Chapter X

Computing the Mordell–Weil Group

A better title for this chapter might be "Computing the *Weak* Mordell–Weil Group," since we will be concerned solely with the problem of computing generators for the group $E(K)/mE(K)$. However, given generators for $E(K)/mE(K)$, a finite amount of computation yields generators for $E(K)$; see (VIII.3.2) and Exercise 8.18. Unfortunately, there is no comparable algorithm currently known that is guaranteed to give generators for $E(K)/mE(K)$ in a finite amount of time!

We start in (X §1) by taking the proof of the weak Mordell–Weil theorem given in (VIII §1) and making it quite explicit. In this way the computation of the quotient $E(K)/mE(K)$ (in a special case) is reduced to the problem of determining whether each of a certain finite set of auxiliary curves, called *homogeneous spaces*, has a single rational point. The question whether a given homogeneous space has a rational point may often be answered either affirmatively by finding a point or negatively by showing that it has no points in some completion K_v of K.

The subsequent two sections develop the general theory of homogeneous spaces (for elliptic curves). Then, in (X §4), we apply this theory to the problem of computing $E(K)/mE(K)$ or, more generally, $E'(K)/\phi\big(E(K)\big)$ for an isogeny

$$\phi : E \to E'.$$

Again this computation is reduced to the problem of the existence of a single rational point on certain homogeneous spaces. The only impediment to solving this latter problem occurs if some homogeneous space has a K_v-rational point for every completion K_v of K, yet fails to have a K-rational point. Unfortunately, this precise situation, the failure of the so-called Hasse principle, does occur. The extent of its failure is quantified by the elements of a certain group, called the *Shafarevich–Tate group*. The question of an effective algorithm for the computation of $E(K)/mE(K)$ is thus finally reduced to the problem of giving a bound for divisibility in the Shafarevich–Tate group, or, even better, proving the conjecture that the Shafarevich–Tate group is finite.

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

In the last section we illustrate the general theory by studying in some detail the family of elliptic curves given by the equations

$$E_D : Y^2 = X^3 + DX, \qquad D \in \mathbb{Q}.$$

In particular, we compute the torsion subgroups and give an upper bound for the rank of $E_D(\mathbb{Q})$, we give a large class of examples for which $E_D(\mathbb{Q})$ has rank 0, and we show that in certain cases $E_D(\mathbb{Q})$ has an associated homogeneous space that violates the Hasse principle, i.e., the homogeneous space has points defined over $\mathbb{R}$ and over $\mathbb{Q}_p$ for every prime p, but it has no $\mathbb{Q}$-rational points.

Unless explicitly stated to the contrary, the notation for this chapter is the same as for Chapter VIII. In particular, K is a number field and M_K is a complete set of inequivalent absolute values on K. However, as indicated in the text, this specification is dropped in (X §§2,3,5), where K is allowed to be an arbitrary (perfect) field.

X.1 An Example

For this section we let E/K be an elliptic curve and $m \geq 2$ an integer, and we assume that

$$E[m] \subset E(K).$$

Recall from (VIII §1) that under this assumption there is a pairing

$$\kappa : E(K) \times G_{\bar{K}/K} \longrightarrow E[m]$$

defined by

$$\kappa(P, \sigma) = Q^\sigma - Q,$$

where $Q \in E(\bar{K})$ is chosen to satisfy $[m]Q = P$. Further, (VIII.1.2) says that the kernel on the left is $mE(K)$, so we may view κ as a homomorphism

$$\delta_E : E(K)/mE(K) \longrightarrow \operatorname{Hom}\bigl(G_{\bar{K}/K}, E[m]\bigr),$$
$$\delta_E(P)(\sigma) = \kappa(P, \sigma).$$

(This is the connecting homomorphism for a group cohomology long exact sequence; see (VIII §2).)

We also observe from (III.8.1.1) that our assumption $E[m] \subset E(K)$ implies that $\boldsymbol{\mu}_m \subset K^*$. This follows from basic properties of the Weil pairing (III.8.1.1),

$$e_m : E[m] \times E[m] \longrightarrow \boldsymbol{\mu}_m.$$

The Weil pairing will play a prominent role in this section.

Finally, since $\boldsymbol{\mu}_m \subset K^*$, Hilbert's Theorem 90 (B.2.5c) says that every homomorphism $G_{\bar{K}/K} \to \boldsymbol{\mu}_m$ has the form

$$\sigma \longmapsto \frac{\beta^\sigma}{\beta} \quad \text{for some } \beta \in \bar{K}^* \text{ satisfying } \beta^m \in K^*.$$

In other words, there is an isomorphism (cf. VIII §2)

$$\delta_K : K^*/(K^*)^m \longrightarrow \operatorname{Hom}(G_{\bar{K}/K}, \boldsymbol{\mu}_m)$$

defined by

$$\delta_K(b)(\sigma) = \beta^\sigma/\beta,$$

where $\beta \in \bar{K}^*$ is chosen to satisfy $\beta^m = b$. Note the close resemblance in the definitions of δ_E and δ_K. This is no coincidence. The map δ_E is the connecting homomorphism for the Kummer sequence associated to the group variety E/K, and δ_K is the connecting homomorphism for the Kummer sequence associated to the group variety $\mathbb{G}_m/K$.

Using these maps, we can make the proof of the weak Mordell–Weil theorem much more explicit, and by doing so, derive formulas that allow us to compute the Mordell–Weil group in certain cases. We start with a theoretical description of the method.

Theorem 1.1. (a) *With notation as above, there is a bilinear pairing*

$$b : E(K)/mE(K) \times E[m] \longrightarrow K^*/(K^*)^m$$

satisfying

$$e_m\bigl(\delta_E(P), T\bigr) = \delta_K\bigl(b(P,T)\bigr).$$

(b) *The pairing in* (a) *is nondegenerate on the left.*

(c) *Let $S \subset M_K$ be the union of the set of infinite places, the set of finite primes at which E has bad reduction, and the set of finite primes dividing m. Then the image of the pairing in* (a) *lies in the following subgroup of $K^*/(K^*)^m$:*

$$K(S,m) = \bigl\{b \in K^*/(K^*)^m : \operatorname{ord}_v(b) \equiv 0 \pmod{m} \textit{ for all } v \notin S\bigr\}.$$

(d) *The pairing in* (a) *may be computed as follows. For each $T \in E[m]$, choose functions $f_T, g_T \in K(E)$ satisfying the conditions*

$$\operatorname{div}(f_T) = m(T) - m(O) \qquad \textit{and} \qquad f_T \circ [m] = g_T^m$$

(*cf. the definition of the Weil pairing* (III §8)). *Then for any point $P \neq T$,*

$$b(P,T) \equiv f_T(P) \pmod{(K^*)^m}.$$

(*If $P = T$, we can compute $b(T,T)$ using linearity. For example, if $[2]T \neq O$, then $b(T,T) = f_T(-T)^{-1}$. More generally, let $Q \in E(K)$ be any point with $Q \neq T$; then $b(T,T) = f_T(T+Q)f_T(Q)^{-1}$.*)

Remark 1.2. Why do we say that (X.1.1) provides formulas that help us to compute the Mordell–Weil group? First, the group $K(S,m)$ in (c) is finite (see the proof of (VIII.1.6)), and in fact it is reasonably easy to explicitly compute $K(S,m)$. Second, the functions f_T in (d) are also fairly easy to compute from the equation of the curve. (This is true even for quite large values of m; see (XI.8.1).) Then the fact that the pairing in (a) is nondegenerate on the left means that in order to compute $E(K)/mE(K)$, it is necessary to do "only" the following:

Fix generators T_1 and T_2 for $E[m]$. For each of the finitely many pairs

$$(b_1, b_2) \in K(S,m) \times K(S,m),$$

check whether the simultaneous equations

$$b_1 z_1^m = f_{T_1}(P) \qquad \text{and} \qquad b_2 z_2^m = f_{T_2}(P)$$

have a solution $(P, z_1, z_2) \in E(K) \times K^* \times K^*$. We can be even more explicit if we express the function f_T in terms of Weierstrass coordinates x and y. Then we are looking for a solution $(x, y, z_1, z_2) \in K \times K \times K^* \times K^*$ satisfying

$$\begin{gathered} y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \\ b_1 z_1^m = f_{T_1}(x,y), \qquad b_2 z_2^m = f_{T_2}(x,y). \end{gathered}$$

These equations define a new curve, called a *homogeneous space for E/K*. (We discuss homogeneous spaces in more detail in (X §3).) What we have done is reduce the problem of calculating $E(K)/mE(K)$ to the problem of the existence or nonexistence of a single rational point on each of an explicitly given finite set of curves. Frequently, many of these curves can be immediately eliminated from consideration because they have no points over some completion K_v of K, which is an easy thing to check. On the other hand, a short search by hand or with a computer often uncovers rational points on some of the others. If, in this way, we can deal with all of the homogeneous spaces in question, then the determination of $E(K)/mE(K)$ is complete. The problem that arises is that occasionally there is a homogeneous space having points defined over every completion K_v, yet having no K-rational points. It is this situation, the failure of the Hasse principle, that makes the Mordell–Weil theorem ineffective.

Remark 1.3. Notice that the condition $\operatorname{div}(f_T) = m(T) - m(O)$ in (X.1.1d) is enough to specify f_T only up to multiplication by an arbitrary element of K^*. However, the equality $f_T \circ [m] = g_T^m$ with $g_T \in K(E)$ means that in fact f_T is well-determined up to multiplication by an element of $(K^*)^m$. Thus the value of $f_T(P)$ in (X.1.1d) is a well-defined element of $K^*/(K^*)^m$.

We now give the proof of (X.1.1), after which we study the case $m = 2$ in more detail and use it to compute $E(K)/2E(K)$ for an example.

PROOF OF (X.1.1). (a) Hilbert's Theorem 90 (B.2.5c) shows that the pairing is well-defined. Bilinearity follows from bilinearity of the Kummer pairing (VIII.1.2b) and bilinearity of the Weil e_m-pairing (III.8.1a).

(b) In order to prove nondegeneracy on the left, we suppose that $b(P,T) = 1$ for all $T \in E[m]$. This means that for all $T \in E[m]$ and all $\sigma \in G_{\bar{K}/K}$,

$$e_m\big(\kappa(P,\sigma), T\big) = 1.$$

The nondegeneracy of the Weil pairing (III.8.1c) implies that $\kappa(P,\sigma)=0$ for all σ, and then (VIII.1.2c) tells us that $P \in mE(K)$.
(c) Let $\beta = b(P,T)^{1/m}$. Tracing through the definitions, we see that the field $K(\beta)$ is contained in the field $K\bigl([m]^{-1}E(K)\bigr)$ described in (VIII.1.2d). Further, applying (VIII.1.5b) tells us that the extension L/K is unramified outside S. But it is easy to see that if $v \in M_K$ is a finite place with $v(m)=0$, then the extension $K(\beta)/K$ is unramified at v if and only if

$$\operatorname{ord}_v(\beta^m) \equiv 0 \pmod{m}.$$

(Here $\operatorname{ord}_v : K^* \twoheadrightarrow \mathbb{Z}$ is the normalized valuation associated to v.) This says precisely that $b(P,T) \in K(S,m)$.
(d) Choose $Q \in E(\bar{K})$ and $\beta \in \bar{K}^*$ satisfying

$$P = [m]Q \qquad \text{and} \qquad b(P,T) = \beta^m.$$

Then for all $\sigma \in G_{\bar{K}/K}$ we have by definition

$$\begin{aligned} e_m\bigl(\delta(P)(\sigma),T\bigr) &= \delta_K\bigl(b(P,T)\bigr)(\sigma), \\ e_m(Q^\sigma - Q,T) &= \beta^\sigma/\beta, \\ g_T(X+Q^\sigma-Q)/g_T(X) &= \beta^\sigma/\beta, \\ g_T(Q)^\sigma/g_T(Q) &= \beta^\sigma/\beta \qquad \text{putting } X=Q. \end{aligned}$$

Since δ_K is an isomorphism, it follows that $g_T(Q)^m \equiv \beta^m \pmod{(K^*)^m}$. (Note that $g_T(Q)^m = f_T(P)$ is in K^*.) Therefore

$$f_T(P) = f_T \circ [m](Q) = g_T(Q)^m \equiv \beta^m = b(P,T) \pmod{(K^*)^m}. \qquad \square$$

We now consider the special case $m=2$, which is by far the easiest with which to work. Under our assumption $E[m] \subset E(K)$, we may take a Weierstrass equation for E of the form

$$y^2 = (x-e_1)(x-e_2)(x-e_3) \qquad \text{with } e_1,e_2,e_3 \in K.$$

The three nontrivial 2-torsion points are

$$T_1 = (e_1,0), \quad T_2 = (e_2,0), \quad T_3 = (e_3,0).$$

Letting $T=(e,0)$ represent any one of these points, we claim that the associated function f_T specified in (X.1.1d) is $f_T = x-e$. It is clear that this function has the correct divisor,

$$\operatorname{div}(x-e) = 2(T) - 2(O).$$

It is then a calculation to check that

$$x \circ [2] = \left(\frac{x^2 - 2ex - 2e^2 + 2(e_1+e_2+e_3)e - (e_1e_2+e_1e_3+e_2e_3)}{2y}\right)^2,$$

so $x - e$ has both of the properties needed to be f_T.

Now suppose that we have chosen a pair $(b_1, b_2) \in K(S,m) \times K(S,m)$ and that we want to determine whether there is a point $P \in E(K)/2E(K)$ satisfying

$$b(P,T_1) = b_1 \qquad \text{and} \qquad b(P,T_2) = b_2.$$

Such a point exists if and only if there is a solution

$$(x, y, z_1, z_2) \in K \times K \times K^* \times K^*$$

to the system of equations

$$y^2 = (x-e_1)(x-e_2)(x-e_3), \qquad b_1 z_1^2 = x - e_1, \qquad b_2 z_2^2 = x - e_2.$$

We substitute the latter two equations into the former and define a new variable z_3 by $y = b_1 b_2 z_1 z_2 z_3$, which is permissible since b_1, b_2, z_1, and z_2 take only nonzero values. This yields the three equations

$$b_1 b_2 z_3^2 = x - e_3, \qquad b_1 z_1^2 = x - e_1, \qquad b_2 z_2^2 = x - e_2.$$

Finally, eliminating x gives the pair of equations

$$b_1 z_1^2 - b_2 z_2^2 = e_2 - e_1, \qquad b_1 z_1^2 - b_1 b_2 z_3^2 = e_3 - e_1.$$

This gives a finite collection of equations, one for each pair (b_1, b_2), and we may use whatever techniques are at our disposal (e.g., v-adic, computer search) to determine whether they have a solution. Notice that if we do find a solution (z_1, z_2, z_3), then we immediately recover the corresponding point in $E(K)/2E(K)$ using the formulas

$$x = b_1 z_1^2 + e_1, \qquad y = b_1 b_2 z_1 z_2 z_3.$$

Finally we must deal with the fact that the definition $b(P,T) = f_T(P)$ cannot be used if it happens that $P = T$. In other words, there are two pairs (b_1, b_2) that do not arise from the above procedure, namely the pairs $\bigl(b(T_1,T_1), b(T_1,T_2)\bigr)$ and $\bigl(b(T_2,T_1), b(T_2,T_2)\bigr)$. These values may be computed using linearity as

$$\begin{aligned} b(T_1,T_1) &= b(T_1, T_1 + T_2) b(T_1,T_2)^{-1} \\ &= b(T_1,T_3) b(T_1,T_2)^{-1} \\ &= \frac{e_1 - e_3}{e_1 - e_2}, \end{aligned}$$

and similarly

$$b(T_2,T_2) = \frac{e_2 - e_3}{e_2 - e_1}.$$

We summarize this entire procedure in the following proposition.

Proposition 1.4. (Complete 2-Descent) *Let E/K be an elliptic curve given by a Weierstrass equation*

$$y^2 = (x-e_1)(x-e_2)(x-e_3) \qquad \textit{with } e_1, e_2, e_3 \in K.$$

Let $S \subset M_K$ be a finite set of places of K including all archimedean places, all places dividing 2, and all places at which E has bad reduction. Further let

$$K(S,2) = \bigl\{ b \in K^*/(K^*)^2 : \operatorname{ord}_v(b) \equiv 0 \ (\operatorname{mod} 2) \textit{ for all } v \notin S \bigr\}.$$

Then there is an injective homomorphism

$$E(K)/2E(K) \longrightarrow K(S,2) \times K(S,2)$$

defined by

$$P = (x,y) \longmapsto \begin{cases} (x-e_1, x-e_2) & \textit{if } x \ne e_1, e_2, \\ \left(\dfrac{e_1-e_3}{e_1-e_2}, e_1-e_2 \right) & \textit{if } x = e_1, \\ \left(e_2-e_1, \dfrac{e_2-e_3}{e_2-e_1} \right) & \textit{if } x = e_2, \\ (1,1) & \textit{if } x = \infty, \textit{ i.e., if } P = O. \end{cases}$$

Let $(b_1, b_2) \in K(S,2) \times K(S,2)$ be a pair that is not the image of one of the three points O, $(e_1, 0)$, $(e_2, 0)$. Then (b_1, b_2) is the image of a point

$$P = (x,y) \in E(K)/2E(K)$$

if and only if the equations

$$\begin{aligned} b_1 z_1^2 - b_2 z_2^2 &= e_2 - e_1, \\ b_1 z_1^2 - b_1 b_2 z_3^2 &= e_3 - e_1, \end{aligned}$$

have a solution $(z_1, z_2, z_3) \in K^* \times K^* \times K$. If such a solution exists, then we can take

$$P = (x,y) = (b_1 z_1^2 + e_1, b_1 b_2 z_1 z_2 z_3).$$

PROOF. As explained above, this is a special case of (X.1.1). □

Example 1.5. We use (X.1.4) to compute $E(\mathbb{Q})/2E(\mathbb{Q})$ for the elliptic curve

$$E : y^2 = x^3 - 12x^2 + 20x = x(x-2)(x-10).$$

This equation has discriminant

$$\Delta = 409600 = 2^{14} 5^2,$$

so it has good reduction except at 2 and 5. Reducing the equation modulo 3, we easily check that $\#\tilde{E}(\mathbb{F}_3) = 4$. Since $E[2] \subset E_{\text{tors}}(\mathbb{Q})$ and $E_{\text{tors}}(\mathbb{Q})$ injects into $\tilde{E}(\mathbb{F}_3)$ from (VII.3.5), we see that

$$E_{\text{tors}}(\mathbb{Q}) = E[2].$$

Let $S = \{2, 5, \infty\} \subset M_{\mathbb{Q}}$. Then a complete set of representatives for

$$\mathbb{Q}(S, 2) = \bigl\{b \in \mathbb{Q}^*/(\mathbb{Q}^*)^2 : \operatorname{ord}_p(b) \equiv 0 \pmod 2 \text{ for all } p \notin S\bigr\}$$

is given by the set

$$\{\pm 1, \pm 2, \pm 5, \pm 10\}.$$

We identify this set with $\mathbb{Q}(S, 2)$. Now consider the map given in (X.1.4),

$$E(\mathbb{Q})/2E(\mathbb{Q}) \longrightarrow \mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2),$$

say with

$$e_1 = 0, \qquad e_2 = 2, \qquad \text{and} \qquad e_3 = 10.$$

There are 64 pairs $(b_1, b_2) \in \mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2)$, and for each pair, we must check to see whether it comes from an element of $E(\mathbb{Q})/2E(\mathbb{Q})$. For example, using (X.1.4), we can compute the image of $E[2]$ in $\mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2)$:

$$O \mapsto (1, 1), \qquad (0, 0) \mapsto (5, -2), \qquad (2, 0) \mapsto (2, -1), \qquad (10, 0) \mapsto (10, 2).$$

It remains to determine, for every other pair (b_1, b_2), whether the equations

$$b_1 z_1^2 - b_2 z_2^2 = 2, \qquad b_1 z_1^2 - b_1 b_2 z_3^2 = 10, \tag{$*$}$$

have a solution $z_1, z_2, z_3 \in \mathbb{Q}$. For example, if $b_1 < 0$ and $b_2 > 0$, then ($*$) clearly has no rational solutions, since the first equation does not even have a solution in $\mathbb{R}$.

Proceeding systematically, we list our results in Table 10.1. The entry for each pair (b_1, b_2) consists of either a point of $E(\mathbb{Q})$ that maps to (b_1, b_2), or else a (local) field over which the equations listed in ($*$) have no solution. (Note that if (z_1, z_2, z_3) is a solution to ($*$), then the corresponding point of $E(\mathbb{Q})$ is $(b_1 z_1^2 + e_1, b_1 b_2 z_1 z_2 z_3)$.) The circled numbers in the table refer to the notes that explain each entry. Finally, we note that since the map $E(\mathbb{Q})/2E(\mathbb{Q}) \to \mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2)$ is a *homomorphism*, it is not necessary to check every pair (b_1, b_2). For example, if both (b_1, b_2) and (b_1', b_2') come from $E(\mathbb{Q})$, then so does $(b_1 b_1', b_2 b_2')$. Similarly, if (b_1, b_2) does and (b_1', b_2') does not, then $(b_1 b_1', b_2 b_2')$ does not. This observation substantially reduces the number of cases of ($*$) that must be considered.

1. If $b_1 < 0$ and $b_2 > 0$, then $b_1 z_1^2 - b_2 z_2^2 = 2$ has no solutions in $\mathbb{R}$.

2. If $b_1 < 0$ and $b_2 < 0$, then $b_1 z_1^2 - b_1 b_2 z_3^2 = 10$ has no solutions in $\mathbb{R}$.

3. The four 2-torsion points $\bigl\{O, (0, 0), (2, 0), (10, 0)\bigr\}$ map respectively to the four points $(1, 1)$, $(5, -2)$, $(2, -1)$, and $(10, 2)$.

4. $(b_1, b_2) = (1, -1)$: By inspection, the equations

$$z_1^2 + z_2^2 = 2 \qquad \text{and} \qquad z_1^2 + z_3^2 = 10$$

have the solution $(1, 1, 3)$. This gives the point $(1, -3) \in E(\mathbb{Q})$.

b_1 b_2	1	2	5	10	-1 -2 -5 -10
1	0	$(18,-48)$ ⑤	$\mathbb{Q}_5$ ⑨		$\mathbb{R}$ ①
2	$\mathbb{Q}_5$ ⑧	$\mathbb{Q}_5$ ⑨	$(20,60)$ ⑤	$(10,0)$ ③	
5 10	$\mathbb{Q}_5$ ⑥		$\mathbb{Q}_5$ ⑦		
-1	$(1,-3)$ ④	$(2,0)$ ③	$\mathbb{Q}_5$ ⑨		$\mathbb{R}$ ②
-2	$\mathbb{Q}_5$ ⑨		$(0,0)$ ③	$(\frac{10}{9},-\frac{80}{27})$ ⑤	
-5 -10	$\mathbb{Q}_5$ ⑥		$\mathbb{Q}_5$ ⑦		

Table 10.1: Computing $E(\mathbb{Q})$ for $E : y^2 = x^3 - 12x^2 + 20x$.

5. Adding $(1,-3) \in E(\mathbb{Q})$ to the nontrivial two-torsion points corresponds to multiplying their (b_1,b_2) values. This gives three pairs $(5,2)$, $(2,1)$, and $(10,-2)$ in $\mathbb{Q}(S,2) \times \mathbb{Q}(S,2)$, which correspond to the three rational points $(20,60)$, $(18,-48)$, and $(10/9,-80/27)$ in $E(\mathbb{Q})$.

6. $b_1 \not\equiv 0 \pmod 5$ and $b_2 \equiv 0 \pmod 5$: The first equation in $(*)$ implies that z_1 and z_2 must be 5-adically integral. Then the second equation shows that $z_1 \equiv 0 \pmod 5$, and so from the first equation we obtain $0 \equiv 2 \pmod 5$. Therefore $(*)$ has no solutions in $\mathbb{Q}_5$.

7. The eight pairs in (6) are $\mathbb{Q}_5$-nontrivial, i.e., there are no $\mathbb{Q}_5$ solutions to $(*)$. If we multiply these eight pairs by the $\mathbb{Q}$-trivial pair $(5,2)$, we obtain eight more $\mathbb{Q}_5$-nontrivial pairs.

8. $(b_1,b_2) = (1,2)$: The two equations in $(*)$ are
$$z_1^2 - 2z_2^2 = 2 \qquad \text{and} \qquad z_1^2 - 2z_3^2 = 10.$$
Since 2 is a quadratic nonresidue modulo 5, the second equation implies that $z_1 \equiv z_3 \equiv 0 \pmod 5$. But then the second equation says that $0 \equiv 10 \pmod{25}$. Therefore there are no solutions in $\mathbb{Q}_5$.

9. Taking the $\mathbb{Q}_5$-nontrivial pair $(1,2)$ from (8) and multiplying it by the seven $\mathbb{Q}$-trivial pairs already in the table gives seven new $\mathbb{Q}_5$-nontrivial pairs that fill the remaining entries in the table.

Conclusion. $E(\mathbb{Q}) \cong \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

X.2 Twisting—General Theory

For this section and the next we drop the requirement that K be a number field, so K will be an arbitrary (perfect) field. As we saw in (X §1), computation of the Mordell–Weil group of an elliptic curve E leads naturally to the problem of the existence or nonexistence of a single rational point on various other curves. These other curves are certain *twists* of E that are called *homogeneous spaces*. In this section we study the general question of twisting which, since it is no more difficult, we develop for curves of arbitrary genus. Then, in the next section, we look at the homogeneous spaces associated to elliptic curves.

Definition. Let C/K be a smooth projective curve. The *isomorphism group of* C, denoted by $\operatorname{Isom}(C)$, is the group of $\bar{K}$-isomorphisms from C to itself. We denote the subgroup of $\operatorname{Isom}(C)$ consisting of isomorphisms defined over K by $\operatorname{Isom}_K(C)$. To ease notation, we write composition of maps multiplicatively, thus $\alpha\beta$ instead of $\alpha \circ \beta$.

Remark 2.1. The group that we are denoting by $\operatorname{Isom}(C)$ is usually called the *automorphism group of* C and denoted by $\operatorname{Aut}(C)$. However, if E is an elliptic curve, then we have defined $\operatorname{Aut}(E)$ to be the group of isomorphisms from E to E that take O to O. Thus $\operatorname{Aut}(E) \neq \operatorname{Isom}(E)$, since for example, the group $\operatorname{Isom}(E)$ contains translation maps $\tau_P : E \to E$. We describe $\operatorname{Isom}(E)$ more fully in (X §5).

Definition. A *twist of* C/K is a smooth curve C'/K that is isomorphic to C over $\bar{K}$. We treat two twists as equivalent if they are isomorphic over K. The set of twists of C/K, modulo K-isomorphism, is denoted by $\operatorname{Twist}(C/K)$.

Let C'/K be a twist of C/K. Thus there is an isomorphism $\phi : C' \to C$ defined over $\bar{K}$. To measure the failure of ϕ to be defined over K, we consider the map

$$\xi : G_{\bar{K}/K} \longrightarrow \operatorname{Isom}(C), \qquad \xi_\sigma = \phi^\sigma \phi^{-1}.$$

It turns out that ξ is a 1-cocycle and that the cohomology class of ξ is uniquely determined by the K-isomorphism class of C'. Further, every cohomology class comes from some twist of C/K. In this way $\operatorname{Twist}(C/K)$ may be identified with a certain cohomology set. We now prove these assertions.

Theorem 2.2. *Let C/K be a smooth projective curve. For each twist C'/K of C/K, choose a $\bar{K}$-isomorphism $\phi : C' \to C$ and define a map $\xi_\sigma = \phi^\sigma\phi^{-1} \in \operatorname{Isom}(C)$ as above.*

(a) *The map ξ is a 1-cocycle, i.e.,*

$$\xi_{\sigma\tau} = (\xi_\sigma)^\tau \xi_\tau \qquad \textit{for all } \sigma, \tau \in G_{\bar{K}/K}.$$

The associated cohomology class in $H^1\big(G_{\bar{K}/K}, \operatorname{Isom}(C)\big)$ is denoted by $\{\xi\}$.

(b) *The cohomology class $\{\xi\}$ is determined by the K-isomorphism class of C' and is independent of the choice of ϕ. We thus obtain a natural map*

$$\operatorname{Twist}(C/K) \longrightarrow H^1\big(G_{\bar{K}/K}, \operatorname{Isom}(C)\big).$$

(c) *The map in* (b) *is a bijection. In other words, the twists of C/K, up to K-isomorphism, are in one-to-one correspondence with the elements of the cohomology set $H^1\big(G_{\bar{K}/K}, \operatorname{Isom}(C)\big)$.*

Remark 2.3. We emphasize that the group $\operatorname{Isom}(C)$ is often nonabelian, and indeed, it is always nonabelian for elliptic curves. Hence $H^1\big(G_{\bar{K}/K}, \operatorname{Isom}(C)\big)$ is generally only a *pointed set*, not a group. See (B §3) for details. However, if $\operatorname{Isom}(C)$ has a $G_{\bar{K}/K}$-invariant abelian subgroup A, then $H^1(G_{\bar{K}/K}, A)$ is a group, and its image in $H^1\big(G_{\bar{K}/K}, \operatorname{Isom}(C)\big)$ gives a natural group structure to some subset of $\operatorname{Twist}(C)$. We apply this observation in (X §3) when C is an elliptic curve, taking for A the group of translations, and in (X §5) we do the same with $A = \operatorname{Aut}(E)$.

PROOF. (a) We compute

$$\xi_{\sigma\tau} = \phi^{\sigma\tau}\phi^{-1} = (\phi^\sigma\phi^{-1})^\tau(\phi^\tau\phi^{-1}) = (\xi_\sigma)^\tau\xi_\tau.$$

(b) Let C''/K be another twist of C/K that is K-isomorphic to C'. Choose a $\bar{K}$-isomorphism $\psi : C'' \to C$. We must show that the cocycles $\phi^\sigma\phi^{-1}$ and $\psi^\sigma\psi^{-1}$ are cohomologous. By assumption there is a K-isomorphism $\theta : C'' \to C'$. Consider the element $\alpha = \phi\theta\psi^{-1} \in \operatorname{Isom}(C)$. We compute

$$\begin{aligned}(\alpha^\sigma)(\psi^\sigma\psi^{-1}) &= (\phi\theta\psi^{-1})^\sigma(\psi^\sigma\psi^{-1}) = \phi^\sigma\theta^\sigma\psi^{-1}\\ &= \phi^\sigma\theta\psi^{-1} = (\phi^\sigma\phi^{-1})(\phi\theta\psi^{-1}) = (\phi^\sigma\phi^{-1})\alpha.\end{aligned}$$

This proves that $\phi^\sigma\phi^{-1}$ and $\psi^\sigma\psi^{-1}$ are cohomologous when viewed as elements of $H^1\big(G_{\bar{K}/K}, \operatorname{Isom}(C)\big)$.

(c) Suppose that C'/K and C''/K are twists of C/K that give the same cohomology class in $H^1\big(G_{\bar{K}/K}, \operatorname{Isom}(C)\big)$. This means that if we choose $\bar{K}$-isomorphisms $\phi : C' \to C$ and $\psi : C'' \to C$, then there is a map $\alpha \in \operatorname{Isom}(C)$ such that

$$\alpha^\sigma(\psi^\sigma\psi^{-1}) = (\phi^\sigma\phi^{-1})\alpha \qquad \text{for all } \sigma \in G_{\bar{K}/K}.$$

In other words, the cocycles associated to ϕ and ψ are cohomologous. We now consider the map $\theta : C'' \to C'$ defined by $\theta = \phi^{-1}\alpha\psi$. It is clearly a $\bar{K}$-isomorphism, and we claim that it is, in fact, defined over K. To prove this, for any $\sigma \in G_{\bar{K}/K}$ we compute

$$\theta^\sigma = (\phi^\sigma)^{-1}(\alpha^\sigma\psi^\sigma) = (\phi^\sigma)^{-1}(\phi^\sigma\phi^{-1}\alpha\psi) = \phi^{-1}\alpha\psi = \theta.$$

Therefore C'' and C' are K-isomorphic, and thus they give the same element of $\operatorname{Twist}(C/K)$. This proves that the map

$$\operatorname{Twist}(C/K) \to H^1\big(G_{\bar{K}/K}, \operatorname{Isom}(C)\big)$$

is injective.

To prove surjectivity, we start with a 1-cocycle

$$\xi : G_{\bar{K}/K} \to \operatorname{Isom}(C)$$

and use it to construct a curve C'/K and an isomorphism $\phi : C' \to C$ satisfying $\xi_\sigma = \phi^\sigma \phi^{-1}$. To do this, we consider a field, denoted by $\bar{K}(C)_\xi$, that is isomorphic, as an abstract field extension of $\bar{K}$, to $\bar{K}(C)$, say by an isomorphism that we denote by $Z : \bar{K}(C) \to \bar{K}(C)_\xi$. The difference between $\bar{K}(C)$ and $\bar{K}(C)_\xi$ lies in the action of the Galois group $G_{\bar{K}/K}$; the action on $\bar{K}(C)_\xi$ is *twisted by* ξ. What this means is that

$$Z(f)^\sigma = Z(f^\sigma \xi_\sigma) \qquad \text{for all } f \in \bar{K}(C) \text{ and all } \sigma \in G_{\bar{K}/K}.$$

In this equality we are viewing f as a map $f : C \to \mathbb{P}^1$ as in (II.2.2), and $f^\sigma \xi_\sigma$ is composition of maps. Equivalently, the map $\xi_\sigma : C \to C$ of curves induces a map $\xi_\sigma^* : \bar{K}(C) \to \bar{K}(C)$ of fields, and $f^\sigma \xi_\sigma$ is an alternative notation for $\xi_\sigma^*(f^\sigma)$.

For this action of $G_{\bar{K}/K}$ on $\bar{K}(C)_\xi$, we consider the subfield $\mathcal{F} \subset \bar{K}(C)_\xi$ consisting of the elements of $\bar{K}(C)_\xi$ that are fixed by $G_{\bar{K}/K}$. We now show, in several steps, that the field $\mathcal{F}$ is the function field of the desired twist of C.

$\boxed{\text{Step (i): } \mathcal{F} \cap \bar{K} = K}$

Suppose that $Z(f) \in \mathcal{F} \cap \bar{K}$. In particular, since Z induces the identity on $\bar{K}$, we have $f \in \bar{K}$. Now the fact that $Z(f) \in \mathcal{F}$, combined with the fact that f is a constant function and thus unaffected by isomorphisms of C, implies that

$$Z(f) = Z(f)^\sigma = Z(f^\sigma \xi_\sigma) = Z(f^\sigma).$$

This holds for all $\sigma \in G_{\bar{K}/K}$, and hence $f \in K$.

$\boxed{\text{Step (ii): } \bar{K}\mathcal{F} = \bar{K}(C)_\xi}$

This is an immediate consequence of (II.5.8.1) applied to the $\bar{K}$-vector space $\bar{K}(C)_\xi$.

It follows from Step (ii) that $\mathcal{F}$ has transcendence degree one over K, and thus using Step (i) and (II.2.4c), we deduce that there exists a smooth curve C'/K such that $\mathcal{F} \cong K(C')$. Further, Step (ii) implies that

$$\bar{K}(C') = \bar{K}\mathcal{F} = \bar{K}(C)_\xi \cong \bar{K}(C),$$

so (II.2.4.1) says that C' and C are isomorphic over $\bar{K}$. In other words, C' is a twist of C, and the final step in proving surjectivity is to show that C' gives the cohomology class $\{\xi\}$.

Let $\phi : C' \to C$ be a $\bar{K}$-isomorphism, as described in (II.2.4b), whose associated map ϕ^* is the isomorphism of fields

$$Z : \bar{K}(C) \longrightarrow \bar{K}(C)_\xi = \bar{K}\mathcal{F} = \bar{K}(C').$$

$\boxed{\text{Step (iii): } \xi_\sigma = \phi^\sigma \phi^{-1} \text{ for all } \sigma \in G_{\bar{K}/K}}$

Having identified ϕ^* with Z, the relation $Z(f)^\sigma = Z(f^\sigma \xi_\sigma)$ used to define the map Z can be rewritten as $(f\phi)^\sigma = f^\sigma \xi_\sigma \phi$. In other words,

$$f^\sigma \phi^\sigma = (f\phi)^\sigma = f^\sigma \xi_\sigma \phi \qquad \text{for all } f \in \bar{K}(C).$$

This implies that $\phi^\sigma = \xi_\sigma \phi$, which is exactly the desired result. □

Example 2.4. Let E/K be an elliptic curve, let $K(\sqrt{d}\,)$ be a quadratic extension of K, and let

$$\chi : G_{\bar{K}/K} \to \{\pm 1\}, \qquad \chi(\sigma) = \sqrt{d}^{\,\sigma}/\sqrt{d},$$

be the quadratic character associated to $K(\sqrt{d}\,)/K$. (Note that $\operatorname{char}(K) \ne 2$.) We use χ to define a 1-cocycle

$$\xi : G_{\bar{K}/K} \longrightarrow \operatorname{Isom}(E), \qquad \xi_\sigma = \bigl[\chi(\sigma)\bigr].$$

Let C/K be the corresponding twist of E/K. We are going to derive an equation for C/K.

We choose a Weierstrass equation for E/K of the form $y^2 = f(x)$ and we write $\bar{K}(E) = \bar{K}(x,y)$ and $\bar{K}(C) = \bar{K}(x,y)_\xi$. Since $[-1](x,y) = (x,-y)$, the action of $\sigma \in G_{\bar{K}/K}$ on $\bar{K}(x,y)_\xi$ is determined by the formulas

$$\sqrt{d}^{\,\sigma} = \chi(\sigma)\sqrt{d}, \qquad x^\sigma = x, \qquad y^\sigma = \chi(\sigma)y.$$

Notice that the functions $x' = x$ and $y' = y/\sqrt{d}$ in $\bar{K}(x,y)_\xi$ are fixed by $G_{\bar{K}/K}$, and they satisfy the equation

$$dy'^2 = f(x'),$$

which is the equation of an elliptic curve defined over K. Further, the identification $(x',y') \mapsto (x', y'\sqrt{d}\,)$ shows that this curve is isomorphic to E over $K(\sqrt{d}\,)$. It is now an easy matter to check that the associated cocycle is ξ, and thus to verify that we have found an equation for C/K. The curve C is a *quadratic twist of* E; more precisely, it is the *twist of* E *by the quadratic character* χ. We will return to this example in more detail in (X §5).

X.3 Homogeneous Spaces

We recall from (VIII §2) that associated to an elliptic curve E/K is a Kummer sequence

$$0 \longrightarrow \frac{E(K)}{mE(K)} \longrightarrow H^1\bigl(G_{\bar{K}/K}, E[m]\bigr) \longrightarrow H^1\bigl(G_{\bar{K}/K}, E\bigr)[m] \longrightarrow 0.$$

The proof of the weak Mordell–Weil theorem hinges on the essential fact that the image of the first term in the second consists of elements that are unramified outside of a certain finite set of primes. In this section we analyze the third term in the sequence by associating to each element of $H^1(G_{\bar{K}/K}, E)$ a certain twist of E called a *homogeneous space*. However, rather than starting with cohomology, we instead begin by directly defining homogeneous spaces and describing their basic properties. We follow this with the cohomological interpretation, which says that homogeneous spaces are those twists that correspond to cocycles taking values in the group of translations.

Definition. Let E/K be an elliptic curve. A (*principal*) *homogeneous space for* E/K is a smooth curve C/K together with a simply transitive algebraic group action of E on C defined over K. In other words, a homogeneous space for E/K consists of a pair (C, μ), where C/K is a smooth curve and

$$\mu : C \times E \longrightarrow C$$

is a morphism defined over K having the following three properties:

(i) $\mu(p, O) = p$ for all $p \in C$.

(ii) $\mu\bigl(\mu(p, P), Q\bigr) = \mu(p, P + Q)$ for all $p \in C$ and $P, Q \in E$.

(iii) For all $p, q \in C$ there is a unique $P \in E$ satisfying $\mu(p, P) = q$.

We will often replace $\mu(p, P)$ with the more intuitive notation $p + P$. Then property (ii) is just the associative law $(p + P) + Q = p + (P + Q)$. Of course, one must determine from context whether $+$ means addition on E or the action of E on C.

In view of the simple transitivity of the action, we may define a *subtraction map* on C by the rule

$$\nu : C \times C \longrightarrow E,$$
$$\nu(q, p) = (\text{the unique } P \in E \text{ satisfying } \mu(p, P) = q).$$

It is not clear, a priori, that the map ν is even a rational map, but we will soon see that ν is a morphism and is defined over K. (This fact also follows from elementary intersection theory on $C \times C$.) In conjunction with our addition notation for μ, we often write $\nu(q, p)$ as $q - p$.

We now verify that addition and subtraction on a homogeneous space have the right properties.

Lemma 3.1. *Let C/K be a homogeneous space for E/K. Then for all $p, q \in C$ and all $P, Q \in E$:*

(a) $$\mu(p, O) = p \quad \textit{and} \quad \nu(p, p) = O.$$

(b) $$\mu\bigl(p, \nu(q, p)\bigr) = q \quad \textit{and} \quad \nu\bigl(\mu(p, P), p\bigr) = P.$$

(c) $$\nu\bigl(\mu(q, Q), \mu(p, P)\bigr) = \nu(q, p) + Q - P.$$

Equivalently, using the alternative "addition" and "subtraction" notation:

(a) $$p + O = p \quad \textit{and} \quad p - p = O.$$

(b) $$p + (q - p) = q \quad \textit{and} \quad (p + P) - p = P.$$

(c) $$(q + Q) - (p + P) = (q - p) + Q - P.$$

In other words, using $+$ and $-$ signs provides the right intuition.

PROOF. (a) The equality $\mu(p, O) = p$ is part of the definition of homogeneous space. Next, the definition of ν says that $\nu(p, p)$ is the unique point $P \in E$ satisfying $\mu(p, P) = p$. We know that this last equation is true for $P = O$, so $\nu(p, p) = O$.
(b) The relation $\mu\bigl(p, \nu(q, p)\bigr) = q$ is the definition of ν. Then, from

$$\mu\bigl(p, \nu(\mu(p,P),p)\bigr) = \mu(p,P),$$

we conclude that $\nu(\mu(p,P),p) = P$.

(c) We start with

$$q = \mu\bigl(p, \nu(q,p)\bigr).$$

Adding Q to both sides gives

$$\begin{aligned}\mu(q,Q) &= \mu\bigl(p, \nu(q,p) + Q\bigr)\\ &= \mu\bigl(p, P + \nu(q,p) + Q - P\bigr)\\ &= \mu\bigl(\mu(p,P), \nu(q,p) + Q - P\bigr).\end{aligned}$$

From the definition of ν, this is equivalent to

$$\nu\bigl(\mu(q,Q), \mu(p,P)\bigr) = \nu(q,p) + Q - P. \qquad \square$$

Next we show that a homogeneous space C/K for E/K is a twist of of E/K as described in (X §2). We also describe addition and subtraction on C in terms of a given $\bar{K}$-isomorphism $E \to C$.

Proposition 3.2. *Let E/K be an elliptic curve, and let C/K be a homogeneous space for E/K. Fix a point $p_0 \in C$ and define a map*

$$\theta : E \longrightarrow C, \qquad \theta(P) = p_0 + P.$$

(a) *The map θ is an isomorphism defined over $K(p_0)$. In particular, the curve C/K is a twist of E/K.*

(b) *For all $p \in C$ and all $P \in E$,*

$$p + P = \theta\bigl(\theta^{-1}(p) + P\bigr).$$

(*N.B. The first $+$ is the action of E on C, while the second $+$ is addition on E.*)

(c) *For all $p, q \in C$,*

$$q - p = \theta^{-1}(q) - \theta^{-1}(p).$$

(d) *The subtraction map*

$$\nu : C \times C \longrightarrow E, \qquad \nu(q,p) = q - p,$$

is a morphism and is defined over K.

PROOF. (a) The action of E on C is defined over K. Hence for any $\sigma \in G_{\bar{K}/K}$ satisfying $p_0^\sigma = p_0$, we have

$$\theta(P)^\sigma = (p_0 + P)^\sigma = p_0^\sigma + P^\sigma = p_0 + P^\sigma = \theta(P^\sigma).$$

This shows that θ is defined over $K(p_0)$. Further, the simple transitivity of the action tells us that θ has degree one, and then (II.2.4.1) allows us to conclude that θ is an isomorphism.

(b) We compute

$$\theta\big(\theta^{-1}(p) + P\big) = p_0 + \theta^{-1}(p) + P = p + P.$$

Note that we are using the fact that $\theta^{-1}(p)$ is the unique point of E that gives p when it is added to p_0.
(c) We compute

$$\theta^{-1}(q) - \theta^{-1}(p) = \big(p_0 + \theta^{-1}(q)\big) - \big(p_0 + \theta^{-1}(p)\big) = q - p.$$

(d) The fact that ν is a morphism follows from (c), since (III.3.6) says that subtraction on E is a morphism. To check that ν is defined over K, we let $\sigma \in G_{\bar{K}/K}$ and use (c) to compute

$$\begin{aligned}
(q-p)^\sigma &= \big(\theta^{-1}(q) - \theta^{-1}(p)\big)^\sigma \\
&= \theta^{-1}(q)^\sigma - \theta^{-1}(p)^\sigma && \text{since subtraction on } E \text{ is defined over } K, \\
&= \big(p_0 + \theta^{-1}(q)\big)^\sigma - \big(p_0 + \theta^{-1}(p)\big)^\sigma && \text{since the action of } E \text{ on } C \text{ is defined over } K, \\
&= q^\sigma - p^\sigma.
\end{aligned}$$

This completes the proof that ν is defined over K. □

Definition. Two homogeneous spaces C/K and C'/K for E/K are *equivalent* if there is an isomorphism $\theta : C \to C'$ defined over K that is compatible with the action of E on C and C'. In other words,

$$\theta(p+P) = \theta(p) + P \qquad \text{for all } p \in C \text{ and all } P \in E.$$

The equivalence class containing E/K, acting on itself by translation, is called the *trivial class*. The collection of equivalence classes of homogeneous spaces for E/K is called the *Weil–Châtelet group for E/K* and is denoted by $\mathrm{WC}(E/K)$. (We will see later why $\mathrm{WC}(E/K)$ is a group.)

The next result explains which homogeneous spaces are trivial.

Proposition 3.3. *Let C/K be a homogeneous space for E/K. Then C/K is in the trivial class if and only if $C(K)$ is not the empty set.*

PROOF. Suppose that C/K is in the trivial class. Then there is a K-isomorphism $\theta : E \to C$, and thus $\theta(O) \in C(K)$.

Conversely, suppose that $p_0 \in C(K)$. Then from (X.3.2a), the map

$$\theta : E \longrightarrow C, \qquad \theta(P) = p_0 + P,$$

is an isomorphism defined over $K(p_0) = K$. The required compatibility condition on θ is

$$p_0 + (P+Q) = (p_0 + P) + Q,$$

which is part of the definition of homogeneous space. □

Remark 3.4. Notice that (X.3.3) says that the problem of checking the triviality of a homogeneous space is exactly equivalent to answering the fundamental Diophantine question whether the given curve has any rational points. Thus our next step, namely the identification of $\mathrm{WC}(E/K)$ with a certain cohomology group, may be regarded as the development of a tool to help us study this difficult Diophantine problem.

Lemma 3.5. *Let $\theta : C/K \to C'/K$ be an equivalence of homogeneous spaces for E/K. Then*

$$\theta(q) - \theta(p) = q - p \qquad \textit{for all } p, q \in C.$$

PROOF. This is just a matter of grouping points so that the additions and subtractions are well-defined. Thus

$$\begin{aligned}\theta(q) - \theta(p) &= \Big(\big(\theta(q) + (p-q)\big) - \theta(p)\Big) + (q-p) \\ &= \Big(\theta\big(q + (p-q)\big) - \theta(p)\Big) + (q-p) \\ &= q - p. \end{aligned}$$ □

Theorem 3.6. *Let E/K be an elliptic curve. There is a natural bijection*

$$\mathrm{WC}(E/K) \longrightarrow H^1(G_{\bar{K}/K}, E)$$

defined as follows:

Let C/K be a homogeneous space for E/K and choose any point $p_0 \in C$. Then

$$\{C/K\} \longmapsto \{\sigma \mapsto p_0^\sigma - p_0\}.$$

(*The braces indicate that we are taking the equivalence class of C/K and the cohomology class of the* 1*-cocycle $\sigma \mapsto p_0^\sigma - p_0$.*)

Remark 3.6.1. Since $H^1(G_{\bar{K}/K}, E)$ is a group, we can use (X.3.6) to define a group structure on the set $\mathrm{WC}(E/K)$. It is also possible to describe the group law on $\mathrm{WC}(E/K)$ geometrically, without using cohomology, which in fact is the way that it was originally defined. See Exercise 10.2 and [307].

PROOF. First we check that the map is well-defined. It is easy to see that the map $\sigma \mapsto p_0^\sigma - p_0$ is a cocycle:

$$p_0^{\sigma\tau} - p_0 = (p_0^{\sigma\tau} - p_0^\tau) + (p_0^\tau - p_0) = (p_0^\sigma - p_0)^\tau + (p_0^\tau - p_0).$$

Now suppose that C'/K is another homogeneous space that is equivalent to C/K. Let $\theta : C \to C'$ be a K-isomorphism giving the equivalence, and let $p_0' \in C'$. We use (X.3.5) to compute

$$\begin{aligned}p_0^\sigma - p_0 &= \theta(p_0^\sigma) - \theta(p_0) \\ &= (p_0'^\sigma - p_0') + \Big(\big(\theta(p_0) - p_0'\big)^\sigma - \big(\theta(p_0) - p_0'\big)\Big).\end{aligned}$$

Hence the cocycles $p_0^\sigma - p_0$ and $p_0'^\sigma - p_0'$ differ by the coboundary generated by the point $\theta(p_0) - p_0' \in E$, so they give the same cohomology class in $H^1(G_{\bar{K}/K}, E)$.

Next we check injectivity. Suppose that the cocycles $p_0^\sigma - p_0$ and $p_0'^\sigma - p_0'$ corresponding to C/K and C'/K are cohomologous. This means that there is a point $P_0 \in E$ satisfying

$$p_0^\sigma - p_0 = p_0'^\sigma - p_0' + (P_0^\sigma - P_0) \qquad \text{for all } \sigma \in G_{\bar{K}/K}.$$

Consider the map

$$\theta : C \longrightarrow C', \qquad \theta(p) = p_0' + (p - p_0) + P_0.$$

It is clear that θ is a $\bar{K}$-isomorphism and that it is compatible with the action of E on C and C'. We claim that θ is defined over K. In order to prove this, we compute

$$\begin{aligned} \theta(p)^\sigma &= p_0'^\sigma + (p^\sigma - p_0^\sigma) + P_0^\sigma \\ &= p_0' + (p^\sigma - p_0) + P_0 + \big((p_0'^\sigma - p_0') + P_0^\sigma - P_0 - (p_0^\sigma - p_0)\big) \\ &= \theta(p^\sigma). \end{aligned}$$

This proves that C and C' are equivalent.

It remains to prove surjectivity. Let $\xi : G_{\bar{K}/K} \to E$ be a 1-cocycle representing an element in $H^1(G_{\bar{K}/K}, E)$. We embed E into $\operatorname{Isom}(E)$ by sending $P \in E$ to the translation map $\tau_P \in \operatorname{Isom}(E)$, and then we may view ξ as living in the cohomology set $H^1\big(G_{\bar{K}/K}, \operatorname{Isom}(E)\big)$. From (X.2.2), there are a curve C/K and a $\bar{K}$-isomorphism $\phi : C \to E$ such that for all $\sigma \in G_{\bar{K}/K}$,

$$\phi^\sigma \circ \phi^{-1} = (\text{translation by } -\xi_\sigma).$$

(The reason for using $-\xi$, rather than ξ, will soon become apparent.)

Define a map

$$\mu : C \times E \longrightarrow C, \qquad \mu(p, P) = \phi^{-1}\big(\phi(p) + P\big).$$

We now show that μ gives C/K the structure of a homogeneous space over E/K and that its associated cohomology class is $\{\xi\}$.

First we check that μ is simply transitive. Let $p, q \in C$. Then by definition we have

$$\mu(p, P) = q \quad \text{if and only if} \quad \phi^{-1}\big(\phi(p) + P\big) = q,$$

so the only choice for P is $P = \phi(q) - \phi(p)$. Second we verify that μ is defined over K. We take $\sigma \in G_{\bar{K}/K}$ and compute

$$\begin{aligned} \mu(p, P)^\sigma &= (\phi^{-1})^\sigma\big(\phi^\sigma(p^\sigma) + P^\sigma\big) \\ &= \phi^{-1}\Big(\big(\phi(p^\sigma) - \xi_\sigma + P^\sigma\big) + \xi_\sigma\Big) \\ &= \mu(p^\sigma, P^\sigma). \end{aligned}$$

Finally, we compute the cohomology class associated to C/K. To do this, we may choose *any* point $p_0 \in C$ and take the class of the cocycle $\sigma \mapsto p_0^\sigma - p_0$. In particular, if we take $p_0 = \phi^{-1}(O)$, then

$$\begin{aligned} p_0^\sigma - p_0 &= (\phi^\sigma)^{-1}(O) - \phi^{-1}(O) \\ &= \phi^{-1}(O + \xi_\sigma) - \phi^{-1}(O) \\ &= \xi_\sigma. \end{aligned}$$

This completes the proof of (X.3.6). □

Remark 3.7. Let E/K be an elliptic curve and let $K(\sqrt{d})/K$ be a quadratic extension, so in particular $\operatorname{char}(K) \ne 2$. Let $T \in E(K)$ be a nontrivial point of order 2. Then the homomorphism

$$\begin{aligned} \xi : G_{\bar{K}/K} &\longrightarrow E, \\ \sigma &\longmapsto \begin{cases} O & \text{if } \sqrt{d}^{\,\sigma} = \sqrt{d}, \\ T & \text{if } \sqrt{d}^{\,\sigma} = -\sqrt{d}, \end{cases} \end{aligned}$$

is a 1-cocycle. We now construct the homogeneous space corresponding to the element $\{\xi\} \in H^1(G_{\bar{K}/K}, E)$.

Since $T \in E(K)$, we may choose a Weierstrass equation for E/K in the form

$$E : y^2 = x^3 + ax^2 + bx \qquad \text{with} \quad T = (0,0).$$

Then the translation-by-T map has the simple form

$$\tau_T(P) = (x,y) + (0,0) = \left(\frac{b}{x}, -\frac{by}{x^2}\right).$$

Thus if we let $\sigma \in G_{\bar{K}/K}$ be the nontrivial automorphism of $K(\sqrt{d})/K$, then the action of σ on the twisted field $\bar{K}(E)_\xi$ may be summarized by

$$\sqrt{d}^{\,\sigma} = -\sqrt{d}, \qquad x^\sigma = \frac{b}{x}, \qquad y^\sigma = -\frac{by}{x^2}.$$

We need to find the subfield of $K(\sqrt{d})(x,y)_\xi$ that is fixed by σ.

The functions

$$\frac{\sqrt{d}\,x}{y} \quad \text{and} \quad \sqrt{d}\left(x - \frac{b}{x}\right)$$

are easily seen to be invariant. Anticipating the form of our final equation, we consider instead the functions

$$z = \frac{\sqrt{d}\,x}{y} \quad \text{and} \quad w = \sqrt{d}\left(x - \frac{b}{x}\right)\left(\frac{x}{y}\right)^2.$$

We find a relation between z and w by computing

$$\begin{aligned} d\left(\frac{w}{z^2}\right)^2 &= \left(x - \frac{b}{x}\right)^2 = \left(x + \frac{b}{x}\right)^2 - 4b \\ &= \left(\left(\frac{y}{x}\right)^2 - a\right)^2 - 4b = \left(\frac{d}{z^2} - a\right)^2 - 4b. \end{aligned}$$

Thus (z, w) are affine coordinates for the hyperelliptic curve

$$C : dw^2 = d^2 - 2adz^2 + (a^2 - 4b)z^4.$$

(See (II.2.5.1) and Exercise 2.14 for general properties of hyperelliptic curves.) We claim that C/K is the twist of E/K corresponding to the cocycle ξ.

First, we recall from (II.2.5.1) that C is a smooth *affine* curve provided that the polynomial $d^2 - 2adz^2 + (a^2 - 4b)z^4$ has four distinct roots in $\bar{K}$. Further, (II.2.5.2) says that if the quartic polynomial has distinct roots, then there is a smooth curve in $\mathbb{P}^3$ that has an affine piece isomorphic to C. This smooth curve consists of C together with the two points

$$\left[0, 0, \pm\sqrt{\frac{a^2 - 4b}{d}}, 1\right]$$

at infinity. (N.B. The projective closure of C in $\mathbb{P}^2$ is always singular.) It is easy to check that the quartic has distinct roots if and only if $b(a^2 - 4b) \neq 0$. On the other hand, since E is nonsingular, we know that $\Delta(E) = 16b^2(a^2 - 4b) \neq 0$. Therefore C is an affine piece of a smooth curve in $\mathbb{P}^3$. To ease notation, we also use C to denote this smooth curve $C \subset \mathbb{P}^3$.

There is a natural map defined over $K(\sqrt{d}\,)$,

$$\begin{aligned} &\phi : E \longrightarrow C, \\ &(x, y) \longmapsto (z, w) = \left(\frac{\sqrt{d}\,x}{y}, \sqrt{d}\left(x - \frac{b}{x}\right)\left(\frac{x}{y}\right)^2\right). \end{aligned}$$

Note that since

$$\frac{x}{y} = \frac{xy}{y^2} = \frac{y}{x^2 + ax + b},$$

the map ϕ may also be written as

$$\phi(x, y) = \left(\frac{\sqrt{d}\,y}{x^2 + ax + b}, \frac{\sqrt{d}\,(x^2 - b)}{x^2 + ax + b}\right).$$

This allows us to evaluate

$$\phi(0, 0) = (0, -\sqrt{d}\,) \quad \text{and} \quad \phi(O) = (0, \sqrt{d}\,).$$

To show that ϕ is an isomorphism, we compute its inverse:

$$\begin{aligned}\frac{\sqrt{d}\,w}{z^2} &= x - \frac{b}{x} = 2x - \left(x + \frac{b}{x}\right) \\ &= 2x - \left(\left(\frac{y}{x}\right)^2 - a\right) = 2x - \left(\frac{d}{z^2} - a\right).\end{aligned}$$

This gives x in terms of z and w, and then $y = \sqrt{d}\,x/z$. Thus

$$\begin{aligned}&\phi^{-1} : C \longrightarrow E, \\ &(z,w) \longmapsto \left(\frac{\sqrt{d}\,w - az^2 + d}{2z^2}, \frac{dw - a\sqrt{d}\,z^2 + d\sqrt{d}}{2z^3}\right).\end{aligned}$$

Since C and E are smooth, it follows from (II.2.4.1) that ϕ is an isomorphism.

Finally, in order to compute the element of $H^1(G_{\bar{K}/K}, E)$ corresponding to the curve C/K, we may choose *any* point $p \in C$ and compute the cocycle

$$\sigma \longmapsto p^\sigma - p = \phi^{-1}(p^\sigma) - \phi^{-1}(p).$$

For instance, we may take $p = (0, \sqrt{d}) \in C$. It is clear that if σ fixes $\sqrt{d}$, then $p^\sigma - p = O$. On the other hand, if $\sqrt{d}^{\,\sigma} = -\sqrt{d}$, then

$$p^\sigma - p = \phi^{-1}(0, -\sqrt{d}) - \phi^{-1}(0, \sqrt{d}) = (0,0).$$

Therefore $p^\sigma - p = \xi_\sigma$ for all $\sigma \in G_{\bar{K}/K}$, so $\{C/K\} \in \mathrm{WC}(E/K)$ maps to $\{\xi\} \in H^1(G_{\bar{K}/K}, E)$. Of course, it was just "luck" that we obtained an equality $p^\sigma - p = \xi_\sigma$. In general, the difference of these two cocycles would be some coboundary.

We conclude this section by showing that if C/K is a homogeneous space for E/K, then $\mathrm{Pic}^0(C)$ may be canonically identified with E. This means that E is the *Jacobian variety of* C/K. Since every curve C/K of genus one is a homogeneous space for some elliptic curve E/K (Exercise 10.3), this shows that the abstract group $\mathrm{Pic}^0(C)$ can always be represented as the group of points of an elliptic curve. The analogous result for curves of higher genus, in which $\mathrm{Pic}^0(C)$ is represented by an abelian variety of dimension equal to the genus of C, is considerably harder to prove.

Theorem 3.8. *Let C/K be a homogeneous space for an elliptic curve E/K. Choose a point $p_0 \in C$ and consider the summation map*

$$\begin{aligned}\mathrm{sum} : \mathrm{Div}^0(C) &\longrightarrow E, \\ \sum n_i(p_i) &\longmapsto \sum [n_i](p_i - p_0).\end{aligned}$$

(a) *There is an exact sequence*

$$1 \longrightarrow \bar{K}^* \longrightarrow \bar{K}(C)^* \xrightarrow{\mathrm{div}} \mathrm{Div}^0(C) \xrightarrow{\mathrm{sum}} E \longrightarrow 0.$$

(b) *The summation map is independent of the choice of the point* p_0.

(c) *The summation map commutes with the natural actions of the Galois group* $G_{\bar{K}/K}$ *on* $\operatorname{Div}^0(C)$ *and on* E. *Hence it induces an isomorphism of* $G_{\bar{K}/K}$*-modules (also denoted by* sum*)*

$$\operatorname{sum} : \operatorname{Pic}^0(C) \xrightarrow{\sim} E.$$

In particular,

$$\operatorname{Pic}^0_K(C) \cong E(K).$$

PROOF. (a) Using (II.3.4), we see that we must check that the summation map is a surjective homomorphism and that its kernel is the set of principal divisors. It is clear that it is a homomorphism. Let $P \in E$ and $D = (p_0 + P) - (p_0) \in \operatorname{Div}^0(C)$. Then

$$\operatorname{sum}(D) = \big((p_0 + P) - p_0\big) - (p_0 - p_0) = P,$$

so sum is surjective.

Next suppose that $D = \sum n_i(p_i) \in \operatorname{Div}^0(C)$ satisfies $\operatorname{sum}(D) = O$. Then the *divisor* $\sum n_i(p_i - p_0) \in \operatorname{Div}^0(E)$ sums to O, so (III.3.5) tells us that it is principal, say

$$\sum n_i(p_i - p_0) = \operatorname{div}(f) \quad \text{for some } f \in \bar{K}(E)^*.$$

We have an isomorphism

$$\phi : C \longrightarrow E, \qquad \phi(p) = p - p_0,$$

and hence applying (II.3.6b),

$$\operatorname{div}(\phi^* f) = \phi^* \operatorname{div}(f) = \sum n_i \phi^*\big((p_i - p_0)\big) = \sum n_i(p_i) = D.$$

Therefore D is principal.

Finally, if $D = \operatorname{div}(g)$ is principal, then

$$\sum n_i(p_i - p_0) = (\phi^{-1})^* \operatorname{div}(g) = \operatorname{div}\big((\phi^{-1})^* g\big),$$

and hence $\operatorname{sum}(D) = O$. This shows that the kernel of the summation map is the set of principal divisors.

(b) Let $\operatorname{sum}' : \operatorname{Div}^0(C) \to E$ be the summation map defined using the base point $p_0' \in C$. Then

$$\begin{aligned}\operatorname{sum}(D) - \operatorname{sum}'(D) &= \sum [n_i]\big((p_i - p_0) - (p_i - p_0')\big) \\ &= \sum [n_i](p_0' - p_0) \\ &= O,\end{aligned}$$

since $\sum n_i = \deg(D) = 0$.

(c) Let $\sigma \in G_{\bar{K}/K}$. Then

$$\operatorname{sum}(D)^\sigma = \sum [n_i](p_i^\sigma - p_0^\sigma) = \operatorname{sum}(D^\sigma),$$

since we know from (b) that the sum is the same if we use p_0^σ as our base point instead of p_0. Now (a) and the definition of $\operatorname{Pic}^0(C)$ tell us that we have a group isomorphism $\operatorname{sum} : \operatorname{Pic}^0(C) \to E$, and the fact that the summation map commutes with the action of $G_{\bar{K}/K}$ says precisely that it is an isomorphism of $G_{\bar{K}/K}$-modules. Finally, the last statement in (X.3.8c) follows by taking $G_{\bar{K}/K}$-invariants. □

X.4 The Selmer and Shafarevich–Tate Groups

We return now to the problem of calculating the Mordell–Weil group of an elliptic curve E/K defined over a number field K. As we have seen in (VIII.3.2) and Exercise 8.18, it is enough to find generators for the finite group $E(K)/mE(K)$ for any integer $m \geq 2$.

Suppose that we are given another elliptic curve E'/K and a nonzero isogeny $\phi : E \to E'$ defined over K. For example, we could take $E = E'$ and $\phi = [m]$. Then there is an exact sequence of $G_{\bar{K}/K}$-modules

$$0 \longrightarrow E[\phi] \longrightarrow E \xrightarrow{\phi} E' \longrightarrow 0,$$

where $E[\phi]$ denotes the kernel of ϕ. Taking Galois cohomology yields the long exact sequence

$$\begin{tikzcd}
0 \arrow[r] & E(K)[\phi] \arrow[r] & E(K) \arrow[r, "\phi"] & E'(K) \arrow[dll, rounded corners, to path={ -- ([xshift=2ex]\tikztostart.east) |- (X.center) \tikztonodes -| ([xshift=-2ex]\tikztotarget.west) -- (\tikztotarget)}, "\delta"'] \\
H^1\big(G_{\bar{K}/K}, E[\phi]\big) \arrow[r] & H^1\big(G_{\bar{K}/K}, E\big) \arrow[r, "\phi"] & H^1\big(G_{\bar{K}/K}, E'\big),
\end{tikzcd}$$

and from this we form the fundamental short exact sequence

$$0 \to E'(K)/\phi\big(E(K)\big) \xrightarrow{\delta} H^1\big(G_{\bar{K}/K}, E[\phi]\big) \to H^1(G_{\bar{K}/K}, E)[\phi] \to 0. \qquad (*)$$

Note that (X.3.6) says that the last term in $(*)$ may be identified with the ϕ-torsion in the Weil–Châtelet group $\mathrm{WC}(E/K)$.

The next step is to replace the second and third terms of $(*)$ with certain finite groups. This is accomplished by local considerations. For each $v \in M_K$ we fix an extension of v to $\bar{K}$, which serves to fix an embedding $\bar{K} \subset \bar{K}_v$ and a decomposition group $G_v \subset G_{\bar{K}/K}$. Now G_v acts on $E(\bar{K}_v)$ and $E'(\bar{K}_v)$, and repeating the above argument yields exact sequences

$$0 \to E'(K_v)/\phi\big(E(K_v)\big) \xrightarrow{\delta} H^1\big(G_v, E[\phi]\big) \to H^1(G_v, E)[\phi] \to 0. \qquad (*_v)$$

The natural inclusions $G_v \subset G_{\bar{K}/K}$ and $E(\bar{K}) \subset E(\bar{K}_v)$ give restriction maps on cohomology, and we thus end up with the following commutative diagram, in which we have replaced each $H^1(G, E)$ with the corresponding Weil–Châtelet group:

$$\begin{tikzcd}
0 \arrow[r] & E'(K)/\phi\bigl(E(K)\bigr) \arrow[r, "\delta"] \arrow[d] & H^1\bigl(G_{\bar{K}/K}, E[\phi]\bigr) \arrow[r] \arrow[d] & \mathrm{WC}(E/K)[\phi] \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \prod_{v\in M_K} E'(K_v)/\phi\bigl(E(K_v)\bigr) \arrow[r, "\delta"] & \prod_{v\in M_K} H^1\bigl(G_v, E[\phi]\bigr) \arrow[r] & \prod_{v\in M_K} \mathrm{WC}(E/K_v)[\phi] \arrow[r] & 0
\end{tikzcd}$$

$(**)$

Our ultimate goal is to compute the image of $E'(K)/\phi\bigl(E(K)\bigr)$ in the cohomology group $H^1\bigl(G_{\bar{K}/K}, E[\phi]\bigr)$, or equivalently, to compute the kernel of the map

$$H^1\bigl(G_{\bar{K}/K}, E[\phi]\bigr) \to \mathrm{WC}(E/K)[\phi].$$

Using (X.3.3), we see that this last problem is the same as determining whether certain homogeneous spaces possess a K-rational point, which may be a very difficult question to answer. On the other hand, by the same reasoning, the determination of each local kernel

$$\ker\Bigl(H^1\bigl(G_v, E[\phi]\bigr) \longrightarrow \mathrm{WC}(E/K_v)[\phi]\Bigr)$$

is straightforward, since the question whether a curve has a point over a complete local field K_v reduces, by Hensel's lemma, to checking whether the curve has a point in some finite ring $R_v/\mathcal{M}_v^e$ for some easily computable integer e, which clearly requires only a finite amount of computation. This prompts the following definitions.

Definition. Let $\phi : E/K \to E'/K$ be an isogeny. The *ϕ-Selmer group of E/K* is the subgroup of $H^1\bigl(G_{\bar{K}/K}, E[\phi]\bigr)$ defined by

$$S^{(\phi)}(E/K) = \ker\left\{H^1\bigl(G_{\bar{K}/K}, E[\phi]\bigr) \longrightarrow \prod_{v\in M_K} \mathrm{WC}(E/K_v)\right\}.$$

The *Shafarevich–Tate group of E/K* is the subgroup of $\mathrm{WC}(E/K)$ defined by

$$Ш(E/K) = \ker\left\{\mathrm{WC}(E/K) \longrightarrow \prod_{v\in M_K} \mathrm{WC}(E/K_v)\right\}.$$

(The Cyrillic letter Ш is pronounced “sha.”)

Remark 4.1.1. The exact sequences ($*_v$) require us to extend each $v \in M_K$ to $\bar{K}$, so the groups $S^{(\phi)}(E/K)$ and $Ш(E/K)$ might depend on this choice. However, in order to determine whether an element of $\mathrm{WC}(E/K)$ becomes trivial in $\mathrm{WC}(E/K_v)$, we must check whether the associated homogeneous space, which is a curve defined over K, has any points defined over K_v. This last problem is clearly independent of our choice of extension of v to $\bar{K}$, since v itself determines the embedding of K into K_v. Therefore $S^{(\phi)}(E/K)$ and $Ш(E/K)$ depend only on E and K.

Alternatively, one can check directly by working with cocycles that the cohomological definitions of $S^{(\phi)}$ and Ш do not depend on the extension of the $v \in M_K$ to $\bar{K}$. We leave this verification for the reader. (See also Exercise B.6.)

Remark 4.1.2. A good way to view $\text{Ш}(E/K)$ is as the group of homogeneous spaces for E/K that possess a K_v-rational point for every $v \in M_K$. Equivalently, the Shafarevich–Tate group $\text{Ш}(E/K)$ is the group of homogeneous spaces, modulo equivalence, that are everywhere locally trivial.

Theorem 4.2. *Let $\phi : E/K \to E'/K$ be an isogeny of elliptic curves defined over K.*
(a) *There is an exact sequence*

$$0 \longrightarrow E'(K)/\phi\bigl(E(K)\bigr) \longrightarrow S^{(\phi)}(E/K) \longrightarrow \text{Ш}(E/K)[\phi] \longrightarrow 0.$$

(b) *The Selmer group $S^{(\phi)}(E/K)$ is finite.*

PROOF. (a) This is immediate from the diagram ($**$) and the definitions of the Selmer and Shafarevich–Tate groups.
(b) If we take $E = E'$ and $\phi = [m]$, then (a) and the finiteness of $S^{(m)}(E/K)$ imply the weak Mordell–Weil theorem. On the other hand, in order to prove that $S^{(\phi)}(E/K)$ is finite for a general map ϕ, we must essentially re-prove the weak Mordell–Weil theorem. The arguement goes as follows.

Let $\xi \in S^{(\phi)}(E/K)$, and let $v \in M_K$ be a finite place of K not dividing $m = \deg(\phi)$ and such that E/K has good reduction at v. We claim that ξ is unramified at v. (See (VIII §2) for the definition of an unramified cocycle.)

To check this, let $I_v \subset G_v$ be the inertia group for v. Since $\xi \in S^{(\phi)}(E/K)$, we know that ξ is trivial in $\text{WC}(E/K_v)$. Hence from the sequence ($*_v$) given earlier, there is a point $P \in E(\bar{K}_v)$ such that

$$\xi_\sigma = \{P^\sigma - P\} \qquad \text{for all } \sigma \in G_v.$$

(Note that $P^\sigma - P \in E[\phi]$.) In particular, this holds for all σ in the inertia group. But if $\sigma \in I_v$, then looking at the "reduction modulo v" map $E \to \tilde{E}_v$ yields

$$\widetilde{P^\sigma - P} = \tilde{P}^\sigma - \tilde{P} = \tilde{O},$$

since by definition inertia acts trivially on $\tilde{E}_v$. Thus $P^\sigma - P$ is in the kernel of reduction modulo v. But $P^\sigma - P$ is also in $E[\phi]$, which is contained in $E[m]$; and from (VIII.1.4) we know that $E(K)[m]$ injects into $\tilde{E}_v$. Therefore $P^\sigma = P$, and hence

$$\xi_\sigma = \{P^\sigma - P\} = 0 \qquad \text{for all } \sigma \in I_v.$$

This proves that every element in $S^{(\phi)}(E/K)$ is unramified at all but a fixed, finite set of places $v \in M_K$. The following lemma allows us to conclude that $S^{(\phi)}(E/K)$ is finite. □

Lemma 4.3. *Let M be a finite (abelian) $G_{\bar{K}/K}$-module, let $S \subset M_K$ be a finite set of places, and define*

$$H^1(G_{\bar{K}/K}, M; S) = \bigl\{\xi \in H^1(G_{\bar{K}/K}, M) : \xi \text{ is unramified outside } S\bigr\}.$$

Then $H^1(G_{\bar{K}/K}, M; S)$ is finite.

PROOF. Since M is finite and $G_{\bar{K}/K}$ acts continuously on M, there is a subgroup of finite index in $G_{\bar{K}/K}$ that fixes every element of M. Using the inflation–restriction sequence (B.2.4), it suffices to prove the lemma with K replaced by a finite extension, so we may assume that the action of $G_{\bar{K}/K}$ on M is trivial. Then

$$H^1(G_{\bar{K}/K}, M; S) = \operatorname{Hom}(G_{\bar{K}/K}, M; S).$$

Let m be the exponent of M, i.e., the smallest positive integer such that $mx = 0$ for all $x \in M$, and let L/K be the maximal abelian extension of K having exponent m that is unramified outside of S. Since M has exponent m, the natural map

$$\operatorname{Hom}(G_{L/K}, M; S) \longrightarrow \operatorname{Hom}(G_{\bar{K}/K}, M; S)$$

is an isomorphism. But we know from (VIII.1.6) that L/K is a *finite* extension. Therefore $\operatorname{Hom}(G_{\bar{K}/K}, M; S)$ is finite. □

We record as a corollary an important property of the Selmer group that was derived during the course of proving (X.4.2), where we use the fact (VII.7.2) that isogenous elliptic curves have the same set of primes of bad reduction.

Corollary 4.4. *Let $\phi : E/K \to E'/K$ be as in* (X.4.2)*, and let $S \subset M_K$ be a finite set of places containing*

$$M_K^\infty \cup \{v \in M_K^0 : E \textit{ has bad reduction at } v\} \cup \{v \in M_K^0 : v(\deg \phi) > 0\}.$$

Then

$$S^{(\phi)}(E/K) \subset H^1(G_{\bar{K}/K}, E[\phi]; S).$$

Remark 4.5. Certainly in theory, and often in practice, the Selmer group is effectively computable. This is true because the finite group $H^1(G_{\bar{K}/K}, E[\phi]; S)$ is effectively computable. Then, in order to determine whether a given element $\xi \in H^1(G_{\bar{K}/K}, E[\phi]; S)$ is in $S^{(\phi)}(E/K)$, we take the corresponding homogeneous spaces $\{C/K\} \in \mathrm{WC}(E/K)$ and check, for each of the finitely many $v \in S$, whether $C(K_v) \neq \emptyset$. This last problem may be reduced, using Hensel's lemma, to a finite amount of computation.

Example 4.5.1. We reformulate the example described in (X §1) in these terms, leaving some details to the reader. Let E/K be an elliptic curve with $E[m] \subset E(K)$, let $S \subset M_K$ be the usual set of places (X.4.4), and let $K(S, m)$ be as in (X.1.1c). We choose a basis for $E[m]$ and use it to identify $E[m]$ with $\boldsymbol{\mu}_m \times \boldsymbol{\mu}_m$ as $G_{\bar{K}/K}$-modules. Then

$$H^1(G_{\bar{K}/K}, E[m]; S) \cong K(S, m) \times K(S, m),$$

where this map uses the isomorphism $K^*/(K^*)^m \xrightarrow{\sim} H^1(G_{\bar{K}/K}, \boldsymbol{\mu}_m)$.

Restricting attention now to the case $m = 2$, the homogeneous space associated to a pair $(b_1, b_2) \in K(S, m) \times K(S, m)$ is the curve in $\mathbb{P}^3$ given by the equations (cf. (X.1.4))

$$C : b_1 z_1^2 - b_2 z_2^2 = (e_2 - e_1) z_0^2, \quad b_1 z_1^2 - b_1 b_2 z_3^2 = (e_3 - e_1) z_0^2.$$

For any given pair (b_1, b_2) and any absolute value $v \in S$, it is easy to check whether $C(K_v) \neq \emptyset$, and thus to calculate $S^{(2)}(E/K)$. For example, the conclusion of (X.1.5) may be summarized by stating that the curve

$$E : y^2 = x^3 - 12x^2 + 20x$$

satisfies

$$S^{(2)}(E/\mathbb{Q}) = (\mathbb{Z}/2\mathbb{Z})^3 \qquad \text{and} \qquad Ш(E/\mathbb{Q})[2] = 0.$$

The conclusion about Ш follows from the exact sequence (X.4.2a), since in (X.1.5) we proved that every element of $S^{(2)}(E/\mathbb{Q})$ is the image of a point in $E(\mathbb{Q})$.

Suppose that we have computed the Selmer group $S^{(\phi)}(E/K)$ for an isogeny ϕ. Each $\xi \in S^{(\phi)}(E/K)$ corresponds to a homogeneous space C_ξ/K that has a point defined over every local field K_v. Suppose further that we are lucky and can show that $Ш(E/K)[\phi] = 0$. This means that we are able to find a K-rational point on each C_ξ. It then follows from (X.4.2a) that $E'(K)/\phi\bigl(E(K)\bigr) \cong S^{(\phi)}(E/K)$, and all that remains is to explain how to find generators for $E'(K)/\phi\bigl(E(K)\bigr)$ in terms of the points that we found in each $C_\xi(K)$. This is done in the next proposition.

Proposition 4.6. *Let $\phi : E/K \to E'/K$ be a K-isogeny, let ξ be a cocycle representing an element of $H^1(G_{\bar{K}/K}, E[\phi])$, and let C/K be a homogeneous space representing the image of ξ in* WC(E/K). *Choose a $\bar{K}$-isomorphism $\theta : C \to E$ satisfying*

$$\theta^\sigma \circ \theta^{-1} = (\textit{translation by } \xi_\sigma) \qquad \textit{for all } \sigma \in G_{\bar{K}/K}.$$

(a) *The map $\phi \circ \theta : C \to E'$ is defined over K.*

(b) *Suppose that there is a point $P \in C(K)$, so $\{C/K\}$ is trivial in* WC(E/K). *Then the point $\phi \circ \theta(P) \in E'(K)$ maps to ξ via the connecting homomorphism $\delta : E'(K) \to H^1\bigl(G_{\bar{K}/K}, E[\phi]\bigr)$.*

PROOF. (a) Let $\sigma \in G_{\bar{K}/K}$ and let $P \in C$. Then, since ϕ is defined over K and $\xi_\sigma \in E[\phi]$, we have

$$\bigl(\phi \circ \theta(P)\bigr)^\sigma = (\phi \circ \theta^\sigma)(P^\sigma) = \phi\bigl(\theta(P^\sigma) + \xi_\sigma\bigr) = \phi \circ \theta(P^\sigma).$$

Therefore $\phi \circ \theta$ is defined over K.

(b) This is just a matter of unwinding definitions. Thus

$$\delta\bigl(\phi \circ \theta(P)\bigr)_\sigma = \theta(P)^\sigma - \theta(P) = \theta(P^\sigma) + \xi_\sigma - \theta(P) = \xi_\sigma. \qquad \square$$

Remark 4.7. We have been working with arbitrary isogenies $\phi : E \to E'$, but in order to compute the Mordell–Weil group of E', we must find generators for $E'(K)/mE'(K)$ for some integer m; simply knowing $E'(K)/\phi\bigl(E(K)\bigr)$ is not enough. The solution to this dilemma is to work with both ϕ and its dual

$\hat{\phi} : E' \to E$. Using the procedure described in this section, we compute both Selmer groups $S^{(\phi)}(E/K)$ and $S^{(\hat{\phi})}(E'/K)$, and with a little bit of luck, we find generators for the two quotient groups $E'(K)/\phi\bigl(E(K)\bigr)$ and $E(K)/\hat{\phi}\bigl(E'(K)\bigr)$. It is then a simple matter to compute generators for $E(K)/mE(K)$, where $m = \deg(\phi)$, using the elementary exact sequence (note that $\hat{\phi} \circ \phi = [m]$)

$$0 \longrightarrow \frac{E'(K)[\hat{\phi}]}{\phi\bigl(E(K)[m]\bigr)} \longrightarrow \frac{E'(K)}{\phi\bigl(E(K)\bigr)} \xrightarrow{\hat{\phi}} \frac{E(K)}{mE(K)} \longrightarrow \frac{E(K)}{\hat{\phi}\bigl(E'(K)\bigr)} \longrightarrow 0.$$

Example 4.8. *Two-isogenies.* We illustrate the general theory by completely analyzing the case of isogenies of degree 2. Let $\phi : E \to E'$ be an isogeny of degree 2 defined over K. Then the kernel $E[\phi] = \{O, T\}$ is defined over K, so $T \in E(K)$. Moving this K-rational 2-torsion point to $(0, 0)$, we can find a Weierstrass equation for E/K of the form

$$E : y^2 = x^3 + ax^2 + bx.$$

Let $S \subset M_K$ be the usual set of places (X.4.4). Identifying $E[\phi]$ with $\boldsymbol{\mu}_2$ (as $G_{\bar{K}/K}$-modules), we see that $K^*/(K^*)^2 \cong H^1(G_{\bar{K}/K}, E[\phi])$. Thus, using notation from (X.1.1c) and (X.4.3), we have

$$H^1(G_{\bar{K}/K}, E[\phi]; S) \cong K(S, 2).$$

More precisely, if $d \in K(S, 2)$, then tracing through the above identification shows that the corresponding cocycle is

$$\sigma \longmapsto \begin{cases} O & \text{if } \sqrt{d}^{\,\sigma} = \sqrt{d}, \\ T & \text{if } \sqrt{d}^{\,\sigma} = -\sqrt{d}. \end{cases}$$

The homogeneous space C_d/K associated to this cocycle was computed in (X.3.7); it is given by the equation

$$C_d : dw^2 = d^2 - 2adz^2 + (a^2 - 4b)z^4.$$

We can now compute the Selmer group $S^{(\phi)}$ by checking whether $C_d(K_v) = \emptyset$ for each of the finitely many $d \in K(S, 2)$ and $v \in S$.

The isogenous curve E'/K has Weierstrass equation

$$E' : Y^2 = X^3 - 2aX^2 + (a^2 - 4b)X,$$

and the isogeny $\phi : E \to E'$ is given by the formula (III.4.5)

$$\phi(x, y) = \left(\frac{y^2}{x^2}, \frac{y(b - x^2)}{x^2} \right).$$

In (X.3.7) we gave an isomorphism $\theta : C_d \to E$ defined over $K(\sqrt{d}\,)$. Computing the composition $\phi \circ \theta$ yields the map

$$\theta \circ \phi : C_d \longrightarrow E', \qquad \theta \circ \phi(z,w) = \left(\frac{d}{z^2}, -\frac{dw}{z^3}\right),$$

described in (X.4.6). Finally, just as we did in (X.1.4) (see also Exercise 10.1), we can compute the connecting homomorphism

$$\delta : E'(K) \longrightarrow H^1(G_{\bar{K}/K}, E[\phi]) \cong K^*/(K^*)^2.$$

It is given by

$$\delta(O) = 1, \qquad \delta(0,0) = a^2 - 4b, \qquad \delta(X,Y) = X \quad \text{if } X \neq 0, \infty.$$

We summarize (X.4.8) in the next proposition.

Proposition 4.9. (Descent via Two-Isogeny) *Let E/K and E'/K be elliptic curves given by the equations*

$$E : y^2 = x^3 + ax^2 + bx \qquad \textit{and} \qquad E' : Y^2 = X^3 - 2aX^2 + (a^2 - 4b)X,$$

and let

$$\phi : E \longrightarrow E', \qquad \phi(x,y) = \left(\frac{y^2}{x^2}, \frac{y(b - x^2)}{x^2}\right),$$

be the isogeny of degree 2 with kernel $E[\phi] = \bigl\{O, (0,0)\bigr\}$. Let

$$S = M_K^\infty \cup \bigl\{v \in M_K^0 : v(2) \neq 0 \textit{ or } v(b) \neq 0 \textit{ or } v(a^2 - 4b) \neq 0\bigr\}.$$

Further, for each $d \in K^*$, let C_d/K be the homogeneous space for E/K given by the equation

$$C_d : dw^2 = d^2 - 2adz^2 + (a^2 - 4b)z^4.$$

Then there is an exact sequence

$$\begin{array}{rcl} 0 \longrightarrow E'(K)/\phi\bigl(E(K)\bigr) & \xrightarrow{\delta} & K(S,2) \longrightarrow \mathrm{WC}(E/K)[\phi], \\ (X,Y) & \longmapsto & X, \qquad d \longmapsto \{C_d/K\}, \\ O & \longmapsto & 1, \\ (0,0) & \longmapsto & a^2 - 4b. \end{array}$$

The ϕ-Selmer group is

$$S^{(\phi)}(E/K) \cong \bigl\{d \in K(S,2) : C_d(K_v) \neq \emptyset \textit{ for all } v \in S\bigr\}.$$

Finally, the map

$$\psi : C_d \longrightarrow E', \qquad \psi(z,w) = \left(\frac{d}{z^2}, -\frac{dw}{z^3}\right),$$

has the property that if $P \in C_d(K)$, then

$$\delta\bigl(\psi(P)\bigr) \equiv d \pmod{(K^*)^2}.$$

Remark 4.9.1. Note that since the isogenous curve E' in (X.4.9) has the same form as E, everything in (X.4.9) applies equally well to the dual isogeny $\hat{\phi} : E' \to E$. Then, using the exact sequence (X.4.7), we can try to compute $E(K)/2E(K)$.

Remark 4.9.2. If E/K is an elliptic curve that has a K-rational 2-torsion point, then (III.4.5) says that E automatically has an isogeny of degree 2 defined over K. Thus the procedure described in (X.4.8) may be applied to any elliptic curve satisfying $E(K)[2] \neq 0$. In particular, (X.4.9) in some sense subsumes (X.1.4), which described how to try to compute $E(K)/2E(K)$ when $E[2] \subset E(K)$.

Example 4.10. We use (X.4.9) to compute $E(\mathbb{Q})/2E(\mathbb{Q})$ for the elliptic curve

$$E : y^2 = x^3 - 6x^2 + 17x.$$

This equation has discriminant $\Delta = -147968 = -2^9 17^2$, so our set S is $\{\infty, 2, 17\}$ and we may identify $\mathbb{Q}(S, 2)$ with $\{\pm 1, \pm 2, \pm 17, \pm 34\}$. The curve that is 2-isogenous to E has equation

$$E : Y^2 = X^3 + 12X^2 - 32X,$$

and for $d \in \mathbb{Q}(S, 2)$, the corresponding homogeneous space is

$$C_d : dw^2 = d^2 + 12dz^2 - 32z^4.$$

From (X.4.9) we know that the point $(0, 0) \in E'(\mathbb{Q})$ maps to

$$\delta(0, 0) = -32 \equiv -2 \pmod{(\mathbb{Q}^*)^2},$$

so $-2 \in S^{(\phi)}(E/\mathbb{Q})$. It remains to check the other values of $d \in \mathbb{Q}(S, 2)$.

$$\boxed{d = 2} \qquad C_2 : 2w^2 = 4 + 24z^2 - 32z^4.$$

Dividing by 2 and letting $z = Z/2$ gives the equation

$$w^2 = 2 + 3Z^2 - Z^4,$$

which by inspection has the rational point $(Z, w) = (1, 2)$. Then (X.4.9) tells us that the point $(z, w) = (\frac{1}{2}, 2) \in C_2(\mathbb{Q})$ maps to to $\psi(\frac{1}{2}, 2) = (8, -32) \in E'(\mathbb{Q})$. Further, as the theory predicts, we have $\delta(8, -32) = 8 \equiv 2 \pmod{(\mathbb{Q}^*)^2}$.

$$\boxed{d = 17} \qquad C_{17} : 17w^2 = 17^2 + 12 \cdot 17z^2 - 32z^4.$$

Suppose that $C_{17}(\mathbb{Q}_{17}) \neq \emptyset$. Since $\operatorname{ord}_{17}(17w^2)$ is odd and $\operatorname{ord}_{17}(32z^4)$ is even, we see that necessarily $z, w \in \mathbb{Z}_{17}$. But then the equation for C_{17} implies first that $z \equiv 0 \pmod{17}$, then that $w \equiv 0 \pmod{17}$, and finally that $17^2 \equiv 0 \pmod{17^3}$. This contradiction shows that $C_{17}(\mathbb{Q}_{17}) = \emptyset$, and hence that $17 \notin S^{(\phi)}(E/\mathbb{Q})$.

We now know that

$$1, -2, 2 \in S^{(\phi)}(E/\mathbb{Q}) \qquad \text{and} \qquad 17 \notin S^{(\phi)}(E/\mathbb{Q}).$$

Since $S^{(\phi)}(E/\mathbb{Q})$ is a subgroup of $\mathbb{Q}(S,2)$, we have $S^{(\phi)}(E/\mathbb{Q}) = \{\pm 1, \pm 2\}$. Further, we have shown that $E'(\mathbb{Q})$ surjects onto $S^{(\phi)}(E/\mathbb{Q})$, and hence from (X.4.2a) we see that $\text{Ш}(E/\mathbb{Q})[\phi] = 0$.

We now repeat the above computation with the roles of E and E' reversed. Thus for $d \in \mathbb{Q}(S,2)$ we look at the homogeneous space

$$C'_d : dw^2 = d^2 - 24dz^2 + 272z^4.$$

As above, the point $(0,0) \in E(\mathbb{Q})$ maps to $\delta(0,0) = 272 \equiv 17 \pmod{(\mathbb{Q}^*)^2}$. Next, if $d < 0$, then clearly $C'_d(\mathbb{R}) = \emptyset$, so $d \notin S^{(\hat{\phi})}(E'/\mathbb{Q})$. Finally, for $d = 2$, if we let $z = Z/2$, then C'_2 has the equation

$$2w^2 = 4 - 12Z^2 + 17Z^4.$$

If $C'_2(\mathbb{Q}_2) \neq \emptyset$, then necessarily $Z, w \in \mathbb{Z}_2$, and then the equation allows us to deduce successively

$$Z \equiv 0 \pmod{2}, \qquad w \equiv 0 \pmod{2}, \qquad 4 \equiv 0 \pmod{2^3}.$$

Therefore $C_2(\mathbb{Q}_2) = \emptyset$, and hence $2 \notin S^{(\hat{\phi})}(E'/\mathbb{Q})$. Thus $S^{(\hat{\phi})}(E'/\mathbb{Q}) = \{1, 17\}$ and $\text{Ш}(E'/\mathbb{Q})[\hat{\phi}] = 0$.

To recapitulate, we now know that

$$E'(\mathbb{Q})/\phi\bigl(E(\mathbb{Q})\bigr) \cong (\mathbb{Z}/2\mathbb{Z})^2 \qquad \text{and} \qquad E(\mathbb{Q})/\hat{\phi}\bigl(E'(\mathbb{Q})\bigr) \cong \mathbb{Z}/2\mathbb{Z},$$

the former being generated by $\bigl\{(0,0),\ (8,-32)\bigr\}$ and the latter by $\bigl\{(0,0)\bigr\}$. The exact sequence (X.4.7) then yields

$$E(\mathbb{Q})/2E(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2 \qquad \text{and} \qquad E'(\mathbb{Q})/2E'(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2,$$

and hence

$$E(\mathbb{Q}) \cong E'(\mathbb{Q}) \cong \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Remark 4.11. In all of the examples up to this point, we have been lucky in the sense that for every locally trivial homogeneous space that has appeared, we were able to find (by inspection) a global rational point. Another way to say this is that we have yet to see a nontrivial element of the Shafarevich–Tate group. The first examples of such spaces are due to Lind [150] and independently, but a bit later, to Reichardt [207]. For example, they proved that the curve

$$2w^2 = 1 - 17z^4$$

has no $\mathbb{Q}$-rational points, while it is easy to check that it has a point defined over every $\mathbb{Q}_p$. Shortly thereafter, Selmer [225, 227] made an extensive study of the curves $ax^3 + by^3 + cz^3 = 0$, which are homogeneous spaces for the elliptic curves $x^3 + y^3 + dz^3 = 0$. He gave many examples of locally trivial, globally nontrivial homogeneous spaces, of which the simplest is

$$3x^3 + 4y^3 + 5z^3 = 0.$$

It is a difficult problem, in general, to divide the Selmer group into the piece coming from rational points on the elliptic curve and the piece giving nontrivial elements of the Shafarevich–Tate group. At present there is no algorithm known that is guaranteed to solve this problem. The procedure that we now describe often works in practice, although it tends to lead to fairly elaborate computations in algebraic number fields.

Recall that for each integer $m \geq 2$ there is an exact sequence (X.4.2a)

$$E(K) \xrightarrow{\delta} S^{(m)}(E/K) \longrightarrow Ш(E/K)[m] \longrightarrow 0,$$

where at least in theory, the finite group $S^{(m)}(E/K)$ is effectively computable; see (X.4.5). If we knew some way of computing $Ш(E/K)[m]$, then we could find generators for $E(K)/mE(K)$, and thence for $E(K)$. Unfortunately, a general procedure for computing $Ш(E/K)[m]$ is still being sought. However, for each integer $n \geq 1$ we can combine different versions of the above exact sequence to form a commutative diagram

$$\begin{tikzcd}
E(K) \arrow[r] \arrow[d, "\text{identity map}"] & S^{(m^n)}(E/K) \arrow[r] \arrow[d] & Ш(E/K)[m^n] \arrow[r] \arrow[d, "\text{multiplication by } m^{n-1}"] & 0 \\
E(K) \arrow[r] & S^{(m)}(E/K) \arrow[r] & Ш(E/K)[m] \arrow[r] & 0
\end{tikzcd}$$

Now at least in principle, the middle column of this diagram is effectively computable. This allows us to make the following refinement to the exact sequence in (X.4.2a).

Proposition 4.12. *Let E/K be an elliptic curve. For any integers $m \geq 2$ and $n \geq 1$, let $S^{(m,n)}(E/K)$ be the image of $S^{(m^n)}(E/K)$ in $S^{(m)}(E/K)$. Then there exists an exact sequence*

$$0 \longrightarrow E(K)/mE(K) \longrightarrow S^{(m,n)}(E/K) \longrightarrow m^{n-1}Ш(E/K)[m^n] \longrightarrow 0.$$

PROOF. This is immediate from the commutative diagram given above. □

Now to find generators for $E(K)$, we can try the following procedure. Compute successively the *relative Selmer groups*

$$S^{(m)}(E/K) = S^{(m,1)}(E/K) \supset S^{(m,2)}(E/K) \supset S^{(m,3)}(E/K) \supset \cdots$$

and the *rational-point groups*

$$T_{(m,1)}(E/K) \subset T_{(m,2)}(E/K) \subset T_{(m,3)}(E/K) \subset \cdots,$$

where $T_{(m,r)}(E/K)$ is the subgroup of $S^{(m)}(E/K)$ generated by all of the points $P \in E(K)$ with height $h_x(P) \leq r$. Eventually, with sufficient perseverance, we hope to arrive at an equality

$$S^{(m,n)}(E/K) = T_{(m,r)}(E/K).$$

Once this happens, we know that $m^{n-1}Ш(E/K)[m^n] = 0$ and that the points with height $h_x(P) \leq r$ generate $E(K)/mE(K)$. The difficulty lies in the fact that as far as is currently known, there is nothing to prevent $Ш(E/K)$ from containing an element that is infinitely m-divisible, i.e., a nonzero element $\xi \in Ш(E/K)$ such that for every $n \geq 1$ there is an element $\xi_n \in Ш(E/K)$ satisfying $\xi = m^n\xi_n$. If such an element exists, then the above procedure never terminates. However, opposed to such a gloomy scenario is the following optimistic conjecture.

Conjecture 4.13. *Let E/K be an elliptic curve. Then $Ш(E/K)$ is finite.*

The finiteness of Ш has been proven for certain elliptic curves by Kolyvagin [130] and Rubin [215]. Note that the successful carrying out of the procedure described above shows only that the m-primary component of $Ш(E/K)$ is finite. This has, of course, been done in many cases. For example, in (X.4.10) we showed that $Ш(E/\mathbb{Q})[2] = 0$ for a particular elliptic curve.

We conclude this section with a beautiful result of Cassels, which says something interesting about the order of a group that is not known in general to be finite.

Theorem 4.14. ([38], [281]) *Let E/K be an elliptic curve. There exists an alternating bilinear pairing*

$$\Gamma : Ш(E/K) \times Ш(E/K) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

whose kernel on each side is exactly the subgroup of divisible elements of $Ш(E/K)$. In other words, if $\Gamma(\alpha,\beta) = 0$ for all $\beta \in Ш(E/K)$, then for every integer $N \geq 1$ there exists an element $\alpha_N \in Ш(E/K)$ satisfying $N\alpha_N = \alpha$.

In particular, if $Ш(E/K)$ is finite, then its order is a perfect square, and the same is true of any p-primary component of $Ш(E/K)$. (See Exercise 10.20.)

X.5 Twisting—Elliptic Curves

As in (X §§2,3), we let K be an arbitrary (perfect) field and we let E/K be an elliptic curve. We saw in (X.2.2) that if we consider E merely to be a curve and ignore the base point O, then the twists of E/K correspond to the elements of the (pointed) cohomology set $H^1\bigl(G_{\bar{K}/K}, \operatorname{Isom}(E)\bigr)$. The group $\operatorname{Isom}(E)$ has two natural subgroups, namely $\operatorname{Aut}(E)$ and E, where we identify E with the set of translations $\{\tau_P\}$ in $\operatorname{Isom}(E)$. We also observe that $\operatorname{Aut}(E)$ acts naturally on E. The next proposition describes $\operatorname{Isom}(E)$.

Proposition 5.1. *The map*

$$E \times \operatorname{Aut}(E) \longrightarrow \operatorname{Isom}(E), \qquad (P,\alpha) \longmapsto \tau_P \circ \alpha,$$

is a bijection of sets. It identifies $\operatorname{Isom}(E)$ with the product of E and $\operatorname{Aut}(E)$ twisted by the natural action of $\operatorname{Aut}(E)$ on E. In other words, the group $\operatorname{Isom}(E)$ is the set of ordered pairs $E \times \operatorname{Aut}(E)$ with the group law

$$(P,\alpha)\cdot(Q,\beta)=(P+\alpha Q,\alpha\circ\beta).$$

PROOF. Let $\phi\in\operatorname{Isom}(E)$. Then $\tau_{-\phi(O)}\circ\phi\in\operatorname{Aut}(E)$, so writing

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

shows that the map is surjective. On the other hand, if $\tau_P\circ\alpha=\tau_Q\circ\beta$, then evaluating at O gives $P=Q$, and then also $\alpha=\beta$. This proves injectivity. Finally, the twisted nature of the group law follows from the calculation

$$\tau_P\circ\alpha\circ\tau_Q\circ\beta=\tau_P\circ\tau_{\alpha Q}\circ\alpha\circ\beta. \qquad\square$$

We have already extensively studied those twists of E/K that arise from translations; these are the twists corresponding to elements of the group

$$H^1(G_{\bar K/K},E)\cong\operatorname{WC}(E/K)$$

that we studied in (X §§3,4). We now look at the twists of E/K coming from isomorphisms of E as an *elliptic curve*, i.e., isomorphisms of the pair (E,O). In other words, we consider the twists of E corresponding to elements of the cohomology group $H^1\bigl(G_{\bar K/K},\operatorname{Aut}(E)\bigr)$. We start with a general proposition and then, for $\operatorname{char}(K)\ne 2,3$, we derive explicit equations for the associated twists.

Remark 5.2. In the literature, the phrase "let C be a twist of E" generally means that C corresponds to an element of $H^1\bigl(G_{\bar K/K},\operatorname{Aut}(E)\bigr)$. More properly, such a C should be called a twist of the pair (E,O), since the group of isomorphisms of (E,O) with itself is the group we denote by $\operatorname{Aut}(E)$. However, one can generally resolve any ambiguity from context.

Proposition 5.3. *Let E/K be an elliptic curve.*

(a) *The natural inclusion* $\operatorname{Aut}(E)\subset\operatorname{Isom}(E)$ *induces an inclusion*

$$H^1\bigl(G_{\bar K/K},\operatorname{Aut}(E)\bigr)\subset H^1\bigl(G_{\bar K/K},\operatorname{Isom}(E)\bigr).$$

Identifying the latter set with $\operatorname{Twist}(E/K)$ *via* (X.2.2)*, we denote the former by* $\operatorname{Twist}\bigl((E,O)/K\bigr)$.

(b) *Let $C/K\in\operatorname{Twist}\bigl((E,O)/K\bigr)$. Then $C(K)\ne\emptyset$, so C/K can be given the structure of an elliptic curve over K. N.B. The curve C/K is generally not K-isomorphic to E/K; cf.* (X.3.3).

(c) *Conversely, if E'/K is an elliptic curve that is isomorphic to E over $\bar K$, then E'/K represents an element of* $\operatorname{Twist}\bigl((E,O)/K\bigr)$.

PROOF. (a) Let $i:\operatorname{Aut}(E)\to\operatorname{Isom}(E)$ be the natural inclusion. From (X.5.1), there is a homomorphism $j:\operatorname{Isom}(E)\to\operatorname{Aut}(E)$ satisfying $j\circ i=1$. It follows that the induced map

$$H^1\bigl(G_{\bar K/K},\operatorname{Aut}(E)\bigr)\xrightarrow{i}H^1\bigl(G_{\bar K/K},\operatorname{Isom}(E)\bigr)$$

is one-to-one.
(b) Let $\phi : C \to E$ be an isomorphism defined over $\bar{K}$ such that the cocycle

$$\sigma \longmapsto \phi^\sigma \circ \phi^{-1}$$

represents the element of $H^1\bigl(G_{\bar{K}/K}, \operatorname{Aut}(E)\bigr)$ corresponding to C/K. Then we have $\phi^\sigma \circ \phi^{-1}(O) = O$, so

$$\phi^{-1}(O) = \phi^{-1}(O)^\sigma \qquad \text{for all } \sigma \in G_{\bar{K}/K}.$$

Hence $\phi^{-1}(O) \in C(K)$, so $\bigl(C, \phi^{-1}(O)\bigr)$ is an elliptic curve defined over K.
(c) Let $\phi : E' \to E$ be a $\bar{K}$-isomorphism of elliptic curves, so in particular, $\phi(O') = O$, where $O \in E(K)$ and $O' \in E'(K)$ are the respective zero points of E and E'. Then for any $\sigma \in G_{\bar{K}/K}$ we have

$$\phi^\sigma \circ \phi^{-1}(O) = \phi^\sigma(O') = \phi(O')^\sigma = O^\sigma = O.$$

Thus $\phi^\sigma \circ \phi^{-1} \in \operatorname{Aut}(E)$, so the cocycle corresponding to E'/K lies in the group $H^1\bigl(G_{\bar{K}/K}, \operatorname{Aut}(E)\bigr)$ as desired. □

If the characteristic of K is not equal to 2 or 3, then the elements of the group $\operatorname{Twist}\bigl((E, O)/K\bigr)$ can be described quite explicitly.

Proposition 5.4. *Assume that* $\operatorname{char}(K) \ne 2, 3$*, and let*

$$n = \begin{cases} 2 & \textit{if } j(E) \ne 0, 1728, \\ 4 & \textit{if } j(E) = 1728, \\ 6 & \textit{if } j(E) = 0. \end{cases}$$

Then $\operatorname{Twist}\bigl((E, O)/K\bigr)$ *is canonically isomorphic to* $K^*/(K^*)^n$*.*

More precisely, choose a Weierstrass equation

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

for E/K, and let $D \in K^*$. Then the elliptic curve $E_D \in$ $\operatorname{Twist}\bigl((E, O)/K\bigr)$ *corresponding to D* $(\operatorname{mod} (K^*)^n)$ *has Weierstrass equation*

(i) $E_D : y^2 = x^3 + D^2Ax + D^3B$ *if* $j(E) \ne 0, 1728$,

(ii) $E_D : y^2 = x^3 + DAx$ *if* $j(E) = 1728$ (*so* $B = 0$),

(iii) $E_D : y^2 = x^3 + DB$ *if* $j(E) = 0$ (*so* $A = 0$).

Corollary 5.4.1. *Define an equivalence relation on the set $K \times K^*$ by*

$$(j, D) \sim (j', D') \qquad \textit{if} \quad j = j' \quad \textit{and} \quad D/D' \in (K^*)^{n(j)},$$

where $n(j) = 2$ (*respectively* 4*, respectively* 6) *if* $j \ne 0, 1728$ (*respectively* $j = 1728$*, respectively* $j = 0$)*. Then the K-isomorphism classes of elliptic curves E/K are in one-to-one correspondence with the elements of the quotient*

$$\frac{K \times K^*}{\sim}.$$

PROOF. From (III.10.2.) we have an isomorphism

$$\operatorname{Aut}(E) \cong \boldsymbol{\mu}_n$$

of $G_{\bar{K}/K}$-modules. It follows from (B.2.5c) that

$$\operatorname{Twist}\bigl((E,O)/K\bigr) = H^1\bigl(G_{\bar{K}/K}, \operatorname{Aut}(E)\bigr) \cong H^1(G_{\bar{K}/K}, \boldsymbol{\mu}_n) \cong K^*/(K^*)^n.$$

The calculation of an equation for the twist of E is straightforward. The case $j(E) \neq 0, 1728$ was done in (X.2.4). We do $j(E) = 1728$ here and leave $j(E) = 0$ for the reader.

Thus let $D \in K^*$, let $\delta \in \bar{K}$ be a fourth root of D, and define a cocycle

$$\xi : G_{\bar{K}/K} \longrightarrow \boldsymbol{\mu}_4, \qquad \xi_\sigma = \delta^\sigma/\delta.$$

We also fix an isomorphism

$$[\ ] : \boldsymbol{\mu}_4 \longrightarrow \operatorname{Aut}(E), \qquad [\zeta](x,y) = (\zeta^2 x, \zeta y).$$

Then E_D corresponds to the cocycle $\sigma \mapsto [\xi_\sigma]$ in $H^1\bigl(G_{\bar{K}/K}, \operatorname{Aut}(E)\bigr)$.

The action of $G_{\bar{K}/K}$ on the twisted field $\bar{K}(E)_\xi$ is given by

$$\delta^\sigma = \xi_\sigma \delta, \qquad x^\sigma = \xi_\sigma^2 x, \qquad y^\sigma = \xi_\sigma y.$$

The subfield fixed by $G_{\bar{K}/K}$ thus contains the functions

$$X = \delta^{-2} x \qquad \text{and} \qquad Y = \delta^{-1} y,$$

and these functions satisfy the equation

$$Y^2 = DX^3 + AX.$$

This gives an equation for the twist E_D/K, and the substitution

$$(X,Y) = (D^{-1}X', D^{-1}Y')$$

puts it into the desired form.

The corollary follows by combining the proposition and (X.5.3c) with (III.1.4bc), which says that up to $\bar{K}$-isomorphism, the elliptic curves E/K are in one-to-one correspondence with their j-invariants $j(E) \in K$. □

X.6 The Curve $Y^2 = X^3 + DX$

Many of the deepest theorems and conjectures in the arithmetic theory of elliptic curves have had as their testing ground one of the families of curves given in (X.5.4). To illustrate the theory that we have developed, let's see what we can say about the family of elliptic curves $E/\mathbb{Q}$ with j-invariant $j(E) = 1728$.

One such curve is given by the equation

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

and then (X.5.3) and (X.5.4) tell us that every such curve has an equation of the form

$$E : y^2 = x^3 + Dx,$$

where D ranges over representatives for the cosets in $\mathbb{Q}^*/(\mathbb{Q}^*)^4$. Thus if we specify that D is a fourth-power-free integer, then D is uniquely determined by E. We observe that the equation for E has discriminant $\Delta(E) = -64D^3$, so E has good reduction at all primes not dividing $2D$, and the given Weierstrass equation is minimal at all odd primes.

Let p be a prime not dividing $2D$ and consider the reduced curve $\tilde{E}$ over the finite field $\mathbb{F}_p$. From (V.4.1) we find that $\tilde{E}$ is supersingular if and only if the coefficient of x^{p-1} in $(x^3 + Dx)^{(p-1)/2}$ is zero. In particular, if $p \equiv 3 \pmod 4$, then $\tilde{E}/\mathbb{F}_p$ is supersingular, and hence we conclude (see Exercise 5.10) that

$$\#\tilde{E}(\mathbb{F}_p) = p + 1 \qquad \text{for all } p \equiv 3 \pmod 4.$$

(See Exercise 10.17 for an elementary derivation of this result.)

Next we recall from (VII.3.5) that if $p \neq 2$ and if E has good reduction at p, then $E_{\text{tors}}(\mathbb{Q})$ injects into the reduction $\tilde{E}(\mathbb{F}_p)$. It follows from this discussion that $\#E_{\text{tors}}(\mathbb{Q})$ divides $p+1$ for all but finitely many primes $p \equiv 3 \pmod 4$, and hence that $\#E_{\text{tors}}(\mathbb{Q})$ divides 4. Since $(0,0) \in E(\mathbb{Q})[2]$, the possibilities for $E_{\text{tors}}(\mathbb{Q})$ are $\mathbb{Z}/2\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^2$, and $\mathbb{Z}/4\mathbb{Z}$.

We have $E[2] \subset E(\mathbb{Q})$ if and only if the polynomial $x^3 + Dx$ factors completely over $\mathbb{Q}$, so if and only if $-D$ is a perfect square. Similarly, $E(\mathbb{Q})$ has a point of order 4 if and only if $(0,0) \in 2E(\mathbb{Q})$. The duplication formula for E reads

$$x(2P) = \frac{(x^2 - D)^2}{4x^3 + 4Dx},$$

so we see that

$$(0,0) = [2]\bigl(D^{1/2}, (4D^3)^{1/4}\bigr).$$

Hence assuming that D is a fourth-power-free integer, we conclude that

$$(0,0) \in 2E(\mathbb{Q}) \quad \text{if and only if} \quad D = 4,$$

in which case $(0,0) = [2](2, \pm 4)$.

Next, since $E(\mathbb{Q})$ contains a 2-torsion point, we can use (X.4.9) to try to calculate $E(\mathbb{Q})/2E(\mathbb{Q})$. The curve E is isogenous to the curve

$$E' : Y^2 = X^3 - 4DX$$

via the isogeny

$$\phi : E \longrightarrow E', \qquad \phi(x,y) = \left(\frac{y^2}{x^2}, \frac{y(D-x^2)}{x^2}\right).$$

The set $S \subset M_{\mathbb{Q}}$ consists of ∞ and the primes dividing $2D$, and for each $d \in \mathbb{Q}(S,2)$, the corresponding homogeneous space $C_d/\mathbb{Q} \in \mathrm{WC}(E/\mathbb{Q})$ is given by the equation

$$C_d : dw^2 = d^2 - 4Dz^4.$$

Similarly, working with the dual isogeny $\hat{\phi} : E' \to E$ leads to the homogeneous spaces $C'_d/\mathbb{Q} \in \mathrm{WC}(E'/\mathbb{Q})$ with equations

$$C'_d : dW^2 = d^2 + DZ^4.$$

(More precisely, using (X.4.9) leads to the equation $dW^2 = d^2 + 16DZ^4$, but we are free to replace Z with $Z/2$.)

Let $\nu(2D)$ denote the number of distinct primes dividing $2D$. The group $\mathbb{Q}(S,2)$ is generated by -1 and the primes dividing $2D$, so we have the estimate

$$\dim_2 E(\mathbb{Q})/2E(\mathbb{Q}) \le 2 + 2\nu(2D) - \dim_2 E'(\mathbb{Q})[\hat{\phi}] + \dim_2 \phi\bigl(E(\mathbb{Q})[2]\bigr).$$

Here $\dim_2$ denotes the dimension of an $\mathbb{F}_2$-vector space. We clearly have

$$E'(\mathbb{Q})[\hat{\phi}] \cong \mathbb{Z}/2\mathbb{Z}.$$

In order to deal with the other two terms, we consider two cases.

(1) $E(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$.
Then $\phi\bigl(E(\mathbb{Q})[2]\bigr) \cong 0$ and $\dim_2 E(\mathbb{Q})/2E(\mathbb{Q}) = \operatorname{rank} E(\mathbb{Q}) + 1$.

(2) $E(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
Then $\phi\bigl(E(\mathbb{Q})[2]\bigr) \cong \mathbb{Z}/2\mathbb{Z}$ and $\dim_2 E(\mathbb{Q})/2E(\mathbb{Q}) = \operatorname{rank} E(\mathbb{Q}) + 2$.

Substituting these values into the above inequality yields in both cases the estimate

$$\operatorname{rank} E(\mathbb{Q}) \le 2\nu(2D).$$

Notice that we have obtained this upper bound without having checked for local triviality of any of the homogeneous spaces C_d and C'_d. By inspection, if $d < 0$, then either $C_d(\mathbb{R}) = \emptyset$ or $C'_d(\mathbb{R}) = \emptyset$. Thus the upper bound my be decreased by 1, giving the small improvement

$$\operatorname{rank} E(\mathbb{Q}) \le 2\nu(2D) - 1.$$

The preceding discussion is summarized in the following proposition.

Proposition 6.1. *Let $D \in \mathbb{Z}$ be a fourth-power-free integer, and let E_D be the elliptic curve*

$$E_D : y^2 = x^3 + Dx.$$

(a)

$$E_{D,\text{tors}}(\mathbb{Q}) \cong \begin{cases} \mathbb{Z}/4\mathbb{Z} & \textit{if } D = 4, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \textit{if } -D \textit{ is a perfect square,} \\ \mathbb{Z}/2\mathbb{Z} & \textit{otherwise.} \end{cases}$$

(b)

$$\operatorname{rank} E(\mathbb{Q}) \le 2\nu(2D) - 1.$$

Remark 6.1.1. The estimate in (X.6.1b) cannot be improved in general. For example, the curve $E : y^2 = x^3 - 82x$ has

$$\operatorname{rank} E(\mathbb{Q}) = 3,$$

while $\nu(-164) = \nu(2^4 \cdot 41) = 2$. See Exercise 10.18.

We now restrict attention to the special case that $D = p$ is an odd prime. The next proposition gives a complete description of the relevant Selmer groups and deduces corresponding upper bounds for the rank of $E(\mathbb{Q})$ and the dimension of $Ш(E/\mathbb{Q})[2]$.

Proposition 6.2. *Let p be an odd prime, let E_p be the elliptic curve*

$$E_p : y^2 = x^3 + px,$$

and let $\phi : E_p \to E'_p$ be the isogeny of degree 2 with kernel $E_p[\phi] = \bigl\{O, (0,0)\bigr\}$.
(a)

$$E_{p,\text{tors}}(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}.$$

(b)

$$S^{(\hat{\phi})}(E'_p/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}.$$

$$S^{(\phi)}(E_p/\mathbb{Q}) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} & \textit{if } p \equiv 7, 11 \pmod{16}, \\ (\mathbb{Z}/2\mathbb{Z})^2 & \textit{if } p \equiv 3, 5, 13, 15 \pmod{16}, \\ (\mathbb{Z}/2\mathbb{Z})^3 & \textit{if } p \equiv 1, 9 \pmod{16}. \end{cases}$$

(c)

$$\operatorname{rank} E_p(\mathbb{Q}) + \dim_2 Ш(E_p/\mathbb{Q})[2] = \begin{cases} 0 & \textit{if } p \equiv 7, 11 \pmod{16}, \\ 1 & \textit{if } p \equiv 3, 5, 13, 15 \pmod{16}, \\ 2 & \textit{if } p \equiv 1, 9 \pmod{16}. \end{cases}$$

PROOF. To ease notation, we let $E = E_p$ and $E' = E'_p$.
(a) This is a special case of (X.6.1a).
(b) As usual, we take representatives $\{\pm 1, \pm 2, \pm p, \pm 2p\}$ for the cosets in the finite group $\mathbb{Q}(S, 2)$. From (X.4.9) we know that the images of the 2-torsion points in the Selmer groups are given by

$$-p \in S^{(\phi)}(E/\mathbb{Q}) \qquad \text{and} \qquad p \in S^{(\hat{\phi})}(E'/\mathbb{Q}).$$

Further, if $d < 0$, then $C_d(\mathbb{R}) = \emptyset$, so $d \notin S^{(\hat{\phi})}(E'/\mathbb{Q})$.

Next we consider the homogeneous space

$$C_2' : 2W^2 = 4 + pZ^4.$$

If $(Z, W) \in C_2'(\mathbb{Q}_2)$, then necessarily $Z, W \in \mathbb{Z}_2$, which allows us to conclude that $Z \equiv 0 \pmod{2}$, so $W \equiv 0 \pmod{2}$, and thus $0 \equiv 4 \pmod{8}$. Therefore $C_2'(\mathbb{Q}_2) = \emptyset$, and hence $2 \notin S^{(\hat{\phi})}(E'/\mathbb{Q})$. We now know that

$$p \in S^{(\hat{\phi})}(E'/\mathbb{Q}) \qquad \text{and} \qquad -1, \pm 2, -p, -2p \notin S^{(\hat{\phi})}(E'/\mathbb{Q}).$$

It follows that $S^{(\hat{\phi})}(E'/\mathbb{Q}) = \{1, p\} \equiv \mathbb{Z}/2\mathbb{Z}$.

It remains to calculate $S^{(\phi)}(E/\mathbb{Q})$, and from the form of the answer, it is clear that there will be many cases to be considered. The best approach is to look at the various $d \in \mathbb{Q}(S, 2)$ and check for which primes the homogeneous space is locally trivial. Note that (X.4.9) says that

$$d \in S^{(\phi)}(E/\mathbb{Q}) \qquad \text{if and only if} \qquad C_d(\mathbb{Q}_p) \neq \emptyset \quad \text{and} \quad C_d(\mathbb{Q}_2) \neq \emptyset,$$

i.e., it suffices to check whether C_d is locally trivial at the primes p and 2. We make frequent use of Hensel's lemma (Exercise 10.12), which gives a criterion for when a solution of an equation modulo q^n lifts to a solution in $\mathbb{Q}_q$.

$\boxed{d = -1}$ $$C_{-1} : w^2 + 1 = 4pz^4.$$

(i) If $(z, w) \in C_{-1}(\mathbb{Q}_p)$, then necessarily $z, w \in \mathbb{Z}_p$, so $w^2 \equiv -1 \pmod{p}$. Conversely, from Exercise 10.12 we see that any solution to the congruence $w^2 \equiv -1 \pmod{p}$ lifts to a point in $C_{-1}(\mathbb{Q}_p)$. Therefore

$$C_{-1}(\mathbb{Q}_p) \neq \emptyset \quad \Longleftrightarrow \quad p \equiv 1 \pmod{4}.$$

(ii) From (i) we may assume that $p \equiv 1 \pmod{4}$. If $p \equiv 1 \pmod{8}$, then we let

$$(z, w) = (Z/4, W/8).$$

Our equation becomes $W^2 + 64 = pZ^4$, and the solution $(1, 1)$ to the congruence

$$W^2 + 64 \equiv pZ^4 \pmod{8}$$

lifts to a point in $C_{-1}(\mathbb{Q}_2)$. Similarly, if $p \equiv 5 \pmod{8}$, then we let

$$(z, w) = (Z/2, W/2)$$

and consider the solution $(Z, W) = (1, 1)$ to the congruence

$$W^2 + 4 = pZ^4 \pmod{8}.$$

This solution lifts to a point in $C_{-1}(\mathbb{Q}_2)$. This shows that if $p \equiv 1 \pmod{4}$, then $C_{-1}(\mathbb{Q}_2) \neq \emptyset$.

Combining (i) and (ii) yields

$$-1 \in S^{(\phi)}(E/\mathbb{Q}) \iff p \equiv 1 \pmod 4.$$

$\boxed{d=-2}$ $$C_{-2} : w^2 + 2 = 2pz^4.$$

(i) If $(z,w) \in C_{-2}(\mathbb{Q}_p)$, then $z,w \in \mathbb{Z}_p$ and $w^2 \equiv -2 \pmod p$. Conversely, a solution to $w^2 \equiv -2 \pmod p$ lifts to a point of $C_{-1}(\mathbb{Q}_p)$. Therefore

$$C_{-2}(\mathbb{Q}_p) \neq \emptyset \iff p \equiv 1,3 \pmod 8.$$

(ii) If $(z,w) \in C_{-2}(\mathbb{Q}_2)$, then $z,w \in \mathbb{Z}_2$ and $w \equiv 0 \pmod 2$. So after setting $(z,w) = (Z, 2W)$, we must check whether the equation

$$2W^2 + 1 = pZ^4$$

has any solutions $Z, W \in \mathbb{Z}_2$. From (i) we see that it suffices to consider primes $p \equiv 1,3 \pmod 8$. The congruence $2W^2 + 1 \equiv pZ^4 \pmod{16}$ has no solutions if $p \equiv 11 \pmod{16}$, so

$$p \equiv 11 \pmod{16} \implies C_{-2}(\mathbb{Q}_2) = \emptyset.$$

On the other hand, if we can find solutions modulo $2^5 = 32$, then Exercise 10.12 says that they lift to points in $C_{-2}(\mathbb{Q}_2)$. The following table gives solutions (Z,W) to the congruence

$$2W^2 + 1 \equiv pZ^4 \pmod{32}$$

for each of the remaining values of p mod 32:

p mod 32	1	3	9	17	19	25
(Z,W)	$(1,0)$	$(3,11)$	$(1,2)$	$(3,0)$	$(1,3)$	$(3,2)$

Combining (i) and (ii), we have proven that

$$-2 \in S^{(\phi)}(E/\mathbb{Q}) \iff p \equiv 1,3,9 \pmod{16}.$$

$\boxed{d=2}$ $$C_2 : w^2 = 2 - 2pz^4.$$

This case is entirely similar to the case $d = -2$ that we just completed. A point $(z,w) \in C_2(\mathbb{Q}_p)$ has $z,w \in \mathbb{Z}_p$ and $w^2 \equiv 2 \pmod p$, and any such solutions lifts, so

$$C_2(\mathbb{Q}_p) \neq \emptyset \iff p \equiv 1,7 \pmod 8.$$

Next, if $p \equiv 1 \pmod 8$, then from above we have $-1, -2 \in S^{(\phi)}(E/\mathbb{Q})$, so certainly $2 \in S^{(\phi)}(E/\mathbb{Q})$. It remains to consider the case $p \equiv 7 \pmod 8$.

A point $(z,w) \in C_2(\mathbb{Q}_2)$ satisfies $(z,w) = (Z, 2W)$ with $Z, W \in \mathbb{Z}_2$ and

$$2W^2 = 1 - pZ^4.$$

If $p \equiv 7 \pmod{16}$, then this equation has no solutions modulo 16. On the other hand, if $p \equiv 15 \pmod{16}$, then we have solutions

$$\begin{aligned} 2 \cdot 3^2 &\equiv 1 - p \cdot 1^4 \pmod{32} &\qquad& \text{if } p \equiv 15 \pmod{32}, \\ 2 \cdot 1^2 &\equiv 1 - p \cdot 1^4 \pmod{32} && \text{if } p \equiv 31 \pmod{32}, \end{aligned}$$

and these solutions lift to points in $C_2(\mathbb{Q}_2)$. Putting all of this together, we have shown that

$$2 \in S^{(\phi)}(E/\mathbb{Q}) \quad\Longleftrightarrow\quad p \equiv 1, 9, 15 \pmod{16}.$$

We have now determined exactly which of the values -1, 2, and -2 are in $S^{(\phi)}(E/\mathbb{Q})$ in terms of the residue of p modulo 16. Since we also know that $-p \in S^{(\phi)}(E/\mathbb{Q})$, it is now a simple matter to reconstruct the table for $S^{(\phi)}(E/\mathbb{Q})$ given in (b). In fact, we obtain more information, namely a precise list of which elements of $\mathbb{Q}(S, 2)$ are in $S^{(\phi)}(E/\mathbb{Q})$.

(c) We use (X.4.7) and (X.4.2a) to compute

$$\begin{aligned} \dim_2 E'(\mathbb{Q})[\hat{\phi}]/\phi\bigl(E(\mathbb{Q})[2]\bigr) &+ \dim_2 E(\mathbb{Q})/2E(\mathbb{Q}) \\ &= \dim_2 E'(\mathbb{Q})/\phi\bigl(E(\mathbb{Q})\bigr) + \dim_2 E(\mathbb{Q})/\hat{\phi}\bigl(E(\mathbb{Q})\bigr) \\ &= \dim_2 S^{(\phi)}(E/\mathbb{Q}) - \dim_2 Ш(E/\mathbb{Q})[\phi] \\ &\qquad + \dim_2 S^{(\hat{\phi})}(E'/\mathbb{Q}) - \dim_2 Ш(E'/\mathbb{Q})[\hat{\phi}]. \end{aligned}$$

From (a) we see that

$$E'(\mathbb{Q})/\phi\bigl(E(\mathbb{Q})[2]\bigr) \cong \mathbb{Z}/2\mathbb{Z} \qquad \text{and} \qquad E(\mathbb{Q})/2E(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^{1+\operatorname{rank} E(\mathbb{Q})}.$$

Further, since $E(\mathbb{Q})/\hat{\phi}\bigl(E'(\mathbb{Q})\bigr) \cong S^{(\hat{\phi})}(E'/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$ from (b), the exact sequence given in (X.4.2a) implies that $Ш(E'/\mathbb{Q})[\hat{\phi}] = 0$. Hence the exact sequence

$$0 \longrightarrow Ш(E/\mathbb{Q})[\phi] \longrightarrow Ш(E/\mathbb{Q})[2] \xrightarrow{\phi} Ш(E'/\mathbb{Q})[\hat{\phi}] = 0$$

gives

$$\dim Ш(E/\mathbb{Q})[2] = \dim_2 Ш(E/\mathbb{Q})[\phi],$$

and combining this with the above results yields

$$1 + \bigl(1 + \operatorname{rank} E(\mathbb{Q})\bigr) = \dim_2 S^{(\phi)}(E/\mathbb{Q}) + \dim_2 S^{(\hat{\phi})}(E'/\mathbb{Q}) - \dim_2 Ш(E/\mathbb{Q})[2].$$

Now (c) is immediate from the calculation of $S^{(\phi)}(E/\mathbb{Q})$ and $S^{(\hat{\phi})}(E'/\mathbb{Q})$ given in (b). □

Corollary 6.2.1. *There are infinitely many elliptic curves $E/\mathbb{Q}$ satisfying*

$$\operatorname{rank} E(\mathbb{Q}) = 0 \qquad \textit{and} \qquad Ш(E/\mathbb{Q})[2] = 0.$$

PROOF. From (X.6.2), the elliptic curves $y^2 = x^3 + px$ with $p \equiv 7, 11 \pmod{16}$ have this property. □

Remark 6.3. One of the consequences of (X.6.2) is that if p is a prime satisfying $p \equiv 5 \pmod 8$, then the elliptic curve

$$E_p : y^2 = x^3 + px$$

has rank at most one. Further, examining the proof of (X.6.2) shows that the group $E_p(\mathbb{Q})$ has rank 1 if and only if the homogeneous space

$$C_{-1} : w^2 + 1 = 4pz^4$$

has a $\mathbb{Q}$-rational point, and if there is such a point, then we can find a point of infinite order in $E(\mathbb{Q})$ by using the map

$$\hat{\phi} \circ \psi : C_1 \longrightarrow E, \qquad \hat{\phi} \circ \psi(z, w) = \left(\frac{w^2}{4z^2}, \frac{w(w^2+2)}{8z^3} \right);$$

cf. (X.4.9). Taking the first few primes $p \equiv 5 \pmod 8$, in each case we find points in $C_{-1}(\mathbb{Q})$, and these give points of infinite order in $E_p(\mathbb{Q})$ as listed in the following table:

p	5	13	29	37
(x, y)	$\left(\frac{1}{4}, \frac{9}{8}\right)$	$\left(\frac{9}{4}, \frac{51}{8}\right)$	$\left(\frac{25}{4}, \frac{165}{8}\right)$	$\left(\frac{22801}{900}, \frac{3540799}{27000}\right)$

Suppose that we knew, a priori, that the Shafarevich–Tate group $Ш(E_p/\mathbb{Q})$ was finite, or even that its 2-primary component was finite. Then the existence of the Cassels pairing (X.4.14) implies that $\dim_2 Ш(E_p/\mathbb{Q})[2]$ is even, and hence that $E_p(\mathbb{Q})$ has rank 1 for *all* primes $p \equiv 5 \pmod 8$. This also follows from a conjecture of Selmer [226] concerning the difference between the number of "first and second descents," and it is also a consequence of the conjecture of Birch and Swinnerton-Dyer (C.16.5). Bremner and Cassels [26, 27] have verified numerically that $\operatorname{rank} E_p(\mathbb{Q}) = 1$ for all such primes less than 20000, and Monsky [182] has shown that $\operatorname{rank} E_p(\mathbb{Q}) = 1$ for all primes $p \equiv 5 \pmod{16}$.

In order to give the reader an idea of the magnitude of the solutions that may occur, we mention that for $p = 877$, the Mordell–Weil group of the elliptic curve

$$y^2 = x^3 + 877x$$

is generated by the 2-torsion point $(0, 0)$ and the point

$$\left(\frac{612776083187947368101^2}{7884153586068390021 0^2}, \frac{256256267988926809388776834045513089648669153204356603464786949}{78841535860683900210^3} \right).$$

Similarly, if $p \equiv 3, 15 \pmod{16}$ and if the 2-primary component of $Ш(E_p/\mathbb{Q})$ is finite, then (X.6.2) and (X.4.14) imply that $E_p(\mathbb{Q})$ has rank exactly one. Thefact that the rank is one for any particular prime p may be verified numerically by searching for a point in $C_{-2}(\mathbb{Q})$ and $C_2(\mathbb{Q})$ respectively. See, for example, the tables in [20] and [54] and online at [53] and [274].

Remark 6.4. If $p \equiv 7, 11 \pmod{16}$, then (X.6.2c) says that $E_p(\mathbb{Q})$ consists of only two points, while if $p \equiv 3, 5, 13, 15 \pmod{16}$, then (X.6.2c) combined with the reasonable conjecture that $Ш(E_p/\mathbb{Q})[2^\infty]$ is finite tells us that $E_p(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$. In the remaining case, namely $p \equiv 1 \pmod 8$, there are two possibilities. First, $E_p(\mathbb{Q})$ might have rank 2. This can certainly occur. For example, the curves

$$y^2 = x^3 + 73x \qquad \text{and} \qquad y^2 = x^3 + 89x$$

both have rank 2, independent points being given by

$$\left(\frac{9}{16}, \frac{411}{64}\right), (36, 222) \in E_{73}(\mathbb{Q}) \quad \text{and} \quad \left(\frac{25}{16}, \frac{765}{64}\right), \left(\frac{4}{9}, \frac{170}{27}\right) \in E_{89}(\mathbb{Q}).$$

Second, $E_p(\mathbb{Q})$ might have rank 0, in which case $Ш(E_p/\mathbb{Q})[2] \cong (\mathbb{Z}/2\mathbb{Z})^2$. (Note that $\operatorname{rank} E_p(\mathbb{Q}) = 1$ is precluded if we assume that $Ш(E/\mathbb{Q})$ is finite.) The next proposition gives a fairly general condition under which the second possibility holds. It also provides our first examples of homogeneous spaces that are everywhere locally trivial, but have no global rational points.

Proposition 6.5. *Let $p \equiv 1 \pmod 8$ be a prime for which 2 is* not *a quartic residue.*

(a) *The curves*

$$w^2 + 1 = 4pz^4, \qquad w^2 + 2 = 2pz^4, \qquad w^2 + 2pz^4 = 2,$$

have points defined over every completion of $\mathbb{Q}$, but they have no $\mathbb{Q}$-rational points.

(b) *The elliptic curve*

$$E_p : y^2 = x^3 + px$$

satisfies

$$\operatorname{rank} E_p(\mathbb{Q}) = 0 \qquad \textit{and} \qquad Ш(E_p/\mathbb{Q})[2] \cong (\mathbb{Z}/2\mathbb{Z})^2.$$

Remark 6.5.1. Any prime $p \equiv 1 \pmod 8$ can be written as $p = A^2 + B^2$ with $A, B \in \mathbb{Z}$ satisfying $AB \equiv 0 \pmod 4$. A theorem of Gauss, which we prove later in this section (X.6.6), says that 2 is a quartic residue modulo p if and only if $AB \equiv 0 \pmod 8$. Thus, for example, 2 is a quartic nonresidue for the primes

$$17 = 1^2 + 4^2, \quad 41 = 5^2 + 4^2, \quad 97 = 9^2 + 4^2, \quad \text{and} \quad 193 = 7^2 + 12^2,$$

so these primes satisfy the conclusion of (X.6.5).

PROOF OF (X.6.5). During the course of proving (X.6.2b), we showed that the Selmer group $S^{(p)}(E_p/\mathbb{Q}) \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$ is given by $\{\pm 1, \pm 2, \pm p, \pm 2p\}$. Further, we showed that $-p$ is the image of the 2-torsion point $(0,0) \in E_p(\mathbb{Q})$. Thus in order to show that $Ш(E_p/\mathbb{Q})[\phi]$ has order 4, it suffices to prove that the homogeneous spaces C_{-1}, C_2, and C_{-2} have no $\mathbb{Q}$-rational points. These are the three curves listed in (a), and so, once we prove that they have no $\mathbb{Q}$-rational points, all of (X.6.5) will follow from (X.6.2). Our proof is based on ideas of Lind and Mordell [150, 41]; see also [207, 184, 20].

Case I.

$$C_{\pm 2} : w^2 = 2 - 2pz^4.$$

Suppose that $(z, w) \in C_{\pm 2}(\mathbb{Q})$. Writing z and w in lowest terms, we see that they necessarily have the form $(z, w) = (r/t, 2s/t^2)$, where $r, s, t \in \mathbb{Z}$ satisfy

$$\pm 2s^2 = t^4 - pr^4 \qquad \text{and} \qquad \gcd(r, s, t) = 1.$$

We write $(a|b)$ for the Legendre symbol. Let q be an odd prime dividing s. Then $(p|q) = 1$, so $(q|p) = 1$ by quadratic reciprocity. Since also $(2|p) = 1$, we see that $(s|p) = 1$, so $(s^2|p)_4 = 1$, i.e., s^2 is a quartic residue modulo p. Now the equation implies that $(\pm 2|p)_4 = 1$. But -1 is always a quartic residue for primes $p \equiv 1 \pmod 8$, while by assumption 2 is a quartic nonresidue modulo p. This contradiction proves that $C_{\pm 2}(\mathbb{Q}) = \emptyset$.

Case II.

$$C_{-1} : -w^2 = 1 - 4pz^4.$$

Writing $(z, w) \in C_{-1}(\mathbb{Q})$ in (almost) lowest terms as $(z, w) = (r/2t, s/2t^2)$, we have

$$s^2 + 4t^4 = pr^4 \qquad \text{with} \qquad \gcd(r, t) = 1.$$

(We do not preclude the possibility that r is even.) Since $p \equiv 1 \pmod 4$, there are integers $A \equiv 1 \pmod 2$ and $B \equiv 0 \pmod 2$ such that

$$p = A^2 + B^2.$$

It is a simple matter to verify the identity

$$(pr^2 + 2Bt^2)^2 = p(Br^2 + 2t^2)^2 + A^2s^2,$$

from which we obtain the factorization

$$(pr^2 + 2Bt^2 + As)(pr^2 + 2Bt^2 - As) = p(Br^2 + 2t^2)^2.$$

It is not difficult to check that $\gcd(pr^2 + 2Bt^2 + As, pr^2 + 2Bt^2 - As)$ is either a square or twice a square; up to multiplication by 2, it is a square divisor of $\gcd(A, s)^2$. Hence the above factorization implies that there are integers u and v satisfying

$$\left[\begin{array}{r} pr^2 + 2Bt^2 \pm As = pu^2 \\ pr^2 + 2Bt^2 \mp As = v^2 \\ Br^2 + 2t^2 = uv \end{array}\right] \qquad \text{or} \qquad \left[\begin{array}{r} pr^2 + 2Bt^2 \pm As = 2pu^2 \\ pr^2 + 2Bt^2 \mp As = 2v^2 \\ Br^2 + 2t^2 = 2uv \end{array}\right].$$

Eliminating s from these equations, we obtain two systems of equations:

$$\boxed{\begin{aligned} 2pr^2 + 4Bt^2 &= pu^2 + v^2 \\ Br^2 + 2t^2 &= uv \end{aligned}} \qquad \boxed{\begin{aligned} pr^2 + 2Bt^2 &= pu^2 + v^2 \\ Br^2 + 2t^2 &= 2uv \end{aligned}}$$

We prove later (X.6.6) that the assumptions that 2 is a quartic nonresidue modulo p and that $p \equiv 1 \pmod 8$ imply that $B \equiv 4 \pmod 8$. Reducing each system of equations modulo 8, it is now a simple matter to verify that in both cases, any solution must satisfy $r \equiv t \equiv 0 \pmod 2$. This contradicts our initial assumption that $\gcd(r, t) = 1$, which completes the proof that $C_{-1}(\mathbb{Q}) = \emptyset$. □

We close this section with the theorem of Gauss describing the quartic character of 2 that was used in the proof of (X.6.5). The proof that we give is due to Dirichlet [66]; see also [184].

Proposition 6.6. *Let p be a prime satisfying $p \equiv 1 \pmod 8$, and write p as a sum of two squares, $p = A^2 + B^2$. Then*

$$\left(\frac{2}{p}\right)_4 = (-1)^{AB/4}.$$

In other words, 2 is a quartic residue modulo p if and only if $AB \equiv 0 \pmod 8$.

PROOF. Using the fact that $A^2 + B^2 \equiv 0 \pmod p$, we compute

$$\begin{aligned} (A+B)^{(p-1)/2} &\equiv (2AB)^{(p-1)/4} \pmod p \\ &\equiv 2^{(p-1)/4}(-1)^{(p-1)/8}A^{(p-1)/2} \pmod p. \end{aligned}$$

Switching A and B if necessary, we may assume that A is odd, and then the fact that $p \equiv 1 \pmod 4$ implies that

$$\left(\frac{A}{p}\right) = \left(\frac{p}{A}\right) = \left(\frac{B^2}{A}\right) = 1.$$

Hence

$$\left(\frac{A+B}{p}\right) = (-1)^{(p-1)/8}\left(\frac{2}{p}\right)_4.$$

Finally, we observe that

$$\left(\frac{A+B}{p}\right) = \left(\frac{p}{A+B}\right) = \left(\frac{2}{A+B}\right)\left(\frac{2p}{A+B}\right) = \left(\frac{2}{A+B}\right) = (-1)^{\frac{(A+B)^2-1}{8}},$$

since the identity

$$2p = (A+B)^2 + (A-B)^2 \quad \text{implies that} \quad \left(\frac{2p}{A+B}\right) = 1.$$

Substituting this above yields

$$\left(\frac{2}{p}\right)_4 = (-1)^{\frac{(A+B)^2-1}{8} - \frac{p-1}{8}} = (-1)^{\frac{AB}{4}}.$$

□

Exercises

10.1. Let $\phi : E/K \to E'/K$ be an isogeny of degree m of elliptic curves defined over an arbitrary (perfect) field K. Assume that $E[\hat{\phi}] \subset E(K)$. Generalize (X.1.1) as follows:

(a) Prove that there is a bilinear pairing

$$b : E'(K)/\phi\bigl(E(K)\bigr) \times E'[\hat{\phi}] \longrightarrow K(S, m)$$

defined by

$$e_\phi\bigl(\delta_\phi(P), T\bigr) = \delta_K\bigl(b(P, T)\bigr).$$

Here e_ϕ is the generalized Weil pairing (Exercise 3.15) and

$$\delta_\phi : E'(K) \to H^1\bigl(G_{\bar{K}/K}, E[\phi]\bigr) \qquad \text{and} \qquad \delta_K : K^* \to H^1(G_{\bar{K}/K}, \boldsymbol{\mu}_m)$$

are the usual connecting homomorphisms.

(b) Prove that the pairing in (a) is nondegenerate on the left.

(c) For $T \in E[\hat{\phi}]$, let $f_T \in K(E')$ and $g_T \in K(E)$ be functions satisfying

$$\operatorname{div}(f_T) = m(T) - m(O) \qquad \text{and} \qquad f_T \circ \phi = g_T^m.$$

Prove that

$$b(P, T) = f_T(P) \bmod (K^*)^m \qquad \text{for all } P \neq O, T.$$

(d) In particular, if $\deg(\phi) = 2$, so $E'[\hat{\phi}] = \{O, T\}$, then

$$b(P, T) = x(P) - x(T) \bmod (K^*)^2.$$

We thus recover part of (X.4.9).

10.2. Let K be an arbitrary (perfect) field, let E/K be an elliptic curve, and let C_1/K and C_2/K be homogeneous spaces for E/K.

(a) Prove that there exist a homogeneous space C_3/K for E/K and a morphism

$$\phi : C_1 \times C_2 \to C_3$$

defined over K such that for all $p_1 \in C_1$, $p_2 \in C_2$, and $P_1, P_2 \in E$,

$$\phi(p_1 + P_1, p_2 + P_2) = \phi(p_1, p_2) + P_1 + P_2.$$

(b) Prove that C_3 is uniquely determined, up to equivalence of homogeneous spaces, by C_1 and C_2.

(c) Prove that

$$\{C_1\} + \{C_2\} = \{C_3\},$$

the sum taking place in $\mathrm{WC}(E/K)$.

10.3. Let C/K be a curve of genus one defined over an arbitrary (perfect) field.

(a) Prove that there exists an elliptic curve E/K such that C/K is a homogeneous space for E/K. (*Hint.* Use Exercise 3.22 to show that $C/K \in \mathrm{Twist}(E/K)$. Then find an element $\{\xi\} \in H^1\bigl(G_{\bar{K}/K}, \mathrm{Aut}(E)\bigr)$ such that C/K is the homogeneous space for the twist of E by ξ.)

(b) Prove that E is unique up to K-isomorphism.

10.4. Let K be an arbitrary (perfect) field and let E/K be an elliptic curve.

(a) Prove that there is a natural action of $\operatorname{Aut}_K(E)$ on $\mathrm{WC}(E/K)$ defined by letting an automorphism $\alpha \in \operatorname{Aut}_K(E)$ act on $\{C/K, \mu\} \in \mathrm{WC}(E/K)$ via

$$\{C/K, \mu\}^\alpha = \bigl\{C/K, \mu \circ (1 \times \alpha)\bigr\}.$$

In other words, take the same curve, but define a new action of E on C by the rule

$$\mu^\alpha(p, P) = \mu(p, \alpha P).$$

(b) Conversely, if $\{C/K, \mu\}$ and $\{C/K, \mu'\}$ are elements of $\mathrm{WC}(E/K)$, prove that there exists an $\alpha \in \operatorname{Aut}_K(E)$ such that $\mu' = \mu \circ (1 \times \alpha)$.

(c) Conclude that for a given curve C/K of genus one, there are only finitely many inequivalent ways to make C/K into a homogeneous space. In particular, if C satisfies $j(C) \neq 0, 1728$, then there are at most two. (See also Exercise B.5.)

10.5. Let $\phi : E/K \to E'/K$ be a separable isogeny of elliptic curves defined over an arbitrary (perfect) field K, and let C/K be a homogeneous space for E/K. The finite group $E[\phi]$ acts on C, and we let $C' = C/E[\phi]$ be the quotient curve (cf. Exercise 3.13).

(a) Prove that C' is a curve of genus one defined over K.

(b) Prove that C'/K is a homogeneous space for E'/K and that the natural map

$$\phi : \mathrm{WC}(E/K) \to \mathrm{WC}(E'/K)$$

sends $\{C/K\}$ to $\{C'/K\}$.

(c) In particular, if $\{C/K\} \in \mathrm{WC}(E/K)[\phi]$, then C' is isomorphic to E' over K. Prove that this isomorphism can be chosen so that the natural projection $C \to C/E[\phi] \cong E'$ is the map $\phi \circ \theta$ defined in (X.4.6a).

10.6. *WC Over Finite Fields.* Let $\mathbb{F}_q$ be a finite field with q elements, let $C/\mathbb{F}_q$ be a curve of genus one, and pick any point of $C(\bar{\mathbb{F}}_q)$ as origin to make C into an elliptic curve. Let $\phi : C \to C$ be the qth-power Frobenius map on C.

(a) Prove that there are an endomorphism $f \in \operatorname{End}(C)$ and a point $P_0 \in C(\bar{\mathbb{F}}_q)$ satisfying $\phi(P) = f(P) + P_0$.

(b) Prove that f is inseparable, and conclude that there exists a point $P_1 \in C(\bar{\mathbb{F}}_q)$ satisfying $(1 - f)(P_1) = P_0$.

(c) Prove that $\phi(P_1) = P_1$, and hence that $P_1 \in C(\mathbb{F}_q)$.

(d) Let $E/\mathbb{F}_q$ be an elliptic curve. Prove that $\mathrm{WC}(E/\mathbb{F}_q) = 0$.

10.7. *WC Over* $\mathbb{R}$. Let $E/\mathbb{R}$ be an elliptic curve.

(a) Prove that

$$\mathrm{WC}(E/\mathbb{R}) = \begin{cases} \mathbb{Z}/2\mathbb{Z} & \text{if } \Delta(E/\mathbb{R}) > 0, \\ 0 & \text{if } \Delta(E/\mathbb{R}) < 0. \end{cases}$$

(b) Assuming that $\Delta(E/\mathbb{R}) > 0$, find an equation for a homogeneous space representing the nontrivial element of $\mathrm{WC}(E/\mathbb{R})$ in terms of a given Weierstrass equation for $E/\mathbb{R}$.

10.8. Let E/K be an elliptic curve, let $m \geq 2$ be an integer, and assume that $E[m] \subset E(K)$. Let $v \in M_K^0$ be a prime not dividing m. Prove that the restriction map

$$\mathrm{WC}(E/K)[m] \longrightarrow \mathrm{WC}(E/K_v)[m]$$

is surjective. (*Hint.* Show that the map on the $H^1\bigl(\,\cdot\,, E[m]\bigr)$ groups is surjective.)

10.9. Let E/K be an elliptic curve, let $T \in E[m]$, and suppose that the field $L = K(T)$ has maximal degree, namely $[L : K] = m^2 - 1$. (Note that L/K is generally not a Galois extension.) Let e_m denote the Weil pairing and consider the chain of maps

$$\alpha : E(K) \xrightarrow{\delta} H^1\big(G_{\bar{K}/K}, E[m]\big) \xrightarrow{\text{res}} H^1\big(G_{\bar{K}/L}, E[m]\big) \to H^1(G_{\bar{K}/L}, \boldsymbol{\mu}_m) \cong L^*/(L^*)^m,$$
$$\xi_\sigma \mapsto e_m(\xi_\sigma, T).$$

(a) Let $f_T \in L(E)$ be as in (X.1.1d), i.e.,

$$\operatorname{div}(f_T) = m(T) - m(O) \qquad \text{and} \qquad f_T \circ [m] \in \big(L(E)^*\big)^m.$$

Prove that

$$\alpha(P) = f_T(P) \bmod (L^*)^m.$$

(b) Prove that for all $P \in E(K)$,

$$\mathrm{N}_{L/K}\big(\alpha(P)\big) \in (K^*)^m.$$

(c) Let $S \subset M_L$ be the set of places of L containing all archimedean places, all places dividing m, and all places at which E/L has bad reduction. Show that if $P \in E(K)$ and $v \in M_L$ with $v \notin S$, then

$$\operatorname{ord}_v\big(\alpha(P)\big) \equiv 0 \pmod{m}.$$

(d) For $m = 2$, prove that the kernel of α is exactly $2E(K)$. Hence in this case there is an *injective* homomorphism from $E(K)/2E(K)$ into the group

$$\big\{a \in L^*/(L^*)^2 : \mathrm{N}_{L/K}(a) \in (K^*)^2 \text{ and } \operatorname{ord}_v(a) \equiv 0 \text{ (mod 2) for all } v \notin S\big\}$$

given by the map

$$P \longmapsto x(P) - x(T).$$

This map may often be used to compute $E(K)/2E(K)$. (*Hint*. Expand the quantity $x(P) - x(T) = r + sx(T) + tx(T)^2$ and use the resulting relations on $r, s, t \in K$ to show that P is in $2E(K)$.)

(e) Use (d) to compute $E(\mathbb{Q})/2E(\mathbb{Q})$ for the curve

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

(*Hint*. Let $K/\mathbb{Q}$ be the totally real cubic field generated by a root of the polynomial $4x^3 - 4x + 1$. Start by showing that K has class number one and that every totally positive unit in K is a square.)

10.10. Let C/K be a curve of genus one, and suppose that $C(K_v) \neq \emptyset$ for all $v \in M_K$. Prove that the map

$$\operatorname{Div}_K(C) \longrightarrow \operatorname{Pic}_K(C)$$

is surjective. (*Hint*. Take Galois cohomology of the exact sequence

$$1 \longrightarrow \bar{K}^* \longrightarrow \bar{K}(C)^* \longrightarrow \operatorname{Div}(C) \longrightarrow \operatorname{Pic}(C) \longrightarrow 0.$$

Use Noether's generalization of Hilbert's Theorem 90,

$$H^1\big(G_{\bar{K}/K}, \bar{K}(C)^*\big) = 0,$$

and the (cohomological version) of the Brauer–Hasse–Noether theorem [288, §9.6], which says that an element of $H^2(G_{\bar{K}/K}, \bar{K}^*)$ is trivial if and only if it is trivial in $H^2(G_{\bar{K}_v/K_v}, \bar{K}_v^*)$ for every $v \in M_K$.)

10.11. *Index and Period in WC.* Let K be an arbitrary (perfect) field, let E/K be an elliptic curve, and let C/K be a homogeneous space for E/K. The *period of* C/K is defined to be the exact order of $\{C/K\}$ in $\mathrm{WC}(E/K)$, and the *index of* C/K is the smallest degree of an extension L/K such that $C(L) \neq \emptyset$. So for example, (X.3.3) says that the period is equal to 1 if and only if the index is equal to 1.

(a) Prove that the period may also be characterized as the smallest integer $m \geq 1$ such that there exists a point $p \in C$ satisfying

$$p^\sigma - p \in E[m] \qquad \text{for every } \sigma \in G_{\bar{K}/K}.$$

(b) Prove that the index may also be characterized as the smallest degree among the *positive* divisors in $\mathrm{Div}_K(C)$.

(c) Prove that the period divides the index.

(d) Prove that the period and the index are divisible by the same set of primes.

(e) * Give an example with $K = \mathbb{Q}$ showing that the period may be strictly smaller than the index.

(f) Prove that if K is a number field and if C/K represents an element of $Ш(E/K)$, then the period and the index are equal. (*Hint.* Use (a), (b), (c), and Exercise 10.10.)

(g) * Let $K/\mathbb{Q}_p$ be a finite extension. Prove that the period and the index are equal.

10.12. *Hensel's Lemma.* The following version of Hensel's lemma is often useful for proving that a homogeneous space is locally trivial. Let R be a ring that is complete with respect to a discrete valuation v.

(a) Let $f(T) \in R[T]$ be a polynomial and $a_0 \in R$ a value satisfying

$$v\bigl(f(a_0)\bigr) > 2v\bigl(f'(a_0)\bigr).$$

Define a sequence of elements $a_n \in R$ recursively by

$$a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)} \qquad \text{for } n = 1, 2, \ldots.$$

Prove that a_n converges to an element $a \in R$ satisfying

$$f(a) = 0 \qquad \text{and} \qquad v(a - a_0) \geq v\left(\frac{f(a_0)}{f'(a_0)^2}\right) > 0.$$

(b) More generally, let $F(X_1, \ldots, X_N) \in R[X_1, \ldots, X_N]$, and suppose that there are an index $1 \leq i \leq N$ and a point $(a_1, \ldots, a_N) \in R^N$ satisfying

$$v\bigl(F(a_1, \ldots, a_N)\bigr) > 2v\left(\frac{\partial F}{\partial X_i}(a_1, \ldots, a_N)\right).$$

Prove that F has a root in R^N.

(c) Show that the curve

$$3X^3 + 4Y^3 + 5Z^3 = 0$$

in $\mathbb{P}^2$ has a point defined over $\mathbb{Q}_p$ for every prime p.

10.13. Use (X.1.4) to compute $E(\mathbb{Q})/2E(\mathbb{Q})$ for each of the following elliptic curves.

(a) $E : y^2 = x(x-1)(x+3)$.

(b) $E : y^2 = x(x-12)(x-36)$.

10.14. Use (X.4.9) to compute $E(\mathbb{Q})/2E(\mathbb{Q})$ for each of the following elliptic curves.
(a) $E : y^2 = x^3 + 6x^2 + x$.
(b) $E : y^2 = x^3 + 14x^2 + x$.
(c) $E : y^2 = x^3 + 9x^2 - x$.

10.15. Let E/K be an elliptic curve, let $\xi \in H^1\bigl(G_{\bar{K}/K}, \mathrm{Aut}(E)\bigr)$, and let E_ξ be the twist of E corresponding to ξ. Let $v \in M_K$ be a finite place at which E has good reduction. Prove that E_ξ has good reduction at v if and only if ξ is unramified at v. (See (VIII §2) for the definition of an unramified cocycle. *Hint.* If the residue characteristic is not 2 or 3, you can use explicit Weierstrass equations. In general, use the criterion of Néron–Ogg–Shafarevich (VII.7.1).)

10.16. Let E/K be an elliptic curve, let $D \in K^*$ be such that $L = K(\sqrt{D}\,)$ is a quadratic extension, and let E_D/K be the twist of E/K given by (X.5.4). Prove that

$$\operatorname{rank} E(L) = \operatorname{rank} E(K) + \operatorname{rank} E_D(K).$$

10.17. Let $p \equiv 3 \pmod 4$ be a prime and let $D \in \mathbb{F}_p^*$.
(a) Show directly that the equation

$$C : v^2 = u^4 - 4D$$

has $p - 1$ solutions $(u, v) \in \mathbb{F}_p \times \mathbb{F}_p$. (*Hint.* Since $p \equiv 3 \pmod 4$, the map $u^2 \mapsto u^4$ is an automorphism of $(\mathbb{F}_p^*)^2$.)
(b) Let $E/\mathbb{F}_p$ be the elliptic curve

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

Use the map

$$\phi : C \longrightarrow E, \qquad \phi(u, v) = \left(\frac{u^2 + v}{2}, \frac{u(u^2 + v)}{2}\right),$$

to prove that

$$\#E(\mathbb{F}_p) = p + 1.$$

10.18. Let p be an odd prime. Do a computation analogous to (X.6.2) to determine the Selmer groups and a bound for the ranks of the following families of elliptic curves $E/\mathbb{Q}$.
(a) $E : y^2 = x^3 - 2px$. (The curve with $p = 41$ has rank 3.)
(b) $E : y^2 = x^3 + p^2 x$.

10.19. Let $E/\mathbb{Q}$ be an elliptic curve with $j(E) = 0$.
(a) Prove that there is a unique sixth-power-free integer D such that E is given by the Weierstrass equation

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

(b) Let $p \equiv 2 \pmod 3$ be a prime not dividing $6D$. Prove that

$$\#E(\mathbb{F}_p) = p + 1.$$

(c) Prove that $\#E(\mathbb{Q})_{\text{tors}}$ divides 6.

(d) More precisely, prove that the following list gives a complete description of $E_{\text{tors}}(\mathbb{Q})$:

$$E_{\text{tors}}(\mathbb{Q}) \cong \begin{cases} \mathbb{Z}/6\mathbb{Z} & \text{if } D = 1, \\ \mathbb{Z}/3\mathbb{Z} & \text{if } D \neq 1 \text{ is a square, or if } D = -432, \\ \mathbb{Z}/2\mathbb{Z} & \text{if } D \neq 1 \text{ is a cube,} \\ 1 & \text{otherwise.} \end{cases}$$

10.20. Let A be a finite abelian group, and suppose that there exists a bilinear, alternating, nondegenerate pairing

$$\Gamma : A \times A \longrightarrow \mathbb{Q}/\mathbb{Z}.$$

Prove that $\#A$ is a perfect square.

10.21. Let E/K be an elliptic curve defined over a field of characteristic not equal to 2 or 3, fix a Weierstrass equation for E/K, and let c_4 and c_6 be the usual quantities (III §1) associated to the equation. Assuming that $j(E) \neq 0, 1728$, we define

$$\gamma(E/K) = -c_4/c_6 \in K^*/(K^*)^2.$$

(a) Prove that $\gamma(E/K)$ is well-defined as an element of $K^*/(K^*)^2$, independent of the choice of Weierstrass equation for E/K.
(b) Let E'/K be another elliptic curve with $j(E') \neq 0, 1728$. Prove that E and E' are isomorphic over K if and only if $j(E) = j(E')$ and $\gamma(E/K) = \gamma(E'/K)$.
(c) If $j(E) = j(E') \neq 0, 1728$, prove that E and E' are isomorphic over the field

$$K\left(\sqrt{\frac{\gamma(E/K)}{\gamma(E'/K)}}\right).$$

10.22. Let E/K be an elliptic curve over an arbitrary (perfect) field, let L/K be a finite Galois extension, and define a trace map

$$T_{L/K} : E(L) \longrightarrow E(K), \qquad P \longmapsto \sum_{\sigma \in G_{L/K}} P^\sigma.$$

(a) Prove that $T_{L/K}$ is a homomorphism.
(b) If K is a finite field, prove that $T_{L/K} : E(L) \to E(K)$ is surjective.
(c) Assume that $[L : K] = 2$ and that $\operatorname{char}(K) \neq 2$, and write $L = K(\sqrt{D}\,)$. Fix a Weierstrass equation for E/K of the form

$$E : y^2 = x^3 + ax^2 + bx + c,$$

and let E_D be the quadratic twist of E given by the equation (cf. (X.5.4))

$$E_D : y^2 = x^3 + Dax^2 + D^2bx + D^3c.$$

(i) Prove that the kernel of $T_{L/K} : E(L) \to E(K)$ is isomorphic to $E_D(K)$.
(ii) Prove that the image of $T_{L/K} : E(L) \to E(K)$ contains $2E(K)$.
(iii) Deduce that there are an exact sequence

$$\begin{tikzcd} 0 \arrow[r] & E_D(K) \arrow[r] & E(L) \arrow[r, "T_{L/K}"] & E(K) \arrow[r] & V \arrow[r] & 0 \end{tikzcd}$$

and a surjective homomorphism $E(K)/2E(K) \twoheadrightarrow V$.

(iv) Suppose further that K is a number field. Re-prove Exercise 10.16, i.e.,

$$\operatorname{rank} E(L) = \operatorname{rank} E(K) + \operatorname{rank} E_D(K).$$

10.23. Let $a \equiv 1 \pmod 4$ be an integer with the property that $p = a^2 + 64$ is prime. (It is conjectured, but not known, that there exist infinitely many such primes.) Let $E_a/\mathbb{Q}$ be the elliptic curve

$$E_a : y^2 = x^3 + ax^2 - 16x.$$

These are known as Neumann–Setzer curves.

(a) Prove that $\mathcal{D}_{E_a/\mathbb{Q}} = (p)$. More precisely, prove that E_a has split multiplicative reduction at p and good reduction at all other primes. (N.B. The given Weierstrass equation is not minimal.)

(b) Perform a two-descent (X.4.9) and prove that

$$E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \qquad \text{and} \qquad Ш(E/\mathbb{Q})[2] = 0.$$

(c) * Let $E/\mathbb{Q}$ be an elliptic curve with the following two properties: (i) $E(\mathbb{Q})$ contains a 2-torsion point. (ii) E has multiplicative reduction at a single prime $p > 17$ and good reduction at all other primes. Prove that p has the form $p = a^2 + 64$ and that E is either isomorphic or 2-isogenous to the curve E_a.

10.24. Let E/K be an elliptic curve and let $m \geq 1$. This exercise describes the *Tate pairing*

$$\langle \cdot\,, \cdot \rangle_{\text{Tate}} : E(K)/mE(K) \times \mathrm{WC}(E/K)[m] \longrightarrow \mathrm{Br}(K),$$

where $\mathrm{Br}(K) = H^2(G_{\bar{K}/K}, \bar{K}^*)$ is the Brauer group of K. (This exercise assumes that the reader is familiar with higher cohomology groups; see for example [9, 233].)

Let $P \in E(K)/mE(K)$ and let $C \in \mathrm{WC}(E/K)[m]$. We use the Kummer sequence (VIII §2)

$$0 \longrightarrow E(K)/mE(K) \xrightarrow{\delta} H^1\big(G_{\bar{K}/K}, E[m]\big) \xrightarrow{\epsilon} \mathrm{WC}(E/K)[m] \longrightarrow 0$$

to push forward the point P by δ and to pull back the homogeneous space C by ϵ to obtain 1-cocycles

$$\delta_P : G_{\bar{K}/K} \longrightarrow E[m] \qquad \text{and} \qquad \xi_C : G_{\bar{K}/K} \longrightarrow E[m].$$

We use δ_P and ξ_C to define a map

$$\lambda_{P,C} : G_{\bar{K}/K} \times G_{\bar{K}/K} \longrightarrow \boldsymbol{\mu}_m, \qquad \lambda_{P,C}(\sigma,\tau) = e_m\big(\delta_P(\sigma), \xi_C(\tau)\big),$$

where e_m is the Weil pairing.

(a) Prove that the map $\lambda_{P,C}$ is a 2-cocycle.

(b) Prove that changing either δ_P or ξ_C by a 1-coboundary has the effect of changing $\lambda_{P,C}$ by a 2-coboundary.

(c) Prove that pulling back C to some other element ξ'_C changes $\lambda_{P,C}$ by a 2-coboundary.

(d) Conclude that

$$\langle P, \xi \rangle_{\text{Tate}} = \text{cohomology class of } \lambda_{P,C}$$

gives a well-defined pairing

$$\langle \cdot\,, \cdot \rangle_{\text{Tate}} : E(K)/mE(K) \times \mathrm{WC}(E/K)[m] \longrightarrow \mathrm{Br}(K).$$

(e) Prove that the pairing in (d) is bilinear.

(f) * Let $K/\mathbb{Q}_p$ be a finite extension. A basic result in local class field theory says that $\mathrm{Br}(K) \cong \mathbb{Q}/\mathbb{Z}$; see [233, XII §3, Theorem 2]. Prove in this case that the Tate pairing is nondegenerate.