this can be proven by an explicit calculation, a painful task that we leave for the reader. Instead, we use (III.5.1) to obtain the desired result. Suppose that we assign fixed values to x_2 and y_2, say by choosing some $Q \in E$ and setting

$$x_2 = x(Q) \qquad \text{and} \qquad y_2 = y(Q).$$

Then

$$dx_2 = dx(Q) = 0, \quad \text{so} \quad \omega(x_2, y_2) = 0,$$

while (III.5.1) tells us that

$$\omega(x_3, y_3) = \tau_Q^*\omega(x_1, y_1) = \omega(x_1, y_1).$$

Substituting these into the expression for $\omega(x_3, y_3)$, we find that

$$f\big(x_1, y_1, x(Q), y(Q)\big) = 1$$

as a rational function in $\bar{K}(x_1, y_1)$. Thus f does not depend on x_1 and y_1, so $f \in \bar{K}(x_2, y_2)$. But we also know that $f(x_2, y_2)$ satisfies $f\big(x(Q), y(Q)\big) = 1$ for *every* point $Q \in E$, so f must be identically 1. The same argument using x_2 and y_2 in place of x_1 and y_1 shows that g is also identically 1.

To recapitulate, we have shown that if

$$(x_3, y_3) = (x_1, y_1) + (x_2, y_2) \qquad (+ \text{ is addition on } E),$$

then

$$\omega(x_3, y_3) = \omega(x_1, y_1) + \omega(x_2, y_2) \qquad (+ \text{ is addition in } \Omega_E).$$

Now let (x', y') be Weierstrass coordinates on E' and set

$$(x_1, y_1) = \phi(x', y'), \qquad (x_2, y_2) = \psi(x', y'), \qquad (x_3, y_3) = (\phi + \psi)(x', y').$$

Substituting this into $\omega(x_3, y_3) = \omega(x_1, y_1) + \omega(x_2, y_2)$ yields

$$\big(\omega \circ (\phi + \psi)\big)(x', y') = (\omega \circ \phi)(x', y') + (\omega \circ \psi)(x', y'),$$

which says exactly that

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

Corollary 5.3. *Let ω be an invariant differential on an elliptic curve E. Let $m \in \mathbb{Z}$. Then*

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

PROOF. The assertion is true for $m = 0$, since $[0]$ is the constant map, and it is true for $m = 1$, since $[1]$ is the identity map. We use (III.5.2) with $\phi = [m]$ and $\psi = [1]$ to obtain

$$[m+1]^*\omega = [m]^*\omega + \omega.$$

The desired result now follows by ascending and descending induction. □

As a first indication of the utility of the invariant differential, we give a new, less computational, proof of part of (III.4.2a).

Corollary 5.4. *Let E/K be an elliptic curve and let $m \in \mathbb{Z}$. Assume that $m \neq 0$ in K. Then the multiplication-by-m map on E is a finite separable endomorphism.*

PROOF. Let ω be an invariant differential on E. Then (III.5.3) and our assumption on m implies that

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

so certainly $[m] \neq [0]$. Hence $[m]$ is finite, and (II.4.2c) tells us that $[m]$ is separable. □

As a second application of (III.5.2) and (III.5.3), we examine when a linear combination involving the Frobenius morphism is separable.

Corollary 5.5. *Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$ of characteristic p, let $\phi : E \to E$ be the q^{th}-power Frobenius morphism* (III.4.6)*, and let $m, n \in \mathbb{Z}$. Then the map*

$$m + n\phi : E \longrightarrow E$$

is separable if and only if $p \nmid m$. In particular, the map $1 - \phi$ is separable.

PROOF. Let ω be an invariant differential on E. From (II.4.2c) we know that a map $\psi : E \to E$ is inseparable if and only if $\psi^*\omega = 0$. We apply this criterion to the map $\psi = m + n\phi$. Using (III.5.2) and (III.5.3), we compute

$$(m + n\phi)^*\omega = m\omega + n\phi^*\omega.$$

Note that $\phi^*\omega = 0$, since ϕ is inseparable, or, by direct calculation,

$$\phi^*\left(\frac{dx}{2y + a_1x + a_3}\right) = \frac{d(x^q)}{2y^q + a_1x^q + a_3} = \frac{qx^{q-1}dx}{2y^q + a_1x^q + a_3} = 0.$$

Hence

$$(m + n\phi)^*\omega = [m]^*\omega + [n]^* \circ \phi^*\omega = m\omega.$$

Since $m\omega = 0$ if and only if $p \mid m$, this gives the desired result. □

Corollary 5.6. *Let E/K be an elliptic curve and let ω be a nonzero invariant differential on E. We define a map from $\mathrm{End}(E)$ to $\bar{K}$ in the following way*:

$$\mathrm{End}(E) \longrightarrow \bar{K}, \qquad \phi \longmapsto a_\phi \quad \textit{such that } \phi^*\omega = a_\phi\omega.$$

(a) *The map $\phi \mapsto a_\phi$ is a ring homomorphism.*
(b) *The kernel of $\phi \mapsto a_\phi$ is the set of inseparable endomorphisms of E.*
(c) *If $\mathrm{char}(K) = 0$, then $\mathrm{End}(E)$ is a commutative ring.*

PROOF. As in the proof of (III.5.1), the fact that Ω_E is a one-dimensional $\bar{K}(E)$-vector space (II.4.2) implies that $\phi^*\omega = a_\phi\omega$ for some function $a_\phi \in \bar{K}(E)$. We claim that $a_\phi \in \bar{K}$. This is clear if $a_\phi = 0$, while if $a_\phi \neq 0$, we use the fact that $\mathrm{div}(\omega) = 0$ to compute

$$\mathrm{div}(a_\phi) = \mathrm{div}(\phi^*\omega) - \mathrm{div}(\omega) = \phi^*\,\mathrm{div}(\omega) - \mathrm{div}(\omega) = 0.$$

Hence a_ϕ has no zeros or poles, so (II.1.2) says that $a_\phi \in \bar{K}$.
(a) We use (III.5.2) to compute

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

This gives $a_{\phi+\psi} = a_\phi + a_\psi$. Similarly,

$$a_{\phi\circ\psi}\omega = (\phi\circ\psi)^*\omega = \psi^*(\phi^*\omega) = \psi^*(a_\phi\omega) = a_\phi\psi^*(\omega) = a_\phi a_\psi\omega,$$

which proves that $a_{\phi\circ\psi} = a_\phi a_\psi$.
(b) We have

$$a_\phi = 0 \quad\Longleftrightarrow\quad \phi^*\omega = 0 \quad\Longleftrightarrow\quad \phi \text{ is inseparable (II.4.2c).}$$

(c) If $\mathrm{char}(K) = 0$, then every endomorphism is separable, so (b) says that $\mathrm{End}(E)$ injects into $\bar{K}^*$. Hence $\mathrm{End}(E)$ is commutative. □

III.6 The Dual Isogeny

Let $\phi : E_1 \to E_2$ be a nonconstant isogeny. We have seen (II.3.7) that ϕ induces a map

$$\phi^* : \mathrm{Pic}^0(E_2) \longrightarrow \mathrm{Pic}^0(E_1).$$

On the other hand, for $i = 1$ and 2 we have group isomorphisms (III.3.4)

$$\kappa_i : E_i \longrightarrow \mathrm{Pic}^0(E_i), \qquad P \longmapsto \text{class of } (P) - (O).$$

This gives a homomorphism going in the opposite direction to ϕ, namely the composition

$$E_2 \xrightarrow{\kappa_2} \mathrm{Pic}^0(E_2) \xrightarrow{\phi^*} \mathrm{Pic}^0(E_1) \xrightarrow{\kappa_1^{-1}} E_1.$$

Later in this section we will verify that this map may be computed as follows. Let $Q \in E_2$, and choose any $P \in E_1$ satisfying $\phi(P) = Q$. Then

$$\kappa_1^{-1} \circ \phi^* \circ \kappa_2(Q) = [\deg \phi](P).$$

It is by no means clear that the homomorphism $\kappa_1^{-1} \circ \phi^* \circ \kappa_2$ is an isogeny, i.e., that it is given by a rational map. The process of finding a point P satisfying $\phi(P) = Q$ involves taking roots of various polynomial equations. If ϕ is separable, one needs to check that applying $[\deg \phi]$ to P causes the conjugate roots to appear symmetrically. (It is actually reasonably clear that this is true if one explicitly writes out $\kappa_1^{-1} \circ \phi^* \circ \kappa_2$.) If ϕ is inseparable, this approach is more complicated. We now show that in all cases there is an actual isogeny that may be computed in the manner described above.

Theorem 6.1. *Let $\phi : E_1 \to E_2$ be a nonconstant isogeny of degree m.*
(a) *There exists a unique isogeny*

$$\hat{\phi} : E_2 \longrightarrow E_1 \qquad \textit{satisfying} \qquad \hat{\phi} \circ \phi = [m].$$

(b) *As a group homomorphism, $\hat{\phi}$ equals the composition*

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

PROOF. (a) First we show uniqueness. Suppose that $\hat{\phi}$ and $\hat{\phi}'$ are two such isogenies. Then

$$(\hat{\phi} - \hat{\phi}') \circ \phi = [m] - [m] = [0].$$

Since ϕ is nonconstant, it follows from (II.2.3) that $\hat{\phi} - \hat{\phi}'$ must be constant, so $\hat{\phi} = \hat{\phi}'$.

Next suppose that $\psi : E_2 \to E_3$ is another nonconstant isogeny, say of degree n, and suppose that we know that $\hat{\phi}$ and $\hat{\psi}$ exist. Then

$$(\hat{\phi} \circ \hat{\psi}) \circ (\psi \circ \phi) = \hat{\phi} \circ [n] \circ \phi = [n] \circ \hat{\phi} \circ \phi = [nm].$$

Thus $\hat{\phi} \circ \hat{\psi}$ has the requisite property to be $\widehat{\psi \circ \phi}$. If K has characteristic 0, then ϕ is separable, while if K has positive characteristic, then (II.2.12) allows us to write ϕ as the composition of a separable isogeny and a Frobenius morphism. It thus suffices to prove the existence of $\hat{\phi}$ when ϕ is either separable or equal to the Frobenius morphism.

Case 1. ϕ is separable Since ϕ has degree m, we have (III.4.10c)

$$\#\ker \phi = m,$$

so every element of $\ker \phi$ has order dividing m, i.e.,

$$\ker \phi \subset \ker[m].$$

It follows immediately from (III.4.11) that there is an isogeny

$$\hat{\phi} : E_2 \longrightarrow E_1 \qquad \text{satisfying} \qquad \hat{\phi} \circ \phi = [m].$$

Case 2. ϕ is a Frobenius morphism If ϕ is the q^{th}-power Frobenius morphism with $q = p^e$, then ϕ is clearly the composition of the p^{th}-power Frobenius morphism with itself e times. Hence it suffices to prove that $\hat{\phi}$ exists if ϕ is the p^{th}-power Frobenius morphism, so in particular, $\deg \phi = p$ from (II.2.11).

We look at the multiplication-by-p map on E. Let ω be an invariant differential. Then from (III.5.3) and the fact that $\operatorname{char}(K) = p$, we see that

$$[p]^*\omega = p\omega = 0.$$

We conclude from (II.4.2c) that $[p]$ is not separable, and thus when we decompose $[p]$ as a Frobenius morphism followed by a separable map (II.2.12), the Frobenius morphism does appear. In other words,

$$[p] = \psi \circ \phi^e$$

for some integer $e \ge 1$ and some separable isogeny ψ. Then we can take

$$\hat{\phi} = \psi \circ \phi^{e-1}.$$

(b) Let $Q \in E_2$. Then the image of Q under the indicated composition is

$$\begin{aligned}
&\operatorname{sum}\bigl(\phi^*\bigl((Q) - (O)\bigr)\bigr) \\
&\qquad = \sum_{P \in \phi^{-1}(Q)} [e_\phi(P)]P - \sum_{T \in \phi^{-1}(O)} [e_\phi(T)]T && \text{by definition of } \phi^*, \\
&\qquad = [\deg_i \phi] \left(\sum_{P \in \phi^{-1}(Q)} P - \sum_{T \in \phi^{-1}(O)} T \right) && \text{from (III.4.10a)}, \\
&\qquad = [\deg_i \phi] \circ [\#\phi^{-1}(Q)]P && \text{for any } P \in \phi^{-1}(Q), \\
&\qquad = [\deg \phi]P && \text{from (III.4.10a)}.
\end{aligned}$$

But by construction,

$$\hat{\phi}(Q) = \hat{\phi} \circ \phi(P) = [\deg \phi]P,$$

so the two maps are the same. □

Definition. Let $\phi : E_1 \to E_2$ be an isogeny. The *dual isogeny* to ϕ is the isogeny

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

given by (III.6.1a). (This assumes that $\phi \ne [0]$. If $\phi = [0]$, then we set $\hat{\phi} = [0]$.)

The next theorem gives the basic properties of the dual isogeny. From these basic facts we will be able to deduce a number of very important corollaries, including a good description of the kernel of the multiplication-by-m map.

Theorem 6.2. *Let*

$$\phi : E_1 \longrightarrow E_2$$

be an isogeny.
(a) *Let* $m = \deg \phi$. *Then*

$$\hat{\phi} \circ \phi = [m] \quad \text{on } E_1 \qquad \text{and} \qquad \phi \circ \hat{\phi} = [m] \quad \text{on } E_2.$$

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

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

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

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

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

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

(e) $\deg \hat{\phi} = \deg \phi$.
(f) $\hat{\hat{\phi}} = \phi$.

PROOF. If ϕ is constant, then the entire theorem is trivial, and similarly (b) and (c) are trivial if λ or ψ is constant. We may thus assume that all isogenies are nonconstant.
(a) The first statement is the defining property of $\hat{\phi}$. For the second, consider

$$(\phi \circ \hat{\phi}) \circ \phi = \phi \circ [m] = [m] \circ \phi.$$

Hence $\phi \circ \hat{\phi} = [m]$, since ϕ is not constant.
(b) Letting $n = \deg \lambda$, we have

$$(\hat{\phi} \circ \hat{\lambda}) \circ (\lambda \circ \phi) = \hat{\phi} \circ [n] \circ \phi = [n] \circ \hat{\phi} \circ \phi = [nm].$$

The uniqueness statement in (III.6.1a) implies that

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

(c) We give a proof in characteristic 0. See Exercise 3.31 for a proof in arbitrary characteristic.

Let $x_1, y_1 \in K(E_1)$ and $x_2, y_2 \in K(E_2)$ be Weierstrass coordinates. We start by looking at E_2 considered as an elliptic curve defined over the field $K(E_1) = K(x_1, y_1)$.[1] Then another way of saying that $\phi : E_1 \to E_2$ is an isogeny is to note that $\phi(x_1, y_1) \in E_2\big(K(x_1, y_1)\big)$, and similarly for $\psi(x_1, y_1)$ and $(\phi + \psi)(x_1, y_1)$. Now consider the divisor

[1] This is where we use the characteristic 0 assumption, since all of our results on elliptic curves have assumed that the base field is perfect.

$$D = \big((\phi+\psi)(x_1,y_1)\big) - \big(\phi(x_1,y_1)\big) - \big(\psi(x_1,y_1)\big) + (O) \in \operatorname{Div}_{K(x_1,y_1)}(E_2).$$

The definition of $\phi+\psi$ implies that D sums to O, so (III.3.5) tells us that D is linearly equivalent to 0. Thus there is a function

$$f \in K(x_1,y_1)(E_2) = K(x_1,y_1,x_2,y_2)$$

that, *when considered as a function of x_2 and y_2*, has divisor D.

We now switch perspective and look at f as a function of x_1 and y_1. In other words, we treat f as a function on E_1 considered as an elliptic curve defined over $K(x_2,y_2)$. Suppose that $P_1 \in E_1\big(\overline{K(x_2,y_2)}\big)$ is a point satisfying $\phi(P_1) = (x_2,y_2)$. Then examining D, specifically the term $-\operatorname{div}\big(\phi(x_1,y_1)\big)$, we see that f has a pole at P_1, i.e., the function $f(x_1,y_1;x_2,y_2)$ has a pole if x_1,y_1,x_2,y_2 satisfy $(x_2,y_2)=\phi(x_1,y_1)$. Further,

$$\operatorname{ord}_{P_1}(f) = e_\phi(P_1).$$

Similarly, f has a pole at P_1 if $(x_2,y_2) = \psi(P_1)$, and it has a zero at P_1 if $(x_2,y_2)=(\phi+\psi)(P_1)$. It follows that as a function of x_1 and y_1, the divisor of f has the form

$$(\phi+\psi)^*\big((x_2,y_2)\big) - \phi^*\big((x_2,y_2)\big) - \psi^*\big((x_2,y_2)\big) + \sum n_i(P_i) \in \operatorname{Div}_{\overline{K(x_2,y_2)}}(E_1),$$

where the P_i's are in $E_1(\bar K)$, i.e., $\sum n_i(P_i) \in \operatorname{Div}_{\bar K}(E_1)$. Since this is the divisor of a function, it sums to O, so using (III.6.1b), we conclude that the point

$$\widehat{(\phi+\psi)}(x_2,y_2) - \hat\phi(x_2,y_2) - \hat\psi(x_2,y_2)$$

does not depend on (x_2,y_2), i.e., it is in $E_1(\bar K)$. Putting $(x_2,y_2)=O$ shows that it is equal to O, which completes the proof that

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

(d) This is true for $m=0$ by definition, and it is clearly true for $m=1$. Using (c) with $\phi=[m]$ and $\psi=[1]$ yields

$$\widehat{[m+1]} = \widehat{[m]} + \widehat{[1]},$$

and ascending and descending induction shows that $\widehat{[m]} = [m]$ holds for all m.

Now let $d=\deg[m]$ and consider the multiplication-by-d map. Thus

$$\begin{aligned} [d] &= \widehat{[m]} \circ [m] && \text{definition of dual isogeny,} \\ &= [m^2] && \text{since } \widehat{[m]} = [m]. \end{aligned}$$

Using the fact (III.4.2b) that the endomorphism ring of an elliptic curve is a torsion-free $\mathbb{Z}$-module, it follows that $d=m^2$.

(e) Let $m = \deg\phi$. Then using (d) and (a), we find that

$$m^2 = \deg[m] = \deg(\phi \circ \hat{\phi}) = (\deg\phi)(\deg\hat{\phi}) = m(\deg\hat{\phi}).$$

Hence $m = \deg\hat{\phi}$.
(f) Again let $m = \deg\phi$. Then using (a), (b), and (d) yields

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

Therefore

$$\phi = \hat{\hat{\phi}}.$$

□

Definition. Let A be an abelian group. A function

$$d : A \longrightarrow \mathbb{R}$$

is a *quadratic form* if it satisfies the following conditions:

(i) $d(\alpha) = d(-\alpha)$ for all $\alpha \in A$.

(ii) The pairing

$$A \times A \longrightarrow \mathbb{R}, \qquad (\alpha, \beta) \longmapsto d(\alpha + \beta) - d(\alpha) - d(\beta),$$

is bilinear.

A quadratic form d is *positive definite* if it further satisfies:

(iii) $d(\alpha) \geq 0$ for all $\alpha \in A$.

(iv) $d(\alpha) = 0$ if and only if $\alpha = 0$.

Corollary 6.3. *Let E_1 and E_2 be elliptic curves. The degree map*

$$\deg : \mathrm{Hom}(E_1, E_2) \longrightarrow \mathbb{Z}$$

is a positive definite quadratic form.

PROOF. Everything is clear except for the fact that the pairing

$$\langle \phi, \psi \rangle = \deg(\phi + \psi) - \deg(\phi) - \deg(\psi)$$

is bilinear. To verify this, we use the injection

$$[\ \ ] : \mathbb{Z} \longrightarrow \mathrm{End}(E_1)$$

and compute

$$\begin{aligned} \big[\langle \phi, \psi \rangle\big] &= \big[\deg(\phi + \psi)\big] - \big[\deg(\phi)\big] - \big[\deg(\psi)\big] \\ &= (\widehat{\phi + \psi}) \circ (\phi + \psi) - \hat{\phi} \circ \phi - \hat{\psi} \circ \psi \\ &= \hat{\phi} \circ \psi + \hat{\psi} \circ \phi \qquad \text{from (III.6.2c).} \end{aligned}$$

Using (III.6.2c) a second time, we see that this last expression is linear in both ϕ and ψ. □

Corollary 6.4. *Let E be an elliptic curve and let $m \in \mathbb{Z}$ with $m \neq 0$.*
(a) $\deg[m] = m^2$.
(b) *If $m \neq 0$ in K, i.e., if either $\operatorname{char}(K) = 0$ or $p = \operatorname{char}(K) > 0$ and $p \nmid m$, then*

$$E[m] = \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}.$$

(c) *If $\operatorname{char}(K) = p > 0$, then one of the following is true*:

$$\text{(i)} \quad E[p^e] = \{O\} \quad \textit{for all } e = 1, 2, 3, \ldots.$$
$$\text{(ii)} \quad E[p^e] = \frac{\mathbb{Z}}{p^e\mathbb{Z}} \quad \textit{for all } e = 1, 2, 3, \ldots.$$

(*Recall that $E[m]$ is another notation for $\ker[m]$, the set of points of order m on E.*)

PROOF. (a) This was proven in (III.6.2d). We record it again here in order to point out that there are other ways of proving that $[m]$ has degree m^2; see for example exercises 3.7, 3.8, and 3.11. Then the fundamental description of $E[m]$ in (b) follows formally from (a).
(b) The assumption on m and the fact that $\deg[m] = m^2$ tells us that $[m]$ is a finite separable map. Hence from (III.4.10c),

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

Further, for every integer d dividing m, we similarly have

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

Writing the finite group $E[m]$ as a product of cyclic groups, it is easy to see that the only possibility is

$$E[m] = \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}.$$

(See Exercise 3.30.)
(c) Let ϕ be the p^{th}-power Frobenius morphism. Then

$$\begin{aligned} \#E[p^e] &= \deg_s[p^e] && \text{from (III.4.10a),} \\ &= \big(\deg_s(\hat{\phi} \circ \phi)\big)^e && \text{from (III.6.2a),} \\ &= (\deg_s \hat{\phi})^e && \text{from (II.2.11b).} \end{aligned}$$

From (III.6.2e) and (II.2.11c) we have

$$\deg \hat{\phi} = \deg \phi = p,$$

so there are two cases. If $\hat{\phi}$ is inseparable, then $\deg_s \hat{\phi} = 1$, so

$$\#E[p^e] = 1 \qquad \text{for all } e.$$

Otherwise $\hat{\phi}$ is separable, so $\deg_s \hat{\phi} = p$ and

$$\#E[p^e] = p^e \qquad \text{for all } e.$$

Again writing $E[p^e]$ as a product of cyclic groups, it is easy to see that this implies that

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

(For a more detailed analysis of $E[p^e]$ in characteristic p and its relationship to the endomorphism ring $\mathrm{End}(E)$, see (V §3).) □

III.7 The Tate Module

Let E/K be an elliptic curve and let $m \geq 2$ be an integer, prime to $\mathrm{char}(K)$ if $\mathrm{char}(K) > 0$. As we have seen,

$$E[m] \cong \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}},$$

the isomorphism being one between abstract groups. However, the group $E[m]$ comes equipped with considerably more structure than an abstract group. For example, each element σ of the Galois group $G_{\bar{K}/K}$ acts on $E[m]$, since if $[m]P = O$, then

$$[m](P^\sigma) = \big([m]P\big)^\sigma = O^\sigma = O.$$

We thus obtain a representation

$$G_{\bar{K}/K} \longrightarrow \mathrm{Aut}\big(E[m]\big) \cong \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}),$$

where the latter isomorphism involves choosing a basis for $E[m]$. Individually, for each m, these representations are not completely satisfactory, since it is generally easier to deal with representations whose matrices have coefficients in a ring of characteristic 0. We are going to fit together these mod m representations for varying m in order to create a characteristic 0 representation. To do this, we mimic the inverse limit construction of the ℓ-adic integers $\mathbb{Z}_\ell$ from the finite groups $\mathbb{Z}/\ell^n\mathbb{Z}$.

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

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

the inverse limit being taken with respect to the natural maps

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

Since each $E[\ell^n]$ is a $\mathbb{Z}/\ell^n\mathbb{Z}$-module, we see that the Tate module has a natural structure as a $\mathbb{Z}_\ell$-module. Further, since the multiplication-by-ℓ maps are surjective, the inverse limit topology on $T_\ell(E)$ is equivalent to the ℓ-adic topology that it gains by being a $\mathbb{Z}_\ell$-module.

Proposition 7.1. *The Tate module has the following structure*:

(a) $T_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$ *as a* $\mathbb{Z}_\ell$*-module, if* $\ell \neq \operatorname{char}(K)$.

(b) $T_p(E) \cong \{0\}$ *or* $\mathbb{Z}_p$ *as a* $\mathbb{Z}_p$*-module, if* $p = \operatorname{char}(K) > 0$.

PROOF. This follows immediately from (III.6.4b,c). □

The action of $G_{\bar{K}/K}$ on each $E[\ell^n]$ commutes with the multiplication-by-ℓ map used to form the inverse limit, so $G_{\bar{K}/K}$ also acts on $T_\ell(E)$. Further, since the profinite group $G_{\bar{K}/K}$ acts continuously on each finite (discrete) group $E[\ell^n]$, the resulting action on $T_\ell(E)$ is also continuous.

Definition. The *ℓ-adic representation* (*of $G_{\bar{K}/K}$ associated to E*) is the homomorphism

$$\rho_\ell : G_{\bar{K}/K} \longrightarrow \operatorname{Aut}\bigl(T_\ell(E)\bigr)$$

induced by the action of $G_{\bar{K}/K}$ on the ℓ^n-torsion points of E.

Convention. From here on, the number ℓ always refers to a prime number that is different from the characteristic of K.

Remark 7.2. If we choose a $\mathbb{Z}_\ell$-basis for $T_\ell(E)$, we obtain a representation

$$G_{\bar{K}/K} \longrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell),$$

and then the natural inclusion $\mathbb{Z}_\ell \subset \mathbb{Q}_\ell$ gives a representation

$$G_{\bar{K}/K} \longrightarrow \mathrm{GL}_2(\mathbb{Q}_\ell).$$

In this way we obtain a two-dimensional representation of $G_{\bar{K}/K}$ over a field of characteristic 0. More intrinsically, we can avoid choosing a basis by using the natural map

$$\rho_\ell : G_{\bar{K}/K} \longrightarrow \operatorname{Aut}\bigl(T_\ell(E)\bigr) \hookrightarrow \operatorname{Aut}\bigl(T_\ell(E)\bigr) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

Remark 7.3. The above construction is analogous to the following, which may be more familiar to the reader. Let

$$\boldsymbol{\mu}_{\ell^n} \subset \bar{K}^*$$

be the group of $(\ell^n)^{\text{th}}$ roots of unity. Raising to the ℓ^{th} power gives maps

$$\boldsymbol{\mu}_{\ell^{n+1}} \xrightarrow{\zeta \mapsto \zeta^\ell} \boldsymbol{\mu}_{\ell^n},$$

and then taking the inverse limit yields the *Tate module of K*,

$$T_\ell(\boldsymbol{\mu}) = \varprojlim_n \boldsymbol{\mu}_{\ell^n}.$$

(More formally, $T_\ell(\boldsymbol{\mu})$ is the Tate module of the multiplicative group $\bar{K}^*$.) As abstract groups, we have

$$\boldsymbol{\mu}_{\ell^n} \cong \mathbb{Z}/\ell^n\mathbb{Z} \qquad \text{and} \qquad T_\ell(\boldsymbol{\mu}) \cong \mathbb{Z}_\ell.$$

Further, the natural action of $G_{\bar{K}/K}$ on each $\boldsymbol{\mu}_{\ell^n}$ induces an action on $T_\ell(\boldsymbol{\mu})$, so we obtain a 1-dimensional representation

$$G_{\bar{K}/K} \longrightarrow \mathrm{Aut}\big(T_\ell(\boldsymbol{\mu})\big) \cong \mathbb{Z}_\ell^*.$$

For $K = \mathbb{Q}$, this cyclotomic representation is surjective, because the ℓ-power cyclotomic polynomials are irreducible over $\mathbb{Q}$.

Remark 7.3.1. In Chapter VI, when we study elliptic curves over the complex numbers, we will see (VI.5.6) that there is a natural way in which the m-torsion subgroup $E[m]$ may be identified with the homology group $H_1(E, \mathbb{Z}/m\mathbb{Z})$, and similarly $T_\ell(E)$ with $H_1(E, \mathbb{Z}_\ell)$. The utility of this identification is that while homology groups do not generally admit a Galois action, the torsion subgroup $E[m]$ and Tate module $T_\ell(E)$ do admit such an action. This idea has been vastly generalized by Grothendieck and others in the theory of étale cohomology.

The Tate module is a useful tool for studying isogenies. Let

$$\phi : E_1 \longrightarrow E_2$$

be an isogeny of elliptic curves. Then ϕ induces maps

$$\phi : E_1[\ell^n] \longrightarrow E_2[\ell^n],$$

and hence it induces a $\mathbb{Z}_\ell$-linear map

$$\phi_\ell : T_\ell(E_1) \longrightarrow T_\ell(E_2).$$

We thus obtain a natural homomorphism

$$\mathrm{Hom}(E_1, E_2) \longrightarrow \mathrm{Hom}\big(T_\ell(E_1), T_\ell(E_2)\big).$$

Further, if $E_1 = E_2 = E$, then the map

$$\mathrm{End}(E) \longrightarrow \mathrm{End}\big(T_\ell(E)\big)$$

is even a homomorphism of rings. It is not hard to show that these maps are injective (see Exercise 3.14), but the following result gives much stronger information about the structure of $\mathrm{Hom}(E_1, E_2)$.

Theorem 7.4. *Let E_1 and E_2 be elliptic curves and let $\ell \neq \mathrm{char}(K)$ be a prime. Then the natural map*

$$\mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_\ell \longrightarrow \mathrm{Hom}\big(T_\ell(E_1), T_\ell(E_2)\big), \qquad \phi \longmapsto \phi_\ell,$$

is injective

PROOF. We start by proving the following statement:

$$\left[\begin{array}{l}\text{Let } M \subset \mathrm{Hom}(E_1, E_2) \text{ be a finitely generated subgroup, and let} \\ M^{\mathrm{div}} = \big\{\phi \in \mathrm{Hom}(E_1, E_2) : [m] \circ \phi \in M \text{ for some integer } m \geq 1\big\}. \\ \text{Then } M^{\mathrm{div}} \text{ is finitely generated.}\end{array}\right] \qquad (*)$$

To prove $(*)$, we extend the degree mapping to the finite-dimensional real vector space $M \otimes \mathbb{R}$, which we equip with the natural topology inherited from $\mathbb{R}$. Then the degree mapping is clearly continuous, so the set

$$U = \{\phi \in M \otimes \mathbb{R} : \deg \phi < 1\}$$

is an open neighborhood of 0. Further, since $\mathrm{Hom}(E_1, E_2)$ is a torsion-free $\mathbb{Z}$-module (III.4.2b), there is a natural inclusion

$$M^{\mathrm{div}} \subset M \otimes \mathbb{R}.$$

Further, it is clear that

$$M^{\mathrm{div}} \cap U = \{0\},$$

since every nonzero isogeny has degree at least one. Hence M^{div} is a discrete subgroup of the finite-dimensional vector space $M \otimes \mathbb{R}$, so it is finitely generated. This completes the proof of $(*)$.

We now turn to the proof of (III.7.4). Let $\phi \in \mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_\ell$, and suppose that $\phi_\ell = 0$. Let

$$M \subset \mathrm{Hom}(E_1, E_2)$$

be some finitely generated subgroup with the property that $\phi \in M \otimes \mathbb{Z}_\ell$. Then, with notation as above, the group M^{div} is finitely generated, so it is also free, since (III.4.2b) tells us that it is torsion-free. Let

$$\psi_1, \ldots, \psi_t \in \mathrm{Hom}(E_1, E_2)$$

be a basis for M^{div}, and write

$$\phi = \alpha_1\psi_1 + \cdots + \alpha_t\psi_t \quad \text{with} \quad \alpha_1, \ldots, \alpha_t \in \mathbb{Z}_\ell.$$

Now fix some $n \ge 1$ and choose $a_1, \ldots, a_t \in \mathbb{Z}$ with

$$a_i \equiv \alpha_i \pmod{\ell^n}.$$

Then the assumption that $\phi_\ell = 0$ implies that the isogeny

$$\psi = [a_1] \circ \psi_1 + \cdots + [a_t] \circ \psi_t \in \mathrm{Hom}(E_1, E_2)$$

annihilates $E_1[\ell^n]$. It follows from (III.4.11) that ψ factors through $[\ell^n]$, so there is an isogeny

$$\lambda \in \mathrm{Hom}(E_1, E_2) \qquad \text{satisfying} \qquad \psi = [\ell^n] \circ \lambda.$$

Further, λ is in M^{div}, so there are integers $b_i \in \mathbb{Z}$ such that

$$\lambda = [b_1] \circ \psi_1 + \cdots + [b_t] \circ \psi_t.$$

Then, since the ψ_i's form a $\mathbb{Z}$-basis for M^{div}, the fact that $\psi = [\ell^n] \circ \lambda$ implies that

$$a_i = \ell^n b_i,$$

and hence

$$\alpha_i \equiv 0 \pmod{\ell^n}.$$

This holds for all n, so we conclude that $\alpha_i = 0$, and hence that $\phi = 0$. (N.B. The reason that we need to use M^{div}, rather than working in M, is because it is essential that ϕ, ψ, and λ be written in terms of a $\mathbb{Z}$-basis that does not depend on the choice of ℓ^n.) □

Corollary 7.5. *Let E_1 and E_2 be elliptic curves. Then*

$$\operatorname{Hom}(E_1, E_2)$$

is a free $\mathbb{Z}$-module of rank at most 4.

PROOF. We know from (III.4.2b) that $\operatorname{Hom}(E_1, E_2)$ is torsion-free. This implies that

$$\operatorname{rank}_{\mathbb{Z}} \operatorname{Hom}(E_1, E_2) = \operatorname{rank}_{\mathbb{Z}_\ell} \operatorname{Hom}(E_1, E_2) \otimes \mathbb{Z}_\ell,$$

in the sense that if one is finite, then the other is finite and they are equal. Next, from (III.7.4) we have the estimate

$$\operatorname{rank}_{\mathbb{Z}_\ell} \operatorname{Hom}(E_1, E_2) \otimes \mathbb{Z}_\ell \le \operatorname{rank}_{\mathbb{Z}_\ell} \operatorname{Hom}\bigl(T_\ell(E_1), T_\ell(E_2)\bigr).$$

Finally, choosing a $\mathbb{Z}_\ell$-basis for $T_\ell(E_1)$ and $T_\ell(E_2)$, we see from (III.7.1a) that

$$\operatorname{Hom}\bigl(T_\ell(E_1), T_\ell(E_2)\bigr) = M_2(\mathbb{Z}_\ell)$$

is the additive group of 2×2 matrices with $\mathbb{Z}_\ell$-coefficients. The $\mathbb{Z}_\ell$-rank of $M_2(\mathbb{Z}_\ell)$ is 4, which proves that $\operatorname{rank}_{\mathbb{Z}} \operatorname{Hom}(E_1, E_2)$ is at most 4. □

Remark 7.6. By definition, an isogeny is defined over K if it commutes with the action of $G_{\bar{K}/K}$. Similarly, we can define

$$\operatorname{Hom}_K\bigl(T_\ell(E_1), T_\ell(E_2)\bigr)$$

to be the group of $\mathbb{Z}_\ell$-linear maps from $T_\ell(E_1)$ to $T_\ell(E_2)$ that commute with the action of $G_{\bar{K}/K}$ as given by the ℓ-adic representation. Then we have a homomorphism

$$\operatorname{Hom}_K(E_1, E_2) \otimes \mathbb{Z}_\ell \longrightarrow \operatorname{Hom}_K\bigl(T_\ell(E_1), T_\ell(E_2)\bigr),$$

and (III.7.4) tells us that this homomorphism is injective. It turns out that in many cases, it is an isomorphism.

Isogeny Theorem 7.7. *Let $\ell \ne \operatorname{char}(K)$ be a prime. The natural map*

$$\operatorname{Hom}_K(E_1, E_2) \otimes \mathbb{Z}_\ell \longrightarrow \operatorname{Hom}_K\bigl(T_\ell(E_1), T_\ell(E_2)\bigr)$$

is an isomorphism in the following two situations:

(a) *K is a finite field.* (Tate [282])
(b) *K is a number field.* (Faltings [82, 84])

The original proofs of both parts of (III.7.7) make heavy use of abelian varieties (higher-dimensional analogues of elliptic curves) and are thus unfortunately beyond the scope of this book. Indeed, the methods used to prove (III.7.7b) include virtually all of the tools needed for Faltings' proof of the Mordell conjecture. See also [237] for a proof of (III.7.7b) in the case that $j(E)$ is nonintegral, and [45, 160, 163] for alternative proofs of (III.7.7b).

One way to interpret (III.7.7) is to view the Tate modules as homology groups, specifically as the first homology with $\mathbb{Z}_\ell$-coefficients (III.7.3.1). Then (III.7.7) characterizes when a map between homology groups comes from an actual geometric map between the curves.

Remark 7.8. It is also natural to ask about the size of the image of $\rho_\ell(G_{\bar{K}/K})$ in $\mathrm{Aut}\bigl(T_\ell(E)\bigr)$. The following theorem of Serre provides an answer for number fields. We do not include the proof. (But see (IX.6.3) and Exercise 9.7.)

Theorem 7.9. (Serre) *Let K be a number field and let E/K be an elliptic curve without complex multiplication.*
(a) *$\rho_\ell(G_{\bar{K}/K})$ is of finite index in $\mathrm{Aut}\bigl(T_\ell(E)\bigr)$ for all primes ℓ.*
(b) *$\rho_\ell(G_{\bar{K}/K}) = \mathrm{Aut}\bigl(T_\ell(E)\bigr)$ for all but finitely many primes ℓ.*

PROOF. See [237] and [231]. □

Remark 7.10. Let E/K be an elliptic curve. Then the elements of $\mathrm{End}_K(E)$ commute with the elements of $G_{\bar{K}/K}$ in their action on $T_\ell(E)$. If

$$\mathrm{End}_K(E) = \mathbb{Z},$$

this gives no additional information. However, if E has complex multiplication over K, i.e., if $\mathrm{End}_K(E) \neq \mathbb{Z}$, then one can show (Exercise 3.24) that this forces the action of $G_{\bar{K}/K}$ on $T_\ell(E)$ to be abelian, i.e., the image $\rho_\ell(G_{\bar{K}/K})$ is an abelian subgroup of $\mathrm{Aut}\bigl(T_\ell(E)\bigr) \cong \mathrm{GL}_2(\mathbb{Z}_\ell)$. In particular, adjoining the coordinates of ℓ^n-torsion points to K leads to explicitly constructed abelian extensions of K, in much the same way that abelian extensions of $\mathbb{Q}$ are obtained by adjoining roots of unity. See (C §11) for a brief discussion, and [140, Part II], [249, Chapter 5], or [266, Chapter II] for further details.

III.8 The Weil Pairing

Let E/K be an elliptic curve. For this section we fix an integer $m \geq 2$, which we assume to be prime to $p = \mathrm{char}(K)$ if $p > 0$.

As an abstract group, the group of m-torsion points $E[m]$ has the form (III.6.4b)

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

Thus $E[m]$ is a free $\mathbb{Z}/m\mathbb{Z}$-module of rank two. We can define a nondegenerate alternating multilinear map on $E[m]$ by fixing a basis $\{T_1, T_2\}$ and setting

$$\det : E[m] \times E[m] \longrightarrow \mathbb{Z}/m\mathbb{Z}, \qquad \det(aT_1 + bT_2, cT_1 + dT_2) = ad - bc.$$

However, there are two drawbacks to this approach. First, the value of the determinant depends on the choice of basis. But this is not so bad, since selecting a new basis simply multplies all of the values by an element of $(\mathbb{Z}/m\mathbb{Z})^*$. Second, and more serious, is that this determinant pairing on $E[m]$ is not Galois invariant, i.e., if $P, Q \in E[m]$ and $\sigma \in G_{\bar{K}/K}$, then the values of $\det(P^\sigma, Q^\sigma)$ and $\det(P, Q)^\sigma$ need not be the same.

We can simultaneously achieve basis independent and Galois invariance by using instead a modified pairing taking values in the group of m^{th} roots of unity. In order to define this pairing, we will make frequent use of (III.3.5), which says that a divisor $\sum n_i(P_i)$ is the divisor of a function if and only if both $\sum n_i = 0$ and $\sum [n_i]P_i = O$.

Let $T \in E[m]$. Then there is a function $f \in \bar{K}(E)$ satisfying

$$\operatorname{div}(f) = m(T) - m(O).$$

Next take $T' \in E$ to be a point with $[m]T' = T$. Then there is similarly a function $g \in \bar{K}(E)$ satisfying

$$\operatorname{div}(g) = [m]^*(T) - [m]^*(O) = \sum_{R \in E[m]} \big((T' + R) - (R)\big).$$

(To see that this divisor sums to O, we observe that $\#E[m] = m^2$ from (III.6.4b) and that $[m^2]T' = O$.) It is easy to verify that the functions $f \circ [m]$ and g^m have the same divisor, so multiplying f by an appropriate constant from $\bar{K}^*$, we may assume that

$$f \circ [m] = g^m.$$

Now let $S \in E[m]$ also be an m-torsion point, where we allow $S = T$. Then for any point $X \in E$, we have

$$g(X + S)^m = f\big([m]X + [m]S\big) = f\big([m]X\big) = g(X)^m.$$

Thus considered as a function of X, the function $g(X + S)/g(X)$ takes on only finitely many values, i.e., for every X, it is an m^{th} root of unity. In particular, the morphism

$$E \longrightarrow \mathbb{P}^1, \qquad X \longmapsto g(X + S)/g(X)$$

is not surjective, so (II.2.3) says that it is constant. This allows us to define a pairing

$$e_m : E[m] \times E[m] \longrightarrow \boldsymbol{\mu}_m$$

by setting

$$e_m(S, T) = \frac{g(X + S)}{g(X)},$$

where $X \in E$ is any point such that $g(X+S)$ and $g(X)$ are both defined and nonzero. (As usual, $\boldsymbol{\mu}_m$ denotes the group of m^{th} roots of unity.) Note that although the function g is well-defined only up to multiplication by an element of $\bar{K}^*$, the value of $e_m(S,T)$ does not depend on this choice. The pairing that we have just defined is called the *Weil e_m-pairing*. We begin by proving some of its basic properties.

Proposition 8.1. *The Weil e_m-pairing has the following properties*:
(a) *It is* bilinear:

$$e_m(S_1+S_2,T) = e_m(S_1,T)e_m(S_2,T),$$
$$e_m(S,T_1+T_2) = e_m(S,T_1)e_m(S,T_2).$$

(b) *It is* alternating:

$$e_m(T,T) = 1.$$

So in particular, $e_m(S,T) = e_m(T,S)^{-1}$.
(c) *It is* nondegenerate:

$$\textit{If } e_m(S,T) = 1 \textit{ for all } S \in E[m], \textit{ then } T = O.$$

(d) *It is* Galois invariant:

$$e_m(S,T)^\sigma = e_m(S^\sigma, T^\sigma) \qquad \textit{for all } \sigma \in G_{\bar{K}/K}.$$

(e) *It is* compatible:

$$e_{mm'}(S,T) = e_m\big([m']S,T\big) \qquad \textit{for all } S \in E[mm'] \textit{ and } T \in E[m].$$

PROOF. (a) Linearity in the first factor is easy:

$$\begin{aligned} e_m(S_1+S_2,T) &= \frac{g(X+S_1+S_2)}{g(X)} = \frac{g(X+S_1+S_2)}{g(X+S_1)}\,\frac{g(X+S_1)}{g(X)} \\ &= e_m(S_2,T)e_m(S_1,T). \end{aligned}$$

Note how useful it is that in computing $e_m(S_2,T) = g(Y+S_2)/g(Y)$, we may choose any value for Y, for example we may take $Y = X+S_1$.

In order to prove linearity in the second factor, let $f_1, f_2, f_3, g_1, g_2, g_3$ be the appropriate functions for the points T_1, T_2, and $T_3 = T_1+T_2$. Choose a function $h \in \bar{K}(E)$ with divisor

$$\operatorname{div}(h) = (T_1+T_2) - (T_1) - (T_2) + (O).$$

Then

$$\operatorname{div}\left(\frac{f_3}{f_1 f_2}\right) = m\operatorname{div}(h),$$

so

$$f_3 = c f_1 f_2 h^m \qquad \text{for some } c \in \bar{K}^*.$$

We compose with the multiplication-by-m map, use the fact that $f_i \circ [m] = g_i^m$, and take m^{th} roots to obtain

$$g_3 = c' \cdot g_1 \cdot g_2 \cdot \bigl(h \circ [m]\bigr) \qquad \text{for some } c' \in \bar{K}^*.$$

This allows us to compute

$$\begin{aligned} e_m(S, T_1 + T_2) &= \frac{g_3(X+S)}{g_3(X)} = \frac{g_1(X+S)g_2(X+S)h\bigl([m]X + [m]S\bigr)}{g_1(X)g_2(X)h\bigl([m]X\bigr)} \\ &= e_m(S,T_1)e_m(S,T_2), \qquad \text{since } [m]S = O. \end{aligned}$$

(b) From (a) we have

$$e_m(S+T, S+T) = e_m(S,S)e_m(S,T)e_m(T,S)e_m(T,T),$$

so it suffices to show that $e_m(T,T) = 1$ for all $T \in E[m]$. For any $P \in E$, recall that $\tau_P : E \to E$ denotes the translation-by-P map (III.4.7). We compute

$$\operatorname{div}\left(\prod_{i=0}^{m-1} f \circ \tau_{[i]T}\right) = m \sum_{i=0}^{m-1} \Bigl(\bigl([1-i]T\bigr) - \bigl([-i]T\bigr)\Bigr) = 0.$$

It follows that

$$\prod_{i=0}^{m-1} f \circ \tau_{[i]T}$$

is constant, and if we choose some $T' \in E$ satisfying $[m]T' = T$, then

$$\prod_{i=0}^{m-1} g \circ \tau_{[i]T'}$$

is also constant, because its m^{th} power is the above product of f's. Therefore the product of the g's takes on the same value at X and at $X + T'$,

$$\prod_{i=0}^{m-1} g\bigl(X + [i]T'\bigr) = \prod_{i=0}^{m-1} g\bigl(X + [i+1]T'\bigr).$$

Canceling like terms from each side gives

$$g(X) = g\bigl(X + [m]T'\bigr) = g(X+T),$$

and hence

$$e_m(T,T) = \frac{g(X+T)}{g(X)} = 1.$$

(c) If $e_m(S,T) = 1$ for all $S \in E[m]$, then $g(X+S) = g(X)$ for all $S \in E[m]$, so (III.4.10b) tells us that $g = h \circ [m]$ for some function $h \in \bar{K}(E)$. But then

$$\big(h\circ[m]\big)^m = g^m = f\circ[m],$$

which implies that $f = h^m$. Hence

$$m\,\mathrm{div}(h) = \mathrm{div}(f) = m(T) - m(O),$$

so

$$\mathrm{div}(h) = (T) - (O).$$

It follows from (III.3.3) that $T = O$.
(d) Let $\sigma \in G_{\bar{K}/K}$. If f and g are the functions for T as above, then clearly f^σ and g^σ are the corresponding functions for T^σ. Then

$$e_m(S^\sigma, T^\sigma) = \frac{g^\sigma(X^\sigma + S^\sigma)}{g^\sigma(X^\sigma)} = \left(\frac{g(X+S)}{g(X)}\right)^\sigma = e_m(S,T)^\sigma.$$

(e) Taking f and g as usual, we have

$$\mathrm{div}(f^{m'}) = mm'(T) - mm'(O)$$

and

$$\big(g\circ[m']\big)^{mm'} = \big(f\circ[mm']\big)^{m'}.$$

Then directly from the definition of $e_{mm'}$ and e_m, we compute

$$e_{mm'}(S,T) = \frac{g\circ[m'](X+S)}{g\circ[m'](X)} = \frac{g\big(Y+[m']S\big)}{g(Y)} = e_m\big([m']S,T\big). \qquad \square$$

The basic properties of the Weil pairing imply its surjectivity, as in the next result.

Corollary 8.1.1. *There exist points $S, T \in E[m]$ such that $e_m(S,T)$ is a primitive m^{th} root of unity. In particular, if $E[m] \subset E(K)$, then $\boldsymbol{\mu}_m \subset K^*$.*

PROOF. The image of $e_m(S,T)$ as S and T range over $E[m]$ is a subgroup of $\boldsymbol{\mu}_m$, say equal to $\boldsymbol{\mu}_d$. It follows that

$$1 = e_m(S,T)^d = e_m\big([d]S,T\big) \qquad \text{for all } S,T \in E[m].$$

The nondegeneracy of the e_m-pairing implies that $[d]S = O$, and since S is arbitrary, it follows from (III.6.4) that $d = m$. Finally, if $E[m] \subset E(K)$, then the Galois invariance of the e_m-pairing implies that $e_m(S,T) \in K^*$ for all $S,T \in E[m]$. Hence $\boldsymbol{\mu}_m \subset K^*$. $\square$

Recall from (III §6) that associated to any isogeny $\phi : E_1 \to E_2$ is a dual isogeny $\hat{\phi} : E_2 \to E_1$ going in the opposite direction. The next proposition says that ϕ and $\hat{\phi}$ are dual (or adjoint) with respect to the Weil pairing.

Proposition 8.2. *Let $\phi : E_1 \to E_2$ be an isogeny of elliptic curves. Then for all m-torsion points $S \in E_1[m]$ and $T \in E_2[m]$,*

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

PROOF. Let

$$\operatorname{div}(f) = m(T) - m(O) \qquad \text{and} \qquad f \circ [m] = g^m$$

be as usual. Then

$$e_m(\phi S, T) = \frac{g(X + \phi S)}{g(X)}.$$

Choose a function $h \in \bar{K}(E_1)$ satisfying

$$\phi^*\big((T)\big) - \phi^*\big((O)\big) = (\hat{\phi}T) - (O) + \operatorname{div}(h).$$

Such an h exists because ((III.6.1ab) tells us that $\hat{\phi}T$ is precisely the sum of the points of the divisor on the left-hand side of this equality. Now we observe that

$$\operatorname{div}\left(\frac{f \circ \phi}{h^m}\right) = \phi^* \operatorname{div}(f) - m \operatorname{div}(h) = m(\hat{\phi}T) - m(O)$$

and

$$\left(\frac{g \circ \phi}{h \circ [m]}\right)^m = \frac{f \circ [m] \circ \phi}{\big(h \circ [m]\big)^m} = \left(\frac{f \circ \phi}{h^m}\right) \circ [m].$$

Then directly from the definition of the e_m-pairing we obtain

$$\begin{aligned} e_m(S, \hat{\phi}T) &= \frac{\big(g \circ \phi / h \circ [m]\big)(X + S)}{\big(g \circ \phi / h \circ [m]\big)(X)} \\ &= \frac{g(\phi X + \phi S)}{g(\phi X)} \cdot \frac{h\big([m]X\big)}{h\big([m]X + [m]S\big)} \\ &= e_m(\phi S, T). \end{aligned}$$

□

Let ℓ be a prime number different from $\operatorname{char}(K)$. We are going to combine the pairings

$$e_{\ell^n} : E[\ell^n] \times E[\ell^n] \longrightarrow \boldsymbol{\mu}_{\ell^n}$$

for $n = 1, 2, \ldots$ in order to create an *ℓ-adic Weil pairing* on the Tate module,

$$e : T_\ell(E) \times T_\ell(E) \longrightarrow T_\ell(\boldsymbol{\mu}).$$

Recall that the inverse limits for $T_\ell(E)$ and $T_\ell(\boldsymbol{\mu})$ are formed using the maps

$$E[\ell^{n+1}] \xrightarrow{[\ell]} E[\ell^n] \qquad \text{and} \qquad \boldsymbol{\mu}_{\ell^{n+1}} \xrightarrow{\zeta \mapsto \zeta^\ell} \boldsymbol{\mu}_{\ell^n}.$$

Thus in order to show that the e_{ℓ^n}-pairings are compatible with taking the inverse limits, we must show that

$$e_{\ell^{n+1}}(S,T)^{\ell} = e_{\ell^n}\big([\ell]S,[\ell]T\big) \qquad \text{for all } S,T \in E[\ell^{n+1}].$$

We use linearity (III.8.1a) to observe that

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

and then the desired compatibility relation follows by applying (III.8.1e) to the points S and $[\ell]T$ with $m = \ell^n$ and $m' = \ell$. This proves that the pairing $e : T_\ell(E) \times T_\ell(E) \to T_\ell(\boldsymbol{\mu})$ is well-defined. Further, it inherits all of the properties described in (III.8.1) and (III.8.2), which completes the proof of the following result.

Proposition 8.3. *There exists a bilinear, alternating, nondegenerate, Galois invariant pairing*

$$e : T_\ell(E) \times T_\ell(E) \longrightarrow T_\ell(\boldsymbol{\mu}).$$

Further, if $\phi : E_1 \to E_2$ is an isogeny, then ϕ and its dual $\hat\phi$ are adjoints for the pairing, i.e., $e(\phi S,T) = e(S,\hat\phi T)$.

Remark 8.4. More generally, if $\phi : E_1 \to E_2$ is any nonconstant isogeny, then there is a Weil pairing

$$e_\phi : \ker\phi \times \ker\hat\phi \longrightarrow \boldsymbol{\mu}_m.$$

See Exercise 3.15.

Remark 8.5. There is an alternative definition of the Weil pairing $e_m(S,T)$ that works as follows. Choose arbitrary points $X,Y \in E$ and functions $f_S, f_T \in \bar K(E)$ satisfying

$$\operatorname{div}(f_S) = m(X+S) - m(X) \qquad \text{and} \qquad \operatorname{div}(f_T) = m(Y+T) - m(Y).$$

Then

$$e_m(S,T) = \frac{f_S(Y+T)}{f_S(Y)} \Big/ \frac{f_T(X+S)}{f_T(X)}.$$

We leave to the reader to prove that this quantity is well-defined and equal to the Weil pairing; see Exercise 3.16.

Recall that we have a representation (III §7)

$$\operatorname{End}(E) \longrightarrow \operatorname{End}\big(T_\ell(E)\big), \qquad \phi \longmapsto \phi_\ell.$$

Choosing a $\mathbb{Z}_\ell$-basis for $T_\ell(E)$, we can write ϕ_ℓ as a 2×2 matrix, and in particular we can compute

$$\det(\phi_\ell) \in \mathbb{Z}_\ell \quad \text{and} \quad \operatorname{tr}(\phi_\ell) \in \mathbb{Z}_\ell.$$

Of course, the value of the determinant and trace do not depend on the choice of basis.

The next result, whose proof uses the Weil pairing, shows how the determinant and trace values may be employed to compute the degree of an isogeny. These formulas are applied in Chapter V to count the number of points on an elliptic curve defined over a finite field (V.2.3.1). If we view the Tate module as a homology group (III.7.3.1), then (III.8.6) says that the degree of an isogeny can be computed topologically via its action on $H_1(E, \mathbb{Z}_\ell)$.

Proposition 8.6. *Let $\phi \in \mathrm{End}(E)$, and let $\phi_\ell : T_\ell(E) \to T_\ell(E)$ be the map that ϕ induces on the Tate module of E. Then*

$$\det(\phi_\ell) = \deg(\phi) \qquad \textit{and} \qquad \mathrm{tr}(\phi_\ell) = 1 + \deg(\phi) - \deg(1-\phi).$$

In particular, $\det(\phi_\ell)$ *and* $\mathrm{tr}(\phi_\ell)$ *are in* $\mathbb{Z}$ *and are independent of* ℓ.

PROOF. Let $\{v_1, v_2\}$ be a $\mathbb{Z}_\ell$-basis for $T_\ell(E)$ and write

$$\phi_\ell(v_1) = av_1 + bv_2, \qquad \phi_\ell(v_2) = cv_1 + dv_2,$$

so the matrix of ϕ_ℓ relative to this basis is

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

Using properties of the Weil pairing (III.8.3), we compute

$$\begin{aligned}
e(v_1,v_2)^{\deg\phi} &= e\big([\deg\phi]v_1, v_2\big) && \text{bilinearity of } e,\\
&= e(\hat{\phi}_\ell\phi_\ell v_1, v_2) && \text{(III.6.1a)},\\
&= e(\phi_\ell v_1, \phi_\ell v_2) && \text{(III.8.3) and (III.6.2f)},\\
&= e(av_1 + bv_2, cv_1 + dv_2)\\
&= e(v_1,v_2)^{ad-bc} && \text{since } e \text{ is bilinear and alternating},\\
&= e(v_1,v_2)^{\det\phi_\ell}.
\end{aligned}$$

Since e is nondegenerate, we conclude that $\deg\phi = \det\phi_\ell$. Finally, for any 2×2 matrix A, a trivial calculation yields

$$\mathrm{tr}(A) = 1 + \det(A) - \det(1-A). \qquad \square$$

III.9 The Endomorphism Ring

Let E be an elliptic curve. In this section we characterize which rings may occur as the endomorphism ring of E. So far we have accumulated the following information:

(i) $\mathrm{End}(E)$ has characteristic 0, no zero divisors, and rank at most four as a $\mathbb{Z}$-module (III.4.2c), (III.7.5).

(ii) $\mathrm{End}(E)$ possesses an anti-involution $\phi \mapsto \hat{\phi}$ (III.6.2bcf).

(iii) For $\phi \in \mathrm{End}(E)$, the product $\phi\hat{\phi}$ is a non-negative integer, and further, $\phi\hat{\phi} = 0$ if and only if $\phi = 0$ (III.6.2a), (III.6.3).

It turns out that any ring satisfying (i)–(iii) is of a very special sort. After giving the relevant definitions, we describe the general classification of rings satisfying (i)–(iii). This may then be applied to the particular case of $\mathrm{End}(E)$.

Definition. Let $\mathcal{K}$ be a (not necessarily commutative) $\mathbb{Q}$-algebra that is finitely generated over $\mathbb{Q}$. An *order* $\mathcal{R}$ of $\mathcal{K}$ is a subring of $\mathcal{K}$ that is finitely generated as a $\mathbb{Z}$-module and satisfies $\mathcal{R} \otimes \mathbb{Q} = \mathcal{K}$.

Example 9.1. Let $\mathcal{K}$ be an imaginary quadratic field and let $\mathcal{O}$ be its ring of integers. Then for each integer $f \geq 1$, the ring $\mathbb{Z} + f\mathcal{O}$ is an order of $\mathcal{K}$. In fact, these are all of the orders of $\mathcal{K}$; see Exercise 3.20.

Definition. A *quaternion algebra* is an algebra of the form

$$\mathcal{K} = \mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\beta + \mathbb{Q}\alpha\beta$$

whose multiplication satisfies

$$\alpha^2, \beta^2 \in \mathbb{Q}, \qquad \alpha^2 < 0, \qquad \beta^2 < 0, \qquad \beta\alpha = -\alpha\beta.$$

Remark 9.2. These quaternion algebras are more properly called *definite quaternion algebras over* $\mathbb{Q}$, but since these are the only quaternion algebras that we use in this book, we generally drop the "definite" appellation.

Theorem 9.3. *Let $\mathcal{R}$ be a ring of characteristic 0 having no zero divisors, and assume that $\mathcal{R}$ has the following properties*:
(i) *$\mathcal{R}$ has rank at most four as a $\mathbb{Z}$-module.*
(ii) *$\mathcal{R}$ has an anti-involution $\alpha \mapsto \hat{\alpha}$ satisfying*

$$\widehat{\alpha+\beta} = \hat{\alpha} + \hat{\beta}, \qquad \widehat{\alpha\beta} = \hat{\beta}\hat{\alpha}, \qquad \hat{\hat{\alpha}} = \alpha, \qquad \hat{a} = a \quad \text{for } a \in \mathbb{Z} \subset \mathcal{R}.$$

(iii) *For $\alpha \in \mathcal{R}$, the product $\alpha\hat{\alpha}$ is a nonnegative integer, and $\alpha\hat{\alpha} = 0$ if and only if $\alpha = 0$.*
Then $\mathcal{R}$ is one of the following types of rings:
(a) *$\mathcal{R} \cong \mathbb{Z}$.*
(b) *$\mathcal{R}$ is an order in an imaginary quadratic extension of $\mathbb{Q}$.*
(c) *$\mathcal{R}$ is an order in a quaternion algebra over $\mathbb{Q}$.*

PROOF. Let $\mathcal{K} = \mathcal{R} \otimes \mathbb{Q}$. Since $\mathcal{R}$ is finitely generated as a $\mathbb{Z}$-module, it suffices to prove that $\mathcal{K}$ is either $\mathbb{Q}$, an imaginary quadratic field, or a quaternion algebra. We extend the anti-involution to $\mathcal{K}$ and define a (reduced) *norm* and *trace* from $\mathcal{K}$ to $\mathbb{Q}$ by

$$\mathrm{N}\alpha = \alpha\hat{\alpha} \qquad \text{and} \qquad \mathrm{T}\alpha = \alpha + \hat{\alpha}.$$

We make several observations about the trace. First, since

$$\mathrm{T}\alpha = 1 + \mathrm{N}\alpha - \mathrm{N}(\alpha - 1),$$

we see that $\mathrm{T}\alpha \in \mathbb{Q}$. Second, the trace is $\mathbb{Q}$-linear, since the involution fixes $\mathbb{Q}$. Third, if $\alpha \in \mathbb{Q}$, then $\mathrm{T}\alpha = 2\alpha$. Finally, if $\alpha \in \mathcal{K}$ satisfies $\mathrm{T}\alpha = 0$, then

$$0 = (\alpha - \alpha)(\alpha - \hat{\alpha}) = \alpha^2 - (\mathrm{T}\alpha)\alpha + \mathrm{N}\alpha = \alpha^2 + \mathrm{N}\alpha,$$

so $\alpha^2 = -\mathrm{N}\alpha$. Thus

$$\alpha \neq 0 \quad \text{and} \quad \mathrm{T}\alpha = 0 \quad \Longrightarrow \quad \alpha^2 \in \mathbb{Q} \quad \text{and} \quad \alpha^2 < 0.$$

If $\mathcal{K} = \mathbb{Q}$, there is nothing to prove. Otherwise we can find some $\alpha \in \mathcal{K}$ with $\alpha \notin \mathbb{Q}$. Replacing α by $\alpha - \frac{1}{2}\mathrm{T}\alpha$, we may assume that $\mathrm{T}\alpha = 0$. Then $\alpha^2 \in \mathbb{Q}$ and $\alpha^2 < 0$, so $\mathbb{Q}(\alpha)$ is a quadratic imaginary field. If $\mathcal{K} = \mathbb{Q}(\alpha)$, we are again done.

Suppose now that $\mathcal{K} \neq \mathbb{Q}(\alpha)$ and choose some $\beta \in \mathcal{K}$ with $\beta \notin \mathbb{Q}(\alpha)$. We may replace β with

$$\beta - \frac{1}{2}\,\mathrm{T}\beta - \frac{\mathrm{T}(\alpha\beta)}{2\alpha^2}\alpha.$$

We know that $\mathrm{T}\alpha = 0$ and $\alpha^2 \in \mathbb{Q}^*$, so an easy calculation shows that

$$\mathrm{T}\beta = \mathrm{T}(\alpha\beta) = 0.$$

In particular, $\beta^2 \in \mathbb{Q}$ and $\beta^2 < 0$. We next write

$$\mathrm{T}\alpha = 0, \quad \mathrm{T}\beta = 0, \quad \mathrm{T}(\alpha\beta) = 0$$

as

$$\alpha = -\hat{\alpha}, \quad \beta = -\hat{\beta}, \quad \alpha\beta = -\hat{\beta}\hat{\alpha}$$

and substitute the first two equalities into the third to obtain

$$\alpha\beta = -\beta\alpha.$$

Hence

$$\mathbb{Q}[\alpha, \beta] = \mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\beta + \mathbb{Q}\alpha\beta$$

is a quaternion algebra. It remains to prove that $\mathbb{Q}[\alpha, \beta] = \mathcal{K}$, and to do this, it suffices to show that $1, \alpha, \beta, \alpha\beta$ are $\mathbb{Q}$-linearly independent, since then $\mathbb{Q}[\alpha, \beta]$ and $\mathcal{K}$ both have dimension 4 over $\mathbb{Q}$.

Suppose that

$$w + x\alpha + y\beta + z\alpha\beta = 0 \qquad \text{with } w, x, y, z \in \mathbb{Q}.$$

Taking the trace yields

$$2w = 0, \quad \text{so} \quad w = 0.$$

Next we multiply by α on the left and by β on the right to obtain

$$(x\alpha^2)\beta + (y\beta^2)\alpha + z\alpha^2\beta^2 = 0.$$

We know that 1, α, and β are $\mathbb{Q}$-linearly independent, since $\alpha \notin \mathbb{Q}$ and $\beta \notin \mathbb{Q}(\alpha)$. Hence this equation implies that

$$x\alpha^2 = y\beta^2 = z\alpha^2\beta^2 = 0,$$

and so $x = y = z = 0$, which completes the proof that 1, α, β, and $\alpha\beta$ are $\mathbb{Q}$-linearly independent. (We have used several times the fact that α^2 and β^2 are in $\mathbb{Q}^*$.) □

Corollary 9.4. *The endomorphism ring of an elliptic curve E/K is either $\mathbb{Z}$, an order in an imaginary quadratic field, or an order in a quaternion algebra. If $\operatorname{char}(K) = 0$, then only the first two are possible.*

PROOF. We have proven in (III.4.2b), (III.6.2), and (III.6.3) all of the facts needed to apply (III.9.3) to the ring $\operatorname{End}(E)$. This proves the first part of the corollary. If $\operatorname{char}(K) = 0$, then (III.5.6c) says that $\operatorname{End}(E)$ is commutative, so in this case $\operatorname{End}(E)$ cannot be an order in a quaternion algebra. (See also Exercise 3.33 for a proof of this corollary that does not require knowing a priori that $\operatorname{End}(E)$ has rank at most four.) □

Remark 9.4.1. If $\operatorname{char}(K) = 0$, then (III.5.6c) tells us that $\operatorname{End}(E) \otimes \mathbb{Q}$ is commutative, so it cannot be a quaternion algebra. (For alternative proofs of this important fact, see (VI.6.1b) and Exercise 3.18b.) On the other hand, if K is a finite field $\mathbb{F}_q$, then we will later see that $\operatorname{End}(E)$ is always larger than $\mathbb{Z}$ (V.3.1) and that there are always elliptic curves defined over $\mathbb{F}_{p^2}$ with $\operatorname{End}(E) \otimes \mathbb{Q}$ a quaternion algebra (V.4.1c). The complete description of $\operatorname{End}(E)$ is given in Deuring's comprehensive article [60].

The next definition and theorem are used in the exercises.

Definition. Let p be a prime or ∞, let $\mathbb{Q}_p$ be the p-adic rationals if p is finite, and let $\mathbb{Q}_\infty = \mathbb{R}$. A quaternion algebra $\mathcal{K}$ is said to *split at p* if

$$\mathcal{K} \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong M_2(\mathbb{Q}_p),$$

where $M_2(K)$ is the algebra of 2×2 matrices with coefficients in K. Otherwise $\mathcal{K}$ is said to be *ramified at p*. The *invariant of $\mathcal{K}$ at p* is defined by

$$\operatorname{inv}_p \mathcal{K} = \begin{cases} 0 & \text{if } \mathcal{K} \text{ splits at } p, \\ \frac{1}{2} & \text{if } \mathcal{K} \text{ ramifies at } p. \end{cases}$$

Theorem 9.5. *Let $\mathcal{K}$ be a quaternion algebra.*
(a) *We have $\operatorname{inv}_p(\mathcal{K}) = 0$ for all but finitely many p, and*

$$\sum_p \operatorname{inv}_p(\mathcal{K}) \in \mathbb{Z}.$$

(*Note that the sum includes $p = \infty$.*)

(b) *Two quaternion algebras $\mathcal{K}$ and $\mathcal{K}'$ are isomorphic as $\mathbb{Q}$-algebras if and only if $\operatorname{inv}_p(\mathcal{K}) = \operatorname{inv}_p(\mathcal{K}')$ for all p.*

PROOF. This is a very special case of the fact that the central simple algebras over a field K are classified by the Brauer group $\operatorname{Br}(K) = H^2(G_{\bar{K}/K}, \bar{K}^*)$ [233, X §5], and the fundamental exact sequence from class field theory [288, §9.6]

$$0 \longrightarrow \operatorname{Br}(\mathbb{Q}) \longrightarrow \bigoplus_p \operatorname{Br}(\mathbb{Q}_p) \xrightarrow{\sum_p \operatorname{inv}_p} \frac{\mathbb{Q}}{\mathbb{Z}} \longrightarrow 0,$$

where

$$\operatorname{Br}(\mathbb{Q}_p) \xrightarrow[\operatorname{inv}_p]{\sim} \begin{cases} \mathbb{Q}/\mathbb{Z} & \text{if } p \neq \infty, \\ \{0, \frac{1}{2}\} & \text{if } p = \infty. \end{cases}$$

Quaternion algebras (definite and indefinite) correspond to elements of order 2 in $\operatorname{Br}(\mathbb{Q})$. □

III.10 The Automorphism Group

If an elliptic curve is given by a Weierstrass equation, it is generally a nontrivial matter to determine the exact structure of its endomorphism ring. The situation is much simpler for the automorphism group.

Theorem 10.1. *Let E/K be an elliptic curve. Then its automorphism group $\operatorname{Aut}(E)$ is a finite group of order dividing 24. More precisely, the order of $\operatorname{Aut}(E)$ is given by the following table*:

$\#\operatorname{Aut}(E)$	$j(E)$	$\operatorname{char}(K)$
2	$j(E) \neq 0, 1728$	—
4	$j(E) = 1728$	$\operatorname{char}(K) \neq 2, 3$
6	$j(E) = 0$	$\operatorname{char}(K) \neq 2, 3$
12	$j(E) = 0 = 1728$	$\operatorname{char}(K) = 3$
24	$j(E) = 0 = 1728$	$\operatorname{char}(K) = 2$

PROOF. We restrict attention to $\operatorname{char}(K) \neq 2, 3$; see (III.1.3) and (A.1.2c). Then E is given by an equation

$$E : y^2 = x^3 + Ax + B,$$

and every automorphism of E has the form

$$x = u^2 x', \qquad y = u^3 y',$$

for some $u \in \bar{K}^*$. Such a substitution gives an automorphism of E if and only if

$$u^{-4} A = A \qquad \text{and} \qquad u^{-6} B = B.$$

If $AB \neq 0$, i.e., if $j(E) \neq 0, 1728$, then the only possibilities are $u = \pm 1$. Similarly, if $B = 0$, then $j(E) = 1728$ and $u^4 = 1$, and if $A = 0$, then $j(E) = 0$ and $u^6 = 1$. Hence $\operatorname{Aut}(E)$ is cyclic of order 2, 4, or 6, depending on whether $AB \neq 0$, $B = 0$, or $A = 0$. □

It is worth remarking that the proof of (III.10.1) gives the structure of $\mathrm{Aut}(E)$ as a $G_{\bar{K}/K}$-module, at least for $\mathrm{char}(K) \neq 2, 3$. We record this as a corollary.

Corollary 10.2. *Let E/K be a curve over a field of characteristic not equal to 2 or 3, and let*

$$n = \begin{cases} 2 & \text{if } j(E) \neq 0, 1728, \\ 4 & \text{if } j(E) = 1728, \\ 6 & \text{if } j(E) = 0. \end{cases}$$

Then there is a natural isomorphism of $G_{\bar{K}/K}$-modules

$$\mathrm{Aut}(E) \cong \boldsymbol{\mu}_n.$$

PROOF. While proving (III.10.1), we showed that the map

$$[\ \ ] : \boldsymbol{\mu}_n \longrightarrow E, \qquad [\zeta](x, y) = (\zeta^2 x, \zeta^3 y),$$

is an isomorphism of abstract groups. It is clear that this map commutes with the action of $G_{\bar{K}/K}$, and hence it is an isomorphism of $G_{\bar{K}/K}$-modules. □

Exercises

3.1. Show that the polynomials

$$x^4 - b_4x^2 - 2b_6x - b_8 \qquad \text{and} \qquad 4x^3 + b_2x^2 + 2b_4x + b_6$$

appearing in the duplication formula (III.2.3d) are relatively prime if and only if the discriminant of the associated Weierstrass equation is nonzero.

3.2. (a) Derive a *triplication formula*, analogous to to the duplication formula (III.2.3), i.e., express $x\big([3]P\big)$ as a rational function of $x(P)$ and $a_1, \ldots, a_6$.

(b) Use the result from (a) to show that if $\mathrm{char}(K) \neq 3$, then E has a nontrivial point of order 3. Conclude that if $\gcd(m, 3) = 1$, then $[m] \neq [0]$. (*Warning*. You'll probably want to use a computer algebra package for this problem.)

3.3. Assume that $\mathrm{char}(K) \neq 3$ and let $A \in K^*$. Then Exercise 2.7 tells us that the curve

$$E : X^3 + Y^3 = AZ^3$$

is a curve of genus one, so together with the point $O = [1, -1, 0]$, it is an elliptic curve.

(a) Prove that three points on E add to O if and only if they are collinear.

(b) Let $P = [X, Y, Z] \in E$. Prove the formulas

$$\begin{aligned} -P &= [Y, X, Z], \\ [2]P &= \big[-Y(X^3 + AZ^3), X(Y^3 + AZ^3), X^3Z - Y^3Z\big]. \end{aligned}$$

(c) Develop an analogous formula for the sum of two distinct points.

(d) Prove that E has j-invariant 0.

3.4. Referring to (III.2.4), express each of the points $P_2, P_4, P_5, P_6, P_7, P_8$ in the form $[m]P_1 + [n]P_3$ with $m, n \in \mathbb{Z}$.

3.5. Let E/K be given by a singular Weierstrass equation.

(a) Suppose that E has a node, and let the tangent lines at the node be

$$y = \alpha_1 x + \beta_1 \qquad \text{and} \qquad y = \alpha_2 x + \beta_2.$$

(i) If $\alpha_1 \in K$, prove that $\alpha_2 \in K$ and

$$E_{\text{ns}}(K) \cong K^*.$$

(ii) If $\alpha_1 \notin K$, prove that $L = K(\alpha_1, \alpha_2)$ is a quadratic extension of K. Note that (i) tells us that $E_{\text{ns}}(K) \subset E_{\text{ns}}(L) \cong L^*$. Prove that

$$E_{\text{ns}}(K) \cong \bigl\{t \in L^* : \mathrm{N}_{L/K}(t) = 1\bigr\}.$$

(b) Suppose that E has a cusp. Prove that

$$E_{\text{ns}}(K) \cong K^+.$$

3.6. Let C be a smooth curve of genus g, let $P_0 \in C$, and let $n \ge 2g+1$ be an integer. Choose a basis $\{f_0, \ldots, f_m\}$ for $\mathcal{L}\bigl(n(P_0)\bigr)$ and define a map

$$\phi : [f_0, \ldots, f_m] : C \longrightarrow \mathbb{P}^m.$$

(a) Prove that the image $C' = \phi(C)$ is a curve in $\mathbb{P}^m$.

(b) Prove that the map $\phi : C \longrightarrow C'$ has degree one.

(c) * Prove that C' is smooth and that $\phi : C \longrightarrow C'$ is an isomorphism.

3.7. This exercise gives an elementary, highly computational, proof that the multiplication-by-m map has degree m^2. Let E be given be the Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

and let b_2, b_4, b_6, b_8 be the usual quantities. (If you're content to work with $\operatorname{char}(K) \neq 2, 3$, you may find it easier to use the short Weierstrass form $E : y^2 = x^3 + Ax + B$.)

We define *division polynomials* $\psi_m \in \mathbb{Z}[a_1, \ldots, a_6, x, y]$ using initial values

$$\begin{aligned}
\psi_1 &= 1,\\
\psi_2 &= 2y + a_1x + a_3,\\
\psi_3 &= 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8,\\
\psi_4 &= \psi_2 \cdot \bigl(2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_6)x + (b_4b_8 - b_6^2)\bigr),
\end{aligned}$$

and then inductively by the formulas

$$\begin{aligned}
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 && \text{for } m \ge 2,\\
\psi_2\psi_{2m} &= \psi_{m-1}^2\psi_m\psi_{m+2} - \psi_{m-2}\psi_m\psi_{m+1}^2 && \text{for } m \ge 3.
\end{aligned}$$

Verify that ψ_m is a polynomial for all $m \ge 1$, and then define further polynomials ϕ_m and ω_m by

$$\begin{aligned}
\phi_m &= x\psi_m^2 - \psi_{m+1}\psi_{m-1},\\
2(2y + a_1x + a_3)\omega_m &= \psi_{m-1}^2\psi_{m+2} + \psi_{m-2}\psi_{m+1}^2.
\end{aligned}$$

(a) Prove that if m is odd, then ψ_m, ϕ_m, and $(2y + a_1x + a_3)^{-1}\omega_m$ are polynomials in

$$\mathbb{Z}\big[a_1, \ldots, a_6, x, (2y + a_1x + a_3)^2\big],$$

and similarly for $(2(2y + a_1x + a_3))^{-1}\psi_m$, ϕ_m, and ω_m if m is even. So replacing $(2y + a_1x + a_3)^2$ by $4x^3 + b_2x^2 + 2b_4x + b_6$, we may treat each of these quantities as a polynomial in $\mathbb{Z}[a_1, \ldots, a_6, x]$.

(b) As polynomials in x, show that

$$\phi_m(x) = x^{m^2} + (\text{lower order terms}),$$
$$\psi_m(x)^2 = m^2 x^{m^2-1} + (\text{lower order terms}).$$

(c) If $\Delta \neq 0$, prove that $\phi_m(x)$ and $\psi_m(x)^2$ are relatively prime polynomials in $K[x]$.

(d) Continuing with the assumption that $\Delta \neq 0$, so E is an elliptic curve, prove that for any point $P = (x_0, y_0) \in E$ we have

$$[m]P = \left(\frac{\phi_m(P)}{\psi_m(P)^2}, \frac{\omega_m(P)}{\psi_m(P)^3}\right).$$

(e) Prove that the map $[m] : E \to E$ has degree m^2.

(f) Prove that the function $\psi_n \in K(E)$ has divisor

$$\operatorname{div}(\psi_n) = \sum_{T \in E[n]} (T) - n^2(O).$$

Thus ψ_n vanishes at precisely the nontrivial n-torsion points and has a corresponding pole at O.

(g) Prove that

$$\psi_{n+m}\psi_{n-m}\psi_r^2 = \psi_{n+r}\psi_{n-r}\psi_m^2 - \psi_{m+r}\psi_{m-r}\psi_n^2 \qquad \text{for all } n > m > r.$$

3.8. (a) Let $E/\mathbb{C}$ be an elliptic curve. We will prove later (VI.5.1.1) that there are a lattice $L \subset \mathbb{C}$ and a complex analytic isomorphism of groups $\mathbb{C}/L \cong E(\mathbb{C})$. (N.B. This isomorphism is given by convergent power series, not by rational functions.) Assuming this fact, prove that

$$\deg[m] = m^2 \qquad \text{and} \qquad E[m] = \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}.$$

(b) Let K be a field with $\operatorname{char}(K) = 0$ and let E/K be an elliptic curve. Use (a) to prove that $\deg[m] = m^2$. (*Hint*. If K can be embedded into $\mathbb{C}$, then the result follows immediately from (a). Reduce to this case.)

3.9. Let E/K be an elliptic curve over a field K with $\operatorname{char}(K) \neq 2, 3$, and fix a a homogeneous Weierstrass equation for E,

$$F(X_0, X_1, X_2) = X_1^2X_2 - X_0^3 - AX_0X_2^2 - BX_2^3 = 0,$$

i.e., $x = X_0/X_2$ and $y = X_1/X_2$ are affine Weierstrass coordinates. Let $P \in E$.

(a) Prove that $[3]P = O$ if and only if the tangent line to E at P intersects E only at P.

(b) Prove that $[3]P = O$ if and only if the Hessian matrix

$$\left(\frac{\partial^2 F}{\partial X_i X_j}(P)\right)_{0\le i,j\le 2}$$

has determinant 0.

(c) Prove that $E[3]$ consists of nine points.

3.10. Let E/K be an elliptic curve with Weierstrass coordinate functions x and y.

(a) Show that the map

$$\phi : E \longrightarrow \mathbb{P}^3, \qquad \phi = [1, x, y, x^2],$$

maps E isomorphically onto the intersection of two quadric surfaces in $\mathbb{P}^3$. (A quadric surface in $\mathbb{P}^3$ is the zero set of a homogeneous polynomial of degree two.) In particular, if $H \subset \mathbb{P}^3$ is a hyperplane, then $H \cap \phi(E)$ consists of exactly four points, counted with appropriate multiplicities.

(b) Show that $\phi(O) = [0, 0, 0, 1]$, and that the hyperplane $\{T_0 = 0\}$ intersects $\phi(E)$ at the single point $\phi(O)$ with multiplicity 4.

(c) Let $P, Q, R, S \in E$. Prove that $P + Q + R + S = O$ if and only if the four points $\phi(P), \phi(Q), \phi(R), \phi(S)$ are coplanar, i.e., if and only if there is a plane $H \subset \mathbb{P}^3$ such that the intersection $E \cap H$, counted with appropriate multiplicities, consists of the points $\phi(P), \phi(Q), \phi(R), \phi(S)$.

(d) Let $P \in E$. Prove that $[4]P = O$ if and only if there exists a hyperplane $H \subset \mathbb{P}^3$ satisfying $H \cap \phi(E) = \{P\}$. If $\operatorname{char}(K) \ne 2$, prove that there are exactly 16 such hyperplanes, and hence that $\#E[4] = 16$.

(e) Continuing with the assumption that $\operatorname{char}(K) \ne 2$, prove that there is a $\bar{K}$-linear change of coordinates such that $\phi(E)$ is given by equations of the form

$$T_0^2 + T_2^2 = T_0 T_3 \qquad \text{and} \qquad T_1^2 + \alpha T_2^2 = T_2 T_3.$$

For what value(s) of α do these equations define a nonsingular curve?

(f) Using the model in (e) and the addition law described in (c), find formulas for $-P$, for $P_1 + P_2$, and for $[2]P$, analogous to the formulas given in (III.2.3).

(g) What is the j-invariant of the elliptic curve described in (e)?

3.11. Generalize Exercise 3.10 as follows. Let E/K be an elliptic curve and choose a basis $f_1, \ldots, f_m$ for $\mathcal{L}\big(m(O)\big)$. For $m \ge 3$, it follows from Exercise 3.6 that the map

$$\phi : E \longrightarrow \mathbb{P}^{m-1}, \qquad \phi = [f_1, \ldots, f_m],$$

is an isomorphism of E onto its image.

(a) Show that $\phi(E)$ is a curve of degree m, i.e., prove that the intersection of $\phi(E)$ and a hyperplane consists of m points, counted with appropriate multiplicities. (*Hint.* Find a hyperplane that intersects $\phi(E)$ at the single point $\phi(O)$ and show that it intersects with multiplicity m.)

(b) Let $P_1, \ldots, P_m \in E$. Prove that $P_1 + \cdots + P_m = O$ if and only if the points $\phi(P_1), \phi(P_2), \ldots, \phi(P_m)$ lie on a hyperplane. (Note that if some of the P_i's coincide, then the hyperplane is required to intersect $\phi(E)$ with correspondingly higher multiplicities at such points.)

(c) ***** Let $P \in E$. Prove that $[m]P = O$ if and only if there is a hyperplane $H \subset \mathbb{P}^{m-1}$ satisfying $H \cap \phi(E) = \{P\}$. If $\operatorname{char}(K) = 0$ or $\operatorname{char}(K) > m$, prove that there are exactly m^2 such points. Use this to deduce that $\deg[m] = m^2$.

3.12. Let $m \ge 2$ be an integer, prime to $\mathrm{char}(K)$ if $\mathrm{char}(K) > 0$. Prove that the natural map

$$\mathrm{Aut}(E) \longrightarrow \mathrm{Aut}\big(E[m]\big)$$

is injective except for $m = 2$, where the kernel is $[\pm 1]$. (You should be able to prove this directly, without using (III.10.1).)

3.13. Generalize (III.4.12) as follows. Let $C/\bar{K}$ be a smooth curve, and let Φ be a finite group of isomorphisms from C to itself. (For example, if E is an elliptic curve, then Φ might contain some translations by torsion points and $[\pm 1]$.) We observe that an element $\alpha \in \Phi$ acts on $\bar{K}(C)$ via the map

$$\alpha^* : \bar{K}(C) \longrightarrow \bar{K}(C), \qquad \alpha^*(f) = f \circ \alpha.$$

(a) Prove that there exist a unique smooth curve $C'/\bar{K}$ and a finite separable morphism $\phi : C \to C'$ such that $\phi^*\bar{K}(C') = \bar{K}(C)^\Phi$, where $\bar{K}(C)^\Phi$ denotes the subfield of $\bar{K}(C)$ fixed by every element of Φ.

(b) Let $P \in C$. Prove that

$$e_\phi(P) = \#\{\alpha \in \Phi : \alpha P = P\}.$$

(c) Prove that ϕ is unramified if and only if every nontrivial element of Φ has no fixed points.

(d) Express the genus of C' in terms of the genus of C, the number of elements in Φ, and the number of fixed points of elements of Φ.

(e) * Suppose that C is defined over K and that Φ is $G_{\bar{K}/K}$-invariant. The latter condition means that for all $\alpha \in \Phi$ and all $\sigma \in G_{\bar{K}/K}$ we have $\alpha^\sigma \in \Phi$. Prove that it is possible to find C' and ϕ as in (a) such that C' and ϕ are defined over K. Prove further that C is unique up to isomorphism over K.

3.14. Prove directly that the natural map

$$\mathrm{Hom}(E_1, E_2) \longrightarrow \mathrm{Hom}\big(T_\ell(E_1), T_\ell(E_2)\big)$$

is injective. (*Hint*. If $\phi : E_1 \to E_2$ satisfies $\phi_\ell = 0$, then $E_1[\ell^n] \subset \ker\phi$ for all $n \ge 1$.) Note that this result is not as strong as (III.7.4).

3.15. Let E_1/K and E_2/K be elliptic curves, and let $\phi : E_1 \to E_2$ be an isogeny of degree m defined over K, where m is prime to $\mathrm{char}(K)$ if $\mathrm{char}(K) > 0$.

(a) Mimic the construction in (III §8) to construct a pairing

$$e_\phi : \ker\phi \times \ker\hat{\phi} \longrightarrow \boldsymbol{\mu}_m.$$

(b) Prove that e_ϕ is bilinear, nondegenerate, and Galois invariant.

(c) Prove that e_ϕ is compatible in the sense that if $\psi : E_2 \to E_3$ is another isogeny, then

$$e_{\psi\circ\phi}(P, Q) = e_\psi(\phi P, Q) \qquad \text{for all } P \in \ker(\psi \circ \phi) \text{ and } Q \in \ker(\hat{\psi}).$$

3.16. *Alternative Definition of the Weil Pairing*. Let E be an elliptic curve. We define a pairing

$$\tilde{e}_m : E[m] \times E[m] \longrightarrow \boldsymbol{\mu}_m$$

as follows: Let $P, Q \in E[m]$ and choose divisors D_P and D_Q in $\mathrm{Div}^0(E)$ that add to P and Q, respectively, i.e., such that $\sigma(D_P) = P$ and $\sigma(D_Q) = Q$, where σ is as in (III.3.4a). Assume further that D_P and D_Q are chosen with disjoint supports. Since P and Q have order m, there are functions $f_P, f_Q \in \bar{K}(E)$ satisfying

$$\mathrm{div}(f_P) = mD_P \qquad \text{and} \qquad \mathrm{div}(f_Q) = mD_Q.$$

We define

$$\tilde{e}_m = \frac{f_P(D_Q)}{f_Q(D_P)}.$$

(See Exercise 2.10 for the definition of the value of a function at a divisor.)

(a) Prove that $\tilde{e}_m(P, Q)$ is well-defined, i.e., its value depends only on P and Q, independent of the various choices of D_P, D_Q, f_P, and f_Q. (*Hint*. Use Weil reciprocity, Exercise 2.11.)

(b) Prove that $\tilde{e}_m(P, Q) \in \boldsymbol{\mu}_m$.

(c) * Prove that $\tilde{e}_m(P, Q) = e_m(Q, P)$, and hence that $\tilde{e}_m = e_m^{-1}$, where e_m is the Weil pairing defined in (III §8).

3.17. Let $\mathcal{K}$ be a definite quaternion algebra. Prove that $\mathcal{K}$ is ramified at ∞. (*Hint*. The ring $M_2(\mathbb{R})$ contains zero divisors.)

3.18. Let E/K be an elliptic curve and suppose that $\mathcal{K} = \mathrm{End}(E) \otimes \mathbb{Q}$ is a quaternion algebra.

(a) Prove that if $p \neq \infty$ and $p \neq \mathrm{char}(K)$, then $\mathcal{K}$ splits at p. (*Hint*. Use (III.7.4).)

(b) Deduce that $\mathrm{char}(K) > 0$. (This gives an alternative proof of (III.5.6c).)

(c) Prove that $\mathcal{K}$ is the unique quaternion algebra that is ramified at ∞ and $\mathrm{char}(K)$ and nowhere else.

(d) * Prove that $\mathrm{End}(E)$ is a maximal order in $\mathcal{K}$. (Note that unlike number fields, a quaternion algebra may have more than one maximal order.)

3.19. Let $\mathcal{K}$ be a quaternion algebra.

(a) Prove that $\mathcal{K} \otimes \bar{\mathbb{Q}} \cong M_2(\bar{\mathbb{Q}})$.

(b) Prove that $\mathcal{K} \otimes \mathcal{K} \cong M_4(\mathbb{Q})$. This shows that $\mathcal{K}$ corresponds to an element of order 2 in the Brauer group $\mathrm{Br}(\mathbb{Q})$. (*Hint*. First show that $\mathcal{K} \otimes \mathcal{K}$ is simple, i.e., has no two-sided ideals. Then prove that the map

$$\mathcal{K} \otimes \mathcal{K} \longrightarrow \mathrm{End}(\mathcal{K}), \qquad a \otimes b \longmapsto (x \mapsto axb),$$

is an isomorphism.)

3.20. Let $\mathcal{K}$ be an imaginary quadratic field with ring of integers $\mathcal{O}$. Prove that the orders of $\mathcal{K}$ are precisely the rings $\mathbb{Z} + f\mathcal{O}$ for integers $f > 0$. The integer f is called the *conductor* of the order.

3.21. Let $C/\bar{K}$ be a curve of genus one. For any point $O \in C$, we can associate to the elliptic curve (C, O) its j-invariant $j(C, O)$. This exercise asks you to prove that the value of $j(C, O)$ is independent of the choice of the base point O. Thus we can assign a *j-invariant* to any curve C of genus one.

(a) Let (C, O) and (C', O') be curves of genus one with associated base points, and suppose that there is an isomorphism of curves $\phi : C \to C'$ satisfying $\phi(O) = O'$. Prove that $j(C, O) = j(C', O')$. (*Hint*. The j-invariant, which is defined in terms of the coefficients of a Weierstrass equation, is independent of the choice of the equation.)
(b) Prove that given any two points $O, O' \in C$, there is an automorphism of C taking O to O'.
(c) Use (a) and (b) to conclude that $j(C, O) = j(C, O')$.

3.22. Let C be a curve of genus one defined over K.
(a) Prove that $j(C) \in K$.
(b) Prove that C is an elliptic curve over K if and only if $C(K) \neq \emptyset$.
(c) Prove that C is always isomorphic, over $\bar{K}$, to an elliptic curve defined over K.

3.23. *Deuring Normal Form.* The following normal form for a Weierstrass equation is sometimes useful when dealing with elliptic curves over (algebraically closed) fields of arbitrary characteristic.
(a) Let E/K be an elliptic curve, and assume that either $\operatorname{char}(K) \neq 3$ or $j(E) \neq 0$. Prove that E has a Weierstrass equation over $\bar{K}$ of the form

$$E : y^2 + \alpha xy + y = x^3 \qquad \text{with } \alpha \in \bar{K}.$$

(b) For the Weierstrass equation in (a), prove that $(0, 0) \in E[3]$.
(c) For what value(s) of α is the Weierstrass equation in (a) singular?
(d) Verify that

$$j(E) = \frac{\alpha^3(\alpha^3 - 24)^3}{\alpha^3 - 27}.$$

3.24. Let E/K be an elliptic curve with complex multiplication over K, i.e., such that $\operatorname{End}_K(E)$ is strictly larger than $\mathbb{Z}$. Prove that for all primes $\ell \neq \operatorname{char}(K)$, the action of $G_{\bar{K}/K}$ on the Tate module $T_\ell(E)$ is abelian. (*Hint*. use the fact that the endomorphisms in $\operatorname{End}_K(E)$ commute with the action of $G_{\bar{K}/K}$ on $T_\ell(E)$.)

3.25. Let E be an elliptic curve and let $P = (x, y) \in E$. As a supplement to the duplication formula (III.2.3d) for x, prove that the quantity $Y\big([2]P\big) = 2y\big([2]P\big) + a_1 x\big([2]P\big) + a_3$ is given by the formula

$$Y\big([2]P\big) = \frac{2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_6)x + (b_4b_8 - b_6^2)}{(2y + a_1x + a_3)^3}.$$

3.26. Let E be the elliptic curve $y^2 = x^3 + x$ having complex multiplication by $\mathbb{Z}[i]$, let $m \geq 2$ be an integer, and let $T \in E[m]$ be a point of exact order m. In each of the following situations, prove that $\big\{T, [i]T\big\}$ is a basis for $E[m]$, and thus that $e_m\big(T, [i]T\big)$ is a primitive m^{th} root of unity.
(a) m is prime and $m \equiv 3 \pmod 4$.
(b) $m \geq 3$ is prime, K is a field with $i \notin K$, and $T \in E(K)$.
The map $[i]$ is an example of a *distortion map*.

3.27. Let E/K be an elliptic curve and let $m \neq 0$ be an integer.
(a) Prove that $x \circ [m] \in K(x)$. In other words, prove that there is a rational function $F_m(x) \in K(x)$ satisfying $x\big([m]P\big) = F_m\big(x(P)\big)$ for all $P \in E$.
(b) Prove that $F_m\big(F_n(x)\big) = F_{mn}(x)$.

(c) Compute $F_2(x)$ and $F_3(x)$ in terms of a given Weierstrass equation for E.

(d) A more intrinsic description of F_m is that it is the unique rational map $F_m : \mathbb{P}^1 \to \mathbb{P}^1$ fitting into the commutative diagram

$$\begin{array}{ccccc} E & \longrightarrow & E/\{\pm 1\} & \xrightarrow{x} & \mathbb{P}^1 \\ {\scriptstyle [m]}\downarrow & & & & \downarrow{\scriptstyle F_m} \\ E & \longrightarrow & E/\{\pm 1\} & \xrightarrow{x} & \mathbb{P}^1. \end{array}$$

Where is F_m ramified and what are the ramification indices at the ramification points?

(e) Find the fixed points of $F_m(x)$, i.e., the points $x \in \mathbb{P}^1(\bar{K})$ satisfying $F_m(x) = x$.

(f) For each fixed point $x \in \mathbb{P}^1(\bar{K})$ of $F_m(x)$, compute the value of the *multiplier* $F_m'(x)$. (*Hint*. The value should depend only on m, independent of the curve E.)

(g) A point $x \in \mathbb{P}^1(\bar{K})$ is called *preperiodic for* F_m if its forward orbit

$$\bigl\{x, F_m(x), F_m(F_m(x)), F_m(F_m(F_m(x))), \dots\bigr\}$$

is finite. Prove that the preperiodic points for F_m are exactly the points in $x\bigl(E(\bar{K})_{\text{tors}}\bigr)$.

The rational map $F_m : \mathbb{P}^1 \to \mathbb{P}^1$ is an example of a *Lattès map*. Lattès maps are important in the theory of dynamical systems. In particular, Lattès proved that over $\mathbb{C}$, the map F_m is everywhere chaotic on $\mathbb{P}^1(\mathbb{C})$. For further information about elliptic curves and dynamical systems, see for example [14, §4.3], [179], or [267, §§1.6.3, 6.4–6.7].

3.28. Let $E \subset \mathbb{P}^2$ be a possibly singular curve given by a Weierstrass equation, and let $L \subset \mathbb{P}^2$ be a line.

(a) Prove directly from the equations that, counted with appropriate multiplicities, the intersection $E \cap L$ consists of exactly three points. (This is a special case of Bézout's theorem.)

(b) Let S be a singular point of E and suppose that $S \in L$. Prove that L intersects E at S with multiplicity at least two. Deduce that $E \cap L$ consists of S and at most one other point.

(c) More generally, let $C \subset \mathbb{P}^2$ be a curve, let $S \in C$ be a singular point of C, and let L be a line containing S. Prove that L intersects C at S with multiplicity at least two.

3.29. Let E be an elliptic curve.

(a) Fix a Weierstrass equation for E, fix a nonzero point $T \in E$, and write $x(P+T) = f\bigl(x(P), y(P)\bigr)$ for some function $f \in K(E) = K(x,y)$. Prove that f is a linear fractional transformation if and only if $T \in E[3]$, where a linear fractional transformation is a function of the form

$$\frac{\alpha x + \beta y + \gamma}{\alpha' x + \beta' y + \gamma'}.$$

(b) More generally, let $m \ge 3$, use a basis for $L\bigl(m(O)\bigr)$ to embed $E \hookrightarrow \mathbb{P}^{m-1}$, and let $T \in E$. Prove that the translation-by-T map $\tau_T : E \to E$ extends to an automorphism of $\mathbb{P}^{m-1}$ if and only if $T \in E[m]$.

3.30. Let A be a finite abelian group of order N^r. Suppose that for every $D \mid N$ we have $\#A[D] = D^r$, where $A[D]$ denotes the subgroup consisting of all elements of order D. Prove that

$$A \cong \left(\frac{\mathbb{Z}}{N\mathbb{Z}}\right)^r.$$

3.31. This exercise sketches an elementary proof of (III.6.2c) in arbitrary characteristic. We start with the case $\operatorname{char}(K) \neq 2$. Let E/K be an elliptic curve.

(a) Use explicit formulas to prove that the doubling map $[2] : E \to E$ has degree 4.

(b) Use (a) to prove that $\deg[2^n] = 4^n$ for all $n \geq 1$.

(c) Use (b) and (III.4.10c) to deduce that $\#E[2^n] = 4^n$ for all $n \geq 1$. (This is where we use the assumption that $\operatorname{char}(K) \neq 2$.)

(d) Use (c) and Exercise 3.30 to conclude that $E[2^n] \cong \mathbb{Z}/2^n\mathbb{Z} \times \mathbb{Z}/2^n\mathbb{Z}$ for all $n \geq 1$.

(e) Verify that the proof of the existence of dual isogenies (III.6.1) is valid in all characteristics.

(f) Suppose that $m \geq 1$ is an integer for which we know, a priori, that $\#E[m] = m^2$. Show that this suffices to prove the existence and basic properties of the Weil pairing $e_m : E[m] \times E[m] \to \boldsymbol{\mu}_m$ as described in (III.8.1) and (III.8.2).

(g) Let $\phi : E_1 \to E_2$ and $\psi : E_1 \to E_2$ be isogenies of elliptic curves. Let $m = 2^n$, so (c) and (f) give the existence of the Weil pairing e_m on E_1 and E_2. Let $T_1 \in E_1[m]$ and $T_2 \in E_2[m]$ be m-torsion points. Use properties of the Weil pairing to prove that

$$e_m\bigl(T_1, (\widehat{\phi+\psi})(T_2)\bigr) = e_m\bigl(T_1, \hat{\phi}(T_2) + \hat{\psi}(T_2)\bigr).$$

Since this holds for all $m = 2^n$, use the nondegeneracy of the Weil pairing to deduce that $\widehat{\phi+\psi} = \hat{\phi} + \hat{\psi}$.

(h) Use (g) to deduce that

$$\hat{[m]} = [m] \quad \text{and} \quad \deg[m] = m^2 \qquad \text{for all integers } m.$$

(Cf. (III.6.2d).)

(i) Let m be any integer such that $m \neq 0$ in K. Use (h) to prove that $\#E[m] = m^2$, and then observe that (f) gives the existence and standard properties of the Weil e_m-pairing.

(j) Finally, if $\operatorname{char}(K) = 2$, replace (a) with a proof via explicit equations that $\deg[3] = 9$. Redo the rest of the exercise with 2^n replaced by 3^n.

3.32. Let $\phi \in \operatorname{End}(E)$ be an endomorphism, and let

$$d = \deg\phi \qquad \text{and} \qquad a = 1 + \deg\phi - \deg(1-\phi).$$

(a) Prove that $\phi^2 - [a] \circ \phi + [d] = [0]$ in $\operatorname{End}(E)$.

(b) Let $\alpha, \beta \in \mathbb{C}$ be the complex roots of the polynomial $t^2 - at + d$. Prove that

$$|\alpha| = |\beta| = \sqrt{d}.$$

(c) Prove that $\deg(1-\phi^n) = 1 + d^n - \alpha^n - \beta^n$ for all $n \geq 1$, and deduce that

$$\bigl|\deg(1-\phi^n) - 1 - d^n\bigr| \leq 2d^{n/2}.$$

(d) Prove that

$$\exp\left(\sum_{n=1}^{\infty} \frac{\deg(1-\phi^n)}{n} X^n\right) = \frac{1 - aX + dX^2}{(1-X)(1-dX)},$$

where the power series converges for $|X| < d^{-1}$.

(*Hint*. Use (III.8.6). For (b), use the fact that $\deg([m] + [n] \circ \phi) \geq 0$ for all $m, n \in \mathbb{Z}$.)

3.33. Let $\mathcal{K}$ be a $\mathbb{Q}$-division algebra, i.e., $\mathcal{K}$ is a (not necessarily commutative) $\mathbb{Q}$-algebra in which every nonzero element has a multiplicative inverse. This exercise sketches a proof of the following theorem, which can be used instead of (III.9.3) to prove (III.9.4). In particular, it is not necessary to know, a priori, that $\mathrm{End}(E)$ has rank at most four (III.7.4), (III.7.5).

Theorem. *Suppose that every element of $\mathcal{K}$ satisfies a quadratic equation with coefficients in $\mathbb{Q}$. Then either $\mathcal{K} = \mathbb{Q}$, $\mathcal{K}$ is a quadratic field, or $\mathcal{K}$ is a quaternion algebra.*

(a) Let $\alpha, \beta \in \mathcal{K}$. Prove that if $\beta \notin \mathbb{Q}(\alpha)$, then $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) = \mathbb{Q}$.
(b) Let $\alpha, \beta \in \mathcal{K}$. Prove that if $\alpha \notin \mathbb{Q}$ and $\alpha\beta = \beta\alpha$, then $\beta \in \mathbb{Q}(\alpha)$.
(c) Let $\alpha, \beta \in \mathcal{K}$. Prove that if $\alpha^2, \beta^2 \in \mathbb{Q}$, $\alpha \notin \mathbb{Q}$, and $\beta \notin \mathbb{Q}(\alpha)$, then $\alpha\beta + \beta\alpha \in \mathbb{Q}$.
(d) Let $\alpha \in \mathcal{K}$. Prove that there exists an $\alpha' \in \mathcal{K}$ such that $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha')$ and $\alpha'^2 \in \mathbb{Q}$.
(e) Let $\alpha, \beta \in \mathcal{K}^*$ satisfy $\alpha^2, \beta^2 \in \mathbb{Q}$. Prove that there exists a $\beta' \in \mathcal{K}$ such that $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha, \beta')$ and $\beta'^2, (\alpha\beta')^2 \in \mathbb{Q}$.
(f) Let $\alpha, \beta \in \mathcal{K}$ satisfy $\alpha \notin \mathbb{Q}$, $\beta \notin \mathbb{Q}(\alpha)$, and $\alpha^2, \beta^2, (\alpha\beta)^2 \in \mathbb{Q}$. Prove that $\alpha\beta = -\beta\alpha$.
(g) Prove the theorem.
(h) Use the theorem to prove (III.9.4).

3.34. Let K be a field. An *elliptic divisibility sequence* (EDS) over K is a sequence $(W_n)_{n\ge1}$ defined by four initial conditions $W_1, W_2, W_3, W_4 \in K$ and satisfying the recurrence

$$W_{m+n}W_{m-n}W_1^2 = W_{m+1}W_{m-1}W_n^2 - W_{n+1}W_{n-1}W_m^2 \qquad \text{for all } m > n > 0.$$

An EDS in *nondegenerate* if $W_1W_2W_3 \ne 0$.
(a) Prove that a sequence $(W_n)_{n\ge1}$ of elements of K with $W_1W_2W_3 \ne 0$ is an EDS if and only if it satisfies the two conditions

$$W_{2n+1}W_1^3 = W_{n+2}W_n^3 - W_{n-1}W_{n+1}^3 \qquad \text{for all } n \ge 2,$$
$$W_{2n}W_2W_1^2 = W_n(W_{n+2}W_{n-1}^2 - W_{n-2}W_{n+1}^2) \qquad \text{for all } n \ge 3.$$

(b) Prove that an EDS satisfies the more general recurrence

$$W_{m+n}W_{m-n}W_r^2 = W_{m+r}W_{m-r}W_n^2 - W_{n+r}W_{n-r}W_m^2 \qquad \text{for all } m > n > r > 0.$$

(c) Let (W_n) be an EDS and let $c \in K^*$. Prove that $(c^{n^2-1}W_n)$ is also an EDS.
(d) Let (W_n) be a nondegenerate EDS. Prove that (W_n/W_1) is an EDS. More generally, if $W_m \ne 0$, prove that $(W_{mn}/W_m)_{n\ge1}$ is an EDS.

3.35. This exercise gives some examples of elliptic divisibility sequences (EDS).
(a) Prove that the sequence $1, 2, 3, \ldots$ is an EDS.
(b) Prove that the sequence $1, 3, 8, 21, 55, 144, 377, 987, \ldots$ consisting of every other term of the Fibonacci sequence is an EDS.
(c) More generally, let $(L_n)_{n\ge1}$ be defined by a linear recurrence of the form

$$L_1 = 1, \qquad L_2 = A, \qquad L_{n+2} = AL_{n+1} - L_n \quad \text{for } n \ge 1.$$

Generalize (b) by finding a subsequence of (L_n) that is an EDS.
(d) The most interesting EDS are associated to points on elliptic curves. Let E/K be an elliptic curve and let $P \in E(K)$ be a nonzero point. Define a sequence

$$W_n = \psi_n(P) \qquad \text{for } n \ge 1,$$

where ψ_n is the n^{th} division polynomial for E as defined in Exercise 3.7. Prove that (W_n) is an EDS.

(e) Let (W_n) be an EDS associated to an elliptic curve E/K and nonzero point $P \in E(K)$ as in (d). Prove that P is a point of finite order at least 4 if and only if $W_n = 0$ for some $n \geq 4$.

(f) * Let (W_n) be an EDS associated to an elliptic curve E/K and a nonzero point $P \in E(K)$ of finite order. Let $r \geq 2$ be the smallest index such that $W_r = 0$. (The number r is called the *rank of apparition* of the sequence.) Assuming that $r \geq 4$, prove that there exist $A, B \in K^*$ such that

$$W_{ri+j} = W_j A^{ij} B^{i^2} \qquad \text{for all } i \geq 0 \text{ and all } j \geq 1.$$

(g) Suppose that K is a finite field and that the rank of apparition r of (W_n) is at least 4. Prove that the sequence (W_n) is periodic with period that is a multiple of r.

3.36. Let R be an integral domain, and let $(W_n)_{n\geq 1}$ be a nondegenerate elliptic divisibility sequence with $W_i \in R$ such that W_1 divides each of W_2, W_3, and W_4, and such that W_2 divides W_4.

(a) Prove that (W_n) is a *divisibility sequence*, in the sense that

$$m \mid n \quad \Longrightarrow \quad W_m \mid W_n.$$

(b) Suppose further that R is a principal ideal domain and that $\gcd(W_3, W_4) = 1$. Prove that (W_n) satisfies the stronger divisibility relation

$$W_{\gcd(m,n)} = \gcd(W_m, W_n) \qquad \text{for all } m, n \geq 1.$$