Chapter 3

Torsion Points

The torsion points, namely those whose orders are finite, play an important role in the study of elliptic curves. We'll see this in Chapter 4 for elliptic curves over finite fields, where all points are torsion points, and in Chapter 8, where we use 2-torsion points in a procedure known as descent. In the present chapter, we first consider the elementary cases of 2- and 3-torsion, then determine the general situation. Finally, we discuss the important Weil and Tate-Lichtenbaum pairings.

3.1 Torsion Points

Let E be an elliptic curve defined over a field K. Let n be a positive integer. We are interested in

$$E[n] = \{P \in E(\overline{K}) \,|\, nP = \infty\}$$

(recall that $\overline{K}$ = algebraic closure of K). We emphasize that $E[n]$ contains points with coordinates in $\overline{K}$, not just in K.

When the characteristic of K is not 2, E can be put in the form $y^2 =$ cubic, and it is easy to determine $E[2]$. Let

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

with $e_1, e_2, e_3 \in \overline{K}$. A point P satisfies $2P = \infty$ if and only if the tangent line at P is vertical. It is easy to see that this means that $y = 0$, so

$$E[2] = \{\infty, (e_1, 0), (e_2, 0), (e_3, 0)\}.$$

As an abstract group, this is isomorphic to $\mathbf{Z}_2 \oplus \mathbf{Z}_2$.

The situation in characteristic 2 is more subtle. In Section 2.8 we showed that E can be assumed to have one of the following two forms:

$$(I) \quad y^2 + xy + x^3 + a_2x^2 + a_6 = 0 \quad \text{or} \quad (II) \quad y^2 + a_3y + x^3 + a_4x + a_6 = 0.$$

In the first case, $a_6 \neq 0$ and in the second case, $a_3 \neq 0$ (otherwise the curves would be singular). If $P = (x, y)$ is a point of order 2, then the tangent at P must be vertical, which means that the partial derivative with respect to y must vanish. In case I, this means that $x = 0$. Substitute $x = 0$ into (I) to obtain $0 = y^2 + a_6 = (y + \sqrt{a_6})^2$. Therefore $(0, \sqrt{a_6})$ is the only point of order 2 (square roots are unique in characteristic 2), so

$$E[2] = \{\infty, (0, \sqrt{a_6})\}.$$

As an abstract group, this is isomorphic to $\mathbf{Z}_2$.

In case II, the partial derivative with respect to y is $a_3 \neq 0$. Therefore, there is no point of order 2, so

$$E[2] = \{\infty\}.$$

We summarize the preceding discussion as follows.

PROPOSITION 3.1

Let E be an elliptic curve over a field K. If the characteristic of K is not 2, then

$$E[2] \simeq \mathbf{Z}_2 \oplus \mathbf{Z}_2.$$

If the characteristic of K is 2, then

$$E[2] \simeq 0 \quad \textit{or} \quad \mathbf{Z}_2.$$

Now let's look at $E[3]$. Assume first that the characteristic of K is not 2 or 3, so that E can be given by the equation $y^2 = x^3 + Ax + B$. A point P satisfies $3P = \infty$ if and only if $2P = -P$. This means that the x-coordinate of $2P$ equals the x-coordinate of P (the y-coordinates therefore differ in sign; of course, if they were equal, then $2P = P$, hence $P = \infty$). In equations, this becomes

$$m^2 - 2x = x, \qquad \text{where } m = \frac{3x^2 + A}{2y}.$$

Using the fact that $y^2 = x^3 + Ax + B$, we find that

$$(3x^2 + A)^2 = 12x(x^3 + Ax + B).$$

This simplifies to

$$3x^4 + 6Ax^2 + 12Bx - A^2 = 0.$$

The discriminant of this polynomial is $-6912(4A^3 + 27B^2)^2$, which is nonzero. Therefore the polynomial has no multiple roots. There are 4 distinct values of x (in $\overline{K}$), and each x yields two values of y, so we have eight points of order 3. Since ∞ is also in $E[3]$, we see that $E[3]$ is a group of order 9 in which every element is 3-torsion. It follows that

$$E[3] \simeq \mathbf{Z}_3 \oplus \mathbf{Z}_3.$$

The case where K has characteristic 2 is Exercise 3.2.

Now let's look at characteristic 3. We may assume that E has the form $y^2 = x^3 + a_2x^2 + a_4x + a_6$. Again, we want the x-coordinate of $2P$ to equal the x-coordinate of P. We calculate the x-coordinate of $2P$ by the usual procedure and set it equal to the x-coordinate x of P. Some terms disappear because $3 = 0$. We obtain

$$\left(\frac{2a_2x + a_4}{2y}\right)^2 - a_2 = 3x = 0.$$

This simplifies to (recall that $4 = 1$)

$$a_2x^3 + a_2a_6 - a_4^2 = 0.$$

Note that we cannot have $a_2 = a_4 = 0$ since then $x^3 + a_6 = (x + a_6^{1/3})^3$ has multiple roots, so at least one of a_2, a_4 is nonzero.

If $a_2 = 0$, then we have $-a_4^2 = 0$, which cannot happen, so there are no values of x. Therefore $E[3] = \{\infty\}$ in this case.

If $a_2 \neq 0$, then we obtain an equation of the form $a_2(x^3 + a) = 0$, which has a single triple root in characteristic 3. Therefore, there is one value of x, and two corresponding values of y. This yields 2 points of order 3. Since there is also the point ∞, we see that $E[3]$ has order 3, so $E[3] \simeq \mathbf{Z}_3$ as abstract groups.

The general situation is given by the following.

THEOREM 3.2

Let E be an elliptic curve over a field K and let n be a positive integer. If the characteristic of K does not divide n, or is 0, then

$$E[n] \simeq \mathbf{Z}_n \oplus \mathbf{Z}_n.$$

If the characteristic of K is $p > 0$ and $p|n$, write $n = p^r n'$ with $p \nmid n'$. Then

$$E[n] \simeq \mathbf{Z}_{n'} \oplus \mathbf{Z}_{n'} \quad \text{or} \quad \mathbf{Z}_n \oplus \mathbf{Z}_{n'}.$$

The theorem will be proved in Section 3.2.

An elliptic curve E in characteristic p is called **ordinary** if $E[p] \simeq \mathbf{Z}_p$. It is called **supersingular** if $E[p] \simeq 0$. Note that the terms "supersingular" and "singular" (as applied to bad points on elliptic curves) are unrelated. In the theory of complex multiplication (see Chapter 10), the "singular" j-invariants are those corresponding to elliptic curves with endomorphism rings larger than $\mathbf{Z}$, and the "supersingular" j-invariants are those corresponding to elliptic curves with the largest possible endomorphism rings, namely, orders in quaternion algebras.

Let n be a positive integer not divisible by the characteristic of K. Choose a **basis** $\{\beta_1, \beta_2\}$ for $E[n] \simeq \mathbf{Z}_n \oplus \mathbf{Z}_n$. This means that every element of $E[n]$ is

expressible in the form $m_1\beta_1 + m_2\beta$ with integers m_1, m_2. Note that m_1, m_2 are uniquely determined mod n. Let $\alpha : E(\overline{K}) \to E(\overline{K})$ be a homomorphism. Then α maps $E[n]$ into $E[n]$. Therefore, there are $a, b, c, d \in \mathbf{Z}_n$ such that

$$\alpha(\beta_1) = a\beta_1 + c\beta_2, \quad \alpha(\beta_2) = b\beta_1 + d\beta_2.$$

Therefore each homomorphism $\alpha : E(\overline{K}) \to E(\overline{K})$ is represented by a 2×2 matrix

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

Composition of homomorphisms corresponds to multiplication of the corresponding matrices.

In many cases, the homomorphism α will be taken to be an endomorphism, which means that it is given by rational functions (see Section 2.9). But α can also come from an automorphism of $\overline{K}$ that fixes K. This leads to the important subject of representations of Galois groups (that is, homomorphisms from Galois groups to groups of matrices).

Example 3.1

Let E be the elliptic curve defined over $\mathbf{R}$ by $y^2 = x^3 - 2$, and let $n = 2$. Then

$$E[2] = \{\infty, (2^{1/3}, 0), (\zeta 2^{1/3}, 0), (\zeta^2 2^{1/3}, 0)\},$$

where ζ is a nontrivial cube root of unity. Let

$$\beta_1 = (2^{1/3}, 0), \quad \beta_2 = (\zeta 2^{1/3}, 0).$$

Then $\{\beta_1, \beta_2\}$ is a basis for $E[2]$, and $\beta_3 = (\zeta^2 2^{1/3}, 0) = \beta_1 + \beta_2$.

Let $\alpha : E(\mathbf{C}) \to E(\mathbf{C})$ be complex conjugation: $\alpha(x, y) = (\overline{x}, \overline{y})$, where the bar denotes complex conjugation. It is easy to verify that α is a homomorphism. In fact, since all the coefficients of the formulas for the group law have real coefficients, we have $\overline{P_1} + \overline{P_2} = \overline{P_1 + P_2}$. This is the same as $\alpha(P_1) + \alpha(P_2) = \alpha(P_1 + P_2)$. We have

$$\alpha(\beta_1) = 1 \cdot \beta_1 + 0 \cdot \beta_2, \quad \alpha(\beta_2) = \beta_3 = 1 \cdot \beta_1 + 1 \cdot \beta_2.$$

Therefore we obtain the matrix $\alpha_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Note that $\alpha \circ \alpha$ is the identity, which corresponds to the fact that α_2^2 is the identity matrix mod 2. □

3.2 Division Polynomials

The goal of this section is to prove Theorem 3.2. We'll also obtain a few other results that will be needed in proofs in Section 4.2.

In order to study the torsion subgroups, we need to describe the map on an elliptic curve given by multiplication by an integer. As in Section 2.9, this is an endomorphism of the elliptic curve and can be described by rational functions. We shall give formulas for these functions.

We start with variables A, B. Define the **division polynomials** $\psi_m \in \mathbf{Z}[x, y, A, B]$ by

$$\begin{aligned}
\psi_0 &= 0 \\
\psi_1 &= 1 \\
\psi_2 &= 2y \\
\psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2 \\
\psi_4 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3) \\
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \text{ for } m \geq 2 \\
\psi_{2m} &= (2y)^{-1}(\psi_m)(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \text{ for } m \geq 3.
\end{aligned}$$

LEMMA 3.3

ψ_n is a polynomial in $\mathbf{Z}[x, y^2, A, B]$ when n is odd, and ψ_n is a polynomial in $2y\mathbf{Z}[x, y^2, A, B]$ when n is even.

PROOF The lemma is true for $n \leq 4$. Assume, by induction, that it holds for all $n < 2m$. We may assume that $2m > 4$, so $m > 2$. Then $2m > m + 2$, so all polynomials appearing in the definition of ψ_{2m} satisfy the induction assumptions. If m is even, then $\psi_m, \psi_{m+2}, \psi_{m-2}$ are in $2y\mathbf{Z}[x, y^2, A, B]$, from which it follows that ψ_{2m} is in $2y\mathbf{Z}[x, y^2, A, B]$. If m is odd, then ψ_{m-1} and ψ_{m+1} are in $2y\mathbf{Z}[x, y^2, A, B]$, so again we find that ψ_{2m} is in $2y\mathbf{Z}[x, y^2, A, B]$. Therefore, the lemma holds for $n = 2m$. Similarly, it holds for $n = 2m + 1$. ∎

Define polynomials

$$\begin{aligned}
\phi_m &= x\psi_m^2 - \psi_{m+1}\psi_{m-1} \\
\omega_m &= (4y)^{-1}(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2).
\end{aligned}$$

LEMMA 3.4

$\phi_n \in \mathbf{Z}[x, y^2, A, B]$ for all n. If n is odd, then $\omega_n \in y\mathbf{Z}[x, y^2, A, B]$. If n is even, then $\omega_n \in \mathbf{Z}[x, y^2, A, B]$.

PROOF If n is odd, then ψ_{n+1} and ψ_{n-1} are in $y\mathbf{Z}[x, y^2, A, B]$, so their product is in $\mathbf{Z}[x, y^2, A, B]$. Therefore, $\phi_n \in \mathbf{Z}[x, y^2, A, B]$. If n is even, the proof is similar.

The facts that $y^{-1}\omega_n \in \mathbf{Z}[x, y^2, A, B]$ for odd n and $\omega_n \in \frac{1}{2}\mathbf{Z}[x, y^2, A, B]$ for even n follow from Lemma 3.3, and these are all that we need for future

applications. However, to get rid of the extra 2 in the denominator, we proceed as follows. Induction (treating separately the various possibilities for n mod 4) shows that

$$\psi_n \equiv (x^2 + A)^{(n^2-1)/4} \pmod 2 \quad \text{when } n \text{ is odd}$$

and

$$(2y)^{-1}\psi_n \equiv \left(\frac{n}{2}\right)(x^2 + A)^{(n^2-4)/4} \pmod 2 \quad \text{when } n \text{ is even.}$$

A straightforward calculation now yields the lemma. ∎

We now consider an elliptic curve

$$E: \quad y^2 = x^3 + Ax + B, \quad 4A^3 + 27B^2 \neq 0.$$

We don't specify what ring or field the coefficients A, B are in, so we continue to treat them as variables. We regard the polynomials in $\mathbf{Z}[x, y^2, A, B]$ as polynomials in $\mathbf{Z}[x, A, B]$ by replacing y^2 with $x^3 + Ax + B$. Therefore, we write $\phi_n(x)$ and $\psi_n^2(x)$. Note that ψ_n is not necessarily a polynomial in x alone, while ψ_n^2 is always a polynomial in x.

LEMMA 3.5

$$\phi_n(x) = x^{n^2} + \textit{lower degree terms}$$
$$\psi_n^2(x) = n^2 x^{n^2-1} + \textit{lower degree terms}$$

PROOF In fact, we claim that

$$\psi_n = \begin{cases} y(nx^{(n^2-4)/2} + \cdots) & \text{if } n \text{ is even} \\ nx^{(n^2-1)/2} + \cdots & \text{if } n \text{ is odd.} \end{cases}$$

This is proved by induction. For example, if $n = 2m + 1$ with m even, then the leading term of $\psi_{m+2}\psi_m^3$ is

$$(m + 2)m^3 y^4 x^{\frac{(m+2)^2-4}{2} + \frac{3m^2-12}{2}}.$$

Changing y^4 to $(x^3 + Ax + B)^2$ yields

$$(m + 2)m^3 x^{\frac{(2m+1)^2-1}{2}}.$$

Similarly, the leading term of $\psi_{m-1}\psi_{m+1}^3$ is

$$(m - 1)(m + 1)^3 x^{\frac{(2m+1)^2-1}{2}}.$$

Subtracting and using the recursion relation shows that the leading term of ψ_{2m+1} is as claimed in the lemma. The other cases are treated similarly. ∎

We can now state the main theorem.

THEOREM 3.6

Let $P = (x, y)$ be a point on the elliptic curve $y^2 = x^3 + Ax + B$ (over some field of characteristic not 2), and let n be a positive integer. Then

$$nP = \left(\frac{\phi_n(x)}{\psi_n^2(x)}, \frac{\omega_n(x,y)}{\psi_n(x,y)^3} \right).$$

The proof will be given in Section 9.5.

COROLLARY 3.7

Let E be an elliptic curve. The endomorphism of E given by multiplication by n has degree n^2.

PROOF From Lemma 3.5, we have that the maximum of the degrees of the numerator and denominator of $\phi_n(x)/\psi_n^2(x)$ is n^2. Therefore, the degree of the endomorphism is n^2 if this rational function is reduced, that is, if $\phi_n(x)$ and $\psi_n^2(x)$ have no common roots. We'll show that this is the case. Suppose not. Let n be the smallest index for which they have a common root.

Suppose $n = 2m$ is even. A quick calculation shows that

$$\phi_2(x) = x^4 - 2Ax^2 - 8Bx + A^2.$$

Computing the x-coordinate of $2m(x, y)$ in two steps by multiplying by m and then by 2, and using the fact that

$$\psi_2^2 = 4y^2 = 4(x^3 + Ax + B),$$

we obtain

$$\begin{aligned} \frac{\phi_{2m}}{\psi_{2m}^2} &= \frac{\phi_2(\phi_m/\psi_m^2)}{\psi_2^2(\phi_m/\psi_m^2)} \\ &= \frac{\phi_m^4 - 2A\phi_m^2\psi_m^4 - 8B\phi_m\psi_m^6 + A^2\psi_m^8}{(4\psi_m^2)(\phi_m^3 + A\phi_m\psi_m^4 + B\psi_m^6)} \\ &= \frac{U}{V}, \end{aligned}$$

where U and V are the numerator and denominator of the preceding expression. To show U and V have no common roots, we need the following.

LEMMA 3.8
Let $\Delta = 4A^3 + 27B^2$ *and let*

$$\begin{aligned}
F(x,z) &= x^4 - 2Ax^2z^2 - 8Bxz^3 + A^2z^4 \\
G(x,z) &= 4z(x^3 + Axz^2 + Bz^3) \\
f_1(x,z) &= 12x^2z + 16Az^3 \\
g_1(x,z) &= 3x^3 - 5Axz^2 - 27Bz^3 \\
f_2(x,z) &= 4\Delta x^3 - 4A^2Bx^2z + 4A(3A^3 + 22B^2)xz^2 + 12B(A^3 + 8B^2)z^3 \\
g_2(x,z) &= A^2Bx^3 + A(5A^3 + 32B^2)x^2z + 2B(13A^3 + 96B^2)xz^2 \\
&\quad - 3A^2(A^3 + 8B^2)z^3.
\end{aligned}$$

Then

$$Ff_1 - Gg_1 = 4\Delta z^7 \text{ and } Ff_2 + Gg_2 = 4\Delta x^7.$$

PROOF This is verified by a straightforward calculation. Where do these identities come from? The polynomials $F(x,1)$ and $G(x,1)$ have no common roots, so the extended Euclidean algorithm, applied to polynomials, finds polynomials $f_1(x), g_1(x)$ such that $F(x,1)f_1(x) + G(x,1)g_1(x) = 1$. Changing x to x/z, multiplying by z^7 (to make everything homogeneous), then multiplying by 4Δ to clear denominators yields the first identity. The second is obtained by reversing the roles of x and z. ∎

The lemma implies that

$$\begin{aligned}
U \cdot f_1(\phi_m, \psi_m^2) - V \cdot g_1(\phi_m, \psi_m^2) &= 4\psi_m^{14}\Delta \\
U \cdot f_2(\phi_m, \psi_m^2) + V \cdot g_2(\phi_m, \psi_m^2) &= 4\phi_m^7\Delta.
\end{aligned}$$

If U, V have a common root, then so do ϕ_m and ψ_m^2. Since $n = 2m$ is the first index for which there is a common root, this is impossible.

It remains to show that $U = \phi_{2m}$ and $V = \psi_{2m}^2$. Since $U/V = \phi_{2m}/\psi_{2m}^2$ and since U, V have no common root, it follows that ϕ_{2m} is a multiple of U and ψ_{2m}^2 is a multiple of V. A quick calculation using Lemma 3.5 shows that

$$U = x^{4m^2} + \text{lower degree terms.}$$

Lemma 3.5 and the fact that ϕ_{2m} is a multiple of U imply that $\phi_{2m} = U$. Therefore, $V = \psi_{2m}^2$. It follows that ϕ_{2m} and ψ_{2m}^2 have no common roots.

Now suppose that the smallest index n such that there is a common root is odd: $n = 2m + 1$. Let r be a common root of ϕ_n and ψ_n^2. Since

$$\phi_n = x\psi_n^2 - \psi_{n-1}\psi_{n+1},$$

and since $\psi_{n+1}\psi_{n-1}$ is a polynomial in x, we have $(\psi_{n+1}\psi_{n-1})(r) = 0$. But $\psi_{n\pm1}^2$ are polynomials in x and their product vanishes at r. Therefore $\psi_{n+\delta}^2(r) = 0$, where δ is either 1 or -1.

Since n is odd, both ψ_n and $\psi_{n+2\delta}$ are polynomials in x. Moreover,

$$(\psi_n\psi_{n+2\delta})^2 = \psi_n^2\psi_{n+2\delta}^2$$

vanishes at r. Therefore $\psi_n\psi_{n+2\delta}$ vanishes at r. Since

$$\phi_{n+\delta} = x\psi_{n+\delta}^2 - \psi_n\psi_{n+2\delta},$$

we find that $\phi_{n+\delta}(r) = 0$. Therefore, $\phi_{n+\delta}$ and $\psi_{n+\delta}^2$ have a common root. Note that $n+\delta$ is even.

When considering the case that n is even, we showed that if ϕ_{2m} and ψ_{2m}^2 have a common root, then ϕ_m and ψ_m^2 have a common root. In the present case, we apply this to $2m = n+\delta$. Since n is assumed to be the smallest index for which there is a common root, we have

$$\frac{n+\delta}{2} \geq n.$$

This implies that $n = 1$. But clearly $\phi_1 = x$ and $\psi_1^2 = 1$ have no common roots, so we have a contradiction.

This proves that ϕ_n and ψ_n^2 have no common roots in all cases. Therefore, as pointed out at the beginning of the proof, the multiplication by n map has degree n^2. This completes the proof of Corollary 3.7. ∎

Recall from Section 2.9 that if $\alpha(x,y) = (R(x), yS(x))$ is an endomorphism of an elliptic curve E, then α is separable if $R'(x)$ is not identically 0. Assume n is not a multiple of the characteristic p of the field. From Theorem 3.6 we see that the multiplication by n map has

$$R(x) = \frac{x^{n^2} + \cdots}{n^2x^{n^2-1} + \cdots}.$$

The numerator of the derivative is $n^2x^{2n^2-2} + \cdots \neq 0$, so $R'(x) \neq 0$. Therefore, multiplication by n is separable. From Corollary 3.7 and Proposition 2.21, $E[n]$, the kernel of multiplication by n, has order n^2. The structure theorem for finite abelian groups (see Appendix B) says that $E[n]$ is isomorphic to

$$\mathbf{Z}_{n_1} \oplus \mathbf{Z}_{n_2} \oplus \cdots \oplus \mathbf{Z}_{n_k},$$

for some integers $n_1, n_2, \ldots, n_k$ with $n_i | n_{i+1}$ for all i. Let ℓ be a prime dividing n_1. Then $\ell | n_i$ for all i. This means that $E[\ell] \subseteq E[n]$ has order ℓ^k. Since we have just proved that $E[\ell]$ has order ℓ^2, we must have $k = 2$. Multiplication by n annihilates $E[n] \simeq \mathbf{Z}_{n_1} \oplus \mathbf{Z}_{n_2}$, so we must have $n_2 | n$. Since $n^2 = \#E[n] = n_1n_2$, it follows that $n_1 = n_2 = n$. Therefore,

$$E[n] \simeq \mathbf{Z}_n \oplus \mathbf{Z}_n$$

when the characteristic p of the field does not divide n.

It remains to consider the case where $p|n$. We first determine the p-power torsion on E. By Proposition 2.28, multiplication by p is not separable. By Proposition 2.21, the kernel $E[p]$ of multiplication by p has order strictly less than the degree of this endomorphism, which is p^2 by Corollary 3.7. Since every element of $E[p]$ has order 1 or p, the order of $E[p]$ is a power of p, hence must be 1 or p. If $E[p]$ is trivial, then $E[p^k]$ must be trivial for all k. Now suppose $E[p]$ has order p. We claim that $E[p^k] \simeq \mathbf{Z}_{p^k}$ for all k. It is easy to see that $E[p^k]$ is cyclic. The hard part is to show that the order is p^k, rather than something smaller (for example, why can't we have $E[p^k] = E[p] \simeq \mathbf{Z}_p$ for all k?). Suppose there exists an element P of order p^j. By Theorem 2.22, multiplication by p is surjective, so there exists a point Q with $pQ = P$. Since

$$p^j Q = p^{j-1} P \neq \infty \quad \text{but} \quad p^{j+1} Q = p^j P = \infty,$$

Q has order p^{j+1}. By induction, there are points of order p^k for all k. Therefore, $E[p^k]$ is cyclic of order p^k.

We can now put everything together. Write $n = p^r n'$ with $r \geq 0$ and $p \nmid n'$. Then

$$E[n] \simeq E[n'] \oplus E[p^r].$$

We have $E[n'] \simeq \mathbf{Z}_{n'} \oplus \mathbf{Z}_{n'}$, since $p \nmid n'$. We have just showed that $E[p^r] \simeq 0$ or $\mathbf{Z}_{p^r}$. Recall that

$$\mathbf{Z}_{n'} \oplus \mathbf{Z}_{p^r} \simeq \mathbf{Z}_{n'p^r} \simeq \mathbf{Z}_n$$

(see Appendix A). Therefore, we obtain

$$E[n] \simeq \mathbf{Z}_{n'} \oplus \mathbf{Z}_{n'} \quad \text{or} \quad \mathbf{Z}_n \oplus \mathbf{Z}_{n'}.$$

This completes the proof of Theorem 3.2. ∎

3.3 The Weil Pairing

The Weil pairing on the n-torsion on an elliptic curve is a major tool in the study of elliptic curves. For example, it will be used in Chapter 4 to prove Hasse's theorem on the number of points on an elliptic curve over a finite field. It will be used in Chapter 5 to attack the discrete logarithm problem for elliptic curves. In Chapter 6, it will be used in a cryptographic setting.

Let E be an elliptic curve over a field K and let n be an integer not divisible by the characteristic of K. Then $E[n] \simeq \mathbf{Z}_n \oplus \mathbf{Z}_n$. Let

$$\mu_n = \{x \in \overline{K} \mid x^n = 1\}$$

be the group of nth roots of unity in $\overline{K}$. Since the characteristic of K does not divide n, the equation $x^n = 1$ has no multiple roots, hence has n roots in

$\overline{K}$. Therefore, μ_n is a cyclic group of order n. Any generator ζ of μ_n is called a **primitive nth root of unity**. This is equivalent to saying that $\zeta^k = 1$ if and only if n divides k.

THEOREM 3.9

Let E be an elliptic curve defined over a field K and let n be a positive integer. Assume that the characteristic of K does not divide n. Then there is a pairing

$$e_n : E[n] \times E[n] \to \mu_n,$$

called the **Weil pairing**, *that satisfies the following properties:*

1. *e_n is bilinear in each variable. This means that*

$$e_n(S_1 + S_2, T) = e_n(S_1, T)e_n(S_2, T)$$

and

$$e_n(S, T_1 + T_2) = e_n(S, T_1)e_n(S, T_2)$$

for all $S, S_1, S_2, T, T_1, T_2 \in E[n]$.

2. *e_n is nondegenerate in each variable. This means that if $e_n(S, T) = 1$ for all $T \in E[n]$ then $S = \infty$ and also that if $e_n(S, T) = 1$ for all $S \in E[n]$ then $T = \infty$.*

3. *$e_n(T, T) = 1$ for all $T \in E[n]$.*

4. *$e_n(T, S) = e_n(S, T)^{-1}$ for all $S, T \in E[n]$.*

5. *$e_n(\sigma S, \sigma T) = \sigma(e_n(S, T))$ for all automorphisms σ of $\overline{K}$ such that σ is the identity map on the coefficients of E (if E is in Weierstrass form, this means that $\sigma(A) = A$ and $\sigma(B) = B$).*

6. *$e_n(\alpha(S), \alpha(T)) = e_n(S, T)^{\deg(\alpha)}$ for all separable endomorphisms α of E. If the coefficients of E lie in a finite field $\mathbf{F}_q$, then the statement also holds when α is the Frobenius endomorphism ϕ_q. (Actually, the statement holds for all endomorphisms α, separable or not. See [38].)*

The proof of the theorem will be given in Chapter 11. In the present section, we'll derive some consequences.

COROLLARY 3.10

Let $\{T_1, T_2\}$ be a basis of $E[n]$. Then $e_n(T_1, T_2)$ is a primitive nth root of unity.

PROOF Suppose $e_n(T_1, T_2) = \zeta$ with $\zeta^d = 1$. Then $e_n(T_1, dT_2) = 1$. Also, $e_n(T_2, dT_2) = e_n(T_2, T_2)^d = 1$ (by (1) and (3)). Let $S \in E[n]$. Then

$S = aT_1 + bT_2$ for some integers a, b. Therefore,

$$e_n(S, dT_2) = e_n(T_1, dT_2)^a e_n(T_2, dT_2)^b = 1.$$

Since this holds for all S, (2) implies that $dT_2 = \infty$. Since $dT_2 = \infty$ if and only if $n|d$, it follows that ζ is a primitive nth root of unity.

COROLLARY 3.11
If $E[n] \subseteq E(K)$, then $\mu_n \subset K$.

REMARK 3.12 Recall that points in $E[n]$ are allowed to have coordinates in $\overline{K}$. The hypothesis of the corollary is that these points all have coordinates in K. ∎

PROOF Let σ be any automorphism of $\overline{K}$ such that σ is the identity on K. Let T_1, T_2 be a basis of $E[n]$. Since T_1, T_2 are assumed to have coordinates in K, we have $\sigma T_1 = T_1$ and $\sigma T_2 = T_2$. By (5),

$$\zeta = e_n(T_1, T_2) = e_n(\sigma T_1, \sigma T_2) = \sigma(e_n(T_1, T_2)) = \sigma(\zeta).$$

The fundamental theorem of Galois theory says that if an element $x \in \overline{K}$ is fixed by all such automorphisms σ, then $x \in K$. Therefore, $\zeta \in K$. Since ζ is a primitive nth root of unity by Corollary 3.10, it follows that $\mu_n \subset K$. (*Technical point:* The fundamental theorem of Galois theory only implies that ζ lies in a purely inseparable extension of K. But an nth root of unity generates a separable extension of K when the characteristic does not divide n, so we conclude that $\zeta \in K$.) ∎

COROLLARY 3.13
Let E be an elliptic curve defined over $\mathbf{Q}$. Then $E[n] \not\subseteq E(\mathbf{Q})$ for $n \geq 3$.

PROOF If $E[n] \subseteq E(\mathbf{Q})$, then $\mu_n \subset \mathbf{Q}$, which is not the case when $n \geq 3$. ∎

REMARK 3.14 When $n = 2$, it is possible to have $E[2] \subseteq E(\mathbf{Q})$. For example, if E is given by $y^2 = x(x-1)(x+1)$, then

$$E[2] = \{\infty, (0,0), (1,0), (-1,0)\}.$$

If $n = 3, 4, 5, 6, 7, 8, 9, 10, 12$, there are elliptic curves E defined over $\mathbf{Q}$ that have points of order n with rational coordinates. However, the corollary says that it is not possible for all points of order n to have rational coordinates for these n. The torsion subgroups of elliptic curves over $\mathbf{Q}$ will be discussed in Chapter 8. ∎

We now use the Weil pairing to deduce two propositions that will be used in the proof of Hasse's theorem in Chapter 4. Recall that if α is an endomorphism of E, then we obtain a matrix $\alpha_n = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with entries in $\mathbf{Z}_n$, describing the action of α on a basis $\{T_1, T_2\}$ of $E[n]$.

PROPOSITION 3.15

Let α be an endomorphism of an elliptic curve E defined over a field K. Let n be a positive integer not divisible by the characteristic of K. Then $\det(\alpha_n) \equiv \deg(\alpha) \pmod{n}$.

PROOF By Corollary 3.10, $\zeta = e_n(T_1, T_2)$ is a primitive nth root of unity. By part (6) of Theorem 3.9, we have

$$\begin{aligned} \zeta^{\deg(\alpha)} &= e_n(\alpha(T_1), \alpha(T_2)) \;=\; e_n(aT_1 + cT_2, bT_1 + dT_2) \\ &= e_n(T_1, T_1)^{ab} e_n(T_1, T_2)^{ad} e_n(T_2, T_1)^{cb} e_n(T_2, T_2)^{cd} \\ &= \zeta^{ad-bc}, \end{aligned}$$

by the properties of the Weil pairing. Since ζ is a primitive nth root of unity, $\deg(\alpha) \equiv ad - bc \pmod{n}$. ∎

As we'll see in the proof of the next result, Proposition 3.15 allows us to reduce questions about the degree to calculations with matrices. Both Proposition 3.15 and Proposition 3.16 hold for all endomorphisms, since part (6) of Theorem 3.9 holds in general. However, we prove part (6) only for separable endomorphisms and for the Frobenius map, which is sufficient for our purposes. We'll state Proposition 3.16 in general, and the proof is sufficient for separable endomorphisms and for all endomorphisms of the form $r + s\phi_q$ with arbitrary integers r, s.

Let α and β be endomorphisms of E and let a, b be integers. The endomorphism $a\alpha + b\beta$ is defined by

$$(a\alpha + b\beta)(P) = a\alpha(P) + b\beta(P).$$

Here $a\alpha(P)$ means multiplication on E of $\alpha(P)$ by the integer a. The result is then added on E to $b\beta(P)$. This process can all be described by rational functions, since this is true for each of the individual steps. Therefore $a\alpha + b\beta$ is an endomorphism.

PROPOSITION 3.16

$$\deg(a\alpha + b\beta) = a^2 \deg\alpha + b^2 \deg\beta + ab(\deg(\alpha + \beta) - \deg\alpha - \deg\beta).$$

PROOF Let n be any integer not divisible by the characteristic of K. Represent α and β by matrices α_n and β_n (with respect to some basis of $E[n]$). Then $a\alpha_n + b\beta_n$ gives the action of $a\alpha + b\beta$ on $E[n]$. A straightforward calculation yields

$$\det(a\alpha_n + b\beta_n) = a^2 \det \alpha_n + b^2 \det \beta_n + ab(\det(\alpha_n + \beta_n) - \det \alpha_n - \det \beta_n)$$

for any matrices α_n and β_n (see Exercise 3.4). Therefore

$$\deg(a\alpha + b\beta) \equiv$$
$$a^2 \deg \alpha + b^2 \deg \beta + ab(\deg(\alpha + \beta) - \deg \alpha - \deg \beta) \pmod{n}.$$

Since this holds for infinitely many n, it must be an equality. ∎

3.4 The Tate-Lichtenbaum Pairing

Starting from the Weil pairing, it is possible to define a pairing that can be used in cases where the full n-torsion is not available, so the Weil pairing does not apply directly. The approach used in this section was inspired by work of Schaefer [96].

THEOREM 3.17
Let E be an elliptic curve over $\mathbf{F}_q$. Let n be an integer such that $n|q-1$. Denote by $E(\mathbf{F}_q)[n]$ the elements of $E(\mathbf{F}_q)$ of order dividing n, and let $\mu_n = \{x \in \mathbf{F}_q \,|\, x^n = 1\}$. Let $P \in E(\mathbf{F}_q)[n]$ and $Q \in E(\mathbf{F}_q)$ and choose $R \in E(\overline{\mathbf{F}}_q)$ satisfying $nR = Q$. Denote by e_n the nth Weil pairing and by $\phi = \phi_q$ the qth power Frobenius endomorphism. Define

$$\tau_n(P, Q) = e_n(P, R - \phi(R)).$$

Then

$$\tau_n : E(\mathbf{F}_q)[n] \times E(\mathbf{F}_q)/nE(\mathbf{F}_q) \longrightarrow \mu_n$$

is a well-defined nondegenerate bilinear pairing.

The pairing of the theorem is called the **modified Tate-Lichtenbaum pairing**. The original **Tate-Lichtenbaum pairing** is obtained by taking the nth root of τ_n, thus obtaining a pairing

$$\langle \cdot, \cdot \rangle_n : E(\mathbf{F}_q)[n] \times E(\mathbf{F}_q)/nE(\mathbf{F}_q) \longrightarrow \mathbf{F}_q^\times/(\mathbf{F}_q^\times)^n.$$

The pairing τ_n is better suited for computations since it gives a definite answer, rather than a coset in $\mathbf{F}_q^\times$ mod nth powers. These pairings can be computed

quickly (using at most a constant times $\log q$ point additions on E). See Section 11.4.

Technically, we should write $\tau_n(P,Q)$ as $\tau_n(P, Q+nE(\mathbf{F}_q))$, since an element of $E(\mathbf{F}_q)/nE(\mathbf{F}_q)$ has the form $Q + nE(\mathbf{F}_q)$. However, we'll simply write $\tau_n(P,Q)$ and similarly for $\langle P,Q\rangle_n$. The fact that τ_n is nondegenerate means that if $\tau_n(P,Q) = 1$ for all Q then $P = \infty$, and if $\tau_n(P,Q) = 1$ for all P then $Q \in nE(\mathbf{F}_q)$. Bilinearity means that

$$\tau_n(P_1 + P_1, Q) = \tau_n(P_1, Q)\tau_n(P_2, Q)$$

and

$$\tau_n(P, Q_1 + Q_2) = \tau_n(P, Q_1)\tau_n(P, Q_2).$$

PROOF We now prove the theorem. First, we need to show that $\tau_n(P,Q)$ is defined and is independent of the choice of R. Since $nR = Q \in E(\mathbf{F}_q)$, we have

$$\infty = Q - \phi(Q) = n\left(R - \phi R\right),$$

so $R - \phi R \in E[n]$ (to lower the number of parentheses, we often write ϕR instead of $\phi(R)$). Since $P \in E[n]$, too, the Weil pairing $e_n(P, R - \phi R)$ is defined. Suppose that $nR' = Q$ gives another choice of R. Let $T = R' - R$. Then $nT = Q - Q = \infty$, so $T \in E[n]$. Therefore,

$$\begin{aligned} e_n(P, R' - \phi R') &= e_n(P, R - \phi R + T - \phi T) \\ &= e_n(P, R - \phi R)e_n(P, T)/e_n(P, \phi T). \end{aligned}$$

But $P = \phi P$, since $P \in E(\mathbf{F}_q)$, so

$$e_n(P, \phi T) = e_n(\phi P, \phi T) = \phi\left(e_n(P, T)\right) = e_n(P, T),$$

since $e_n(P,T) \in \mu_n \subset \mathbf{F}_q$. Therefore,

$$e_n(P, R' - \phi R') = e_n(P, R - \phi R),$$

so τ_n does not depend on the choice of R.

Since Q is actually a representative of a coset in $E(\mathbf{F}_q)/nE(\mathbf{F}_q)$, we need to show that the value of τ_n depends only on the coset, not on the particular choice of representative. Therefore, suppose $Q' - Q = nU \in nE(\mathbf{F}_q)$. Let $nR = Q$ and let $R' = R + U$. Then $nR' = Q'$. We have

$$e_n(P, R' - \phi R') = e_n(P, R - \phi R + U - \phi U) = e_n(P, R - \phi R),$$

since $U = \phi U$ for $U \in E(\mathbf{F}_q)$. Therefore, the value does not depend on the choice of coset representative. This completes the proof that τ_n is well defined.

The fact that $\tau_n(P,Q)$ is bilinear in P follows immediately from the corresponding fact for e_n. For bilinearity in Q, suppose that $nR_1 = Q_1$ and

$nR_2 = Q_2$. Then $n(R_1 + R_2) = Q_1 + Q_2$, so

$$\begin{aligned}\tau_n(P, Q_1 + Q_2) &= e_n(P, R_1 + R_2 - \phi R_1 - \phi R_2) \\ &= e_n(P, R_1 - \phi R_1) e_n(P, R_2 - \phi R_2) \\ &= \tau_n(P, Q_1)\tau_n(P, Q_2).\end{aligned}$$

It remains to prove the nondegeneracy. This we postpone to Section 11.7. ∎

The Tate-Lichtenbaum pairing can be used in some situations where the Weil pairing does not apply. The Weil pairing needs $E[n] \subseteq E(\mathbf{F}_q)$, which implies that $\mu_n \subseteq \mathbf{F}_q^\times$, by Corollary 3.11. The Tate-Lichtenbaum pairing requires that $\mu_n \subseteq \mathbf{F}_q^\times$, but only needs a point of order n, rather than all of $E[n]$, to be in $E(\mathbf{F}_q)$. In fact, it doesn't even need a point of order n. If $E(\mathbf{F}_q)[n]$ is trivial, for example, then we have a pairing between two trivial groups.

Exercises

3.1 Let E be the elliptic curve $y^2 = x^3 + 1 \bmod 5$.

(a) Compute the division polynomial $\psi_3(x)$.

(b) Show that $\gcd(x^5 - x, \psi_3(x)) = x$.

(c) Use the result of part (b) to show that the 3-torsion points in $E(\mathbf{F}_5)$ are $\{\infty, (0, 1), (0, -1)\}$.

3.2 Let E be an elliptic curve in characteristic 2. Show that $E[3] \simeq \mathbf{Z}_3 \oplus \mathbf{Z}_3$. (*Hint:* Use the formulas at the end of Section 2.8.)

3.3 Let E be an elliptic curve over a field of characteristic not 2. Let $E[2] = \{\infty, P_1, P_2, P_3\}$. Show that $e_2(P_i, P_j) = -1$ whenever $i \neq j$.

3.4 Let M and N be 2×2 matrices with $N = \begin{pmatrix} w & x \\ y & z \end{pmatrix}$. Define $\tilde{N} = \begin{pmatrix} z & -x \\ -y & w \end{pmatrix}$ (this is the adjoint matrix).

(a) Show that $\text{Trace}(M\tilde{N}) = \det(M + N) - \det(M) - \det(N)$.

(b) Use (a) to show that

$$\begin{aligned}&\det(aM + bN) - a^2 \det M - b^2 \det N \\ &= ab(\det(M + N) - \det M - \det N)\end{aligned}$$

for all scalars a, b. This is the relation used in the proof of Proposition 3.16.

3.5 Show that part (6) of Theorem 3.9 holds when α is the endomorphism given by multiplication by an integer m.

3.6 Let E be an elliptic curve over a field K and let P be a point of order n (where n is not divisible by the characteristic of the field K). Let $Q \in E[n]$. Show that there exists an integer k such that $Q = kP$ if and only if $e_n(P, Q) = 1$.

3.7 Write the equation of the elliptic curve E as

$$F(x, y, z) = y^2z - x^3 - Axz^2 - Bz^3 = 0.$$

Show that a point P on E is in $E[3]$ if and only if

$$\det \begin{pmatrix} F_{xx} & F_{xy} & F_{xz} \\ F_{yx} & F_{yy} & F_{yz} \\ F_{zx} & F_{zy} & F_{zz} \end{pmatrix} = 0$$

at the point P, where F_{ab} denotes the 2nd partial derivative with respect to a, b. The determinant is called the *Hessian*. For a curve in $\mathbf{P}^2$ defined by an equation $F = 0$, a point where the Hessian is zero is called a *flex* of the curve.

3.8 The division polynomials ψ_n were defined for $n \geq 0$. Show that if we let $\psi_{-n} = -\psi_n$, then the recurrence relations preceding Lemma 3.3, which are stated only for $m \geq 2$, hold for all integers m. (Note that this requires verifying the relations for $m \leq -2$ and for $m = -1, 0, 1$.)