26.1 Genus 1 curves with no rational points

Let C/k be a (smooth, projective, geometrically irreducible) curve of genus 1 over a perfect field k. Let n be the least positive integer for which $\mathrm{Div}_k C$ contains an effective divisor D of degree n (such divisors exist; take the pole divisor of any non-constant function in $k(C)$, for example). If C has a k-rational point, then $n = 1$ and C is an elliptic curve. We now consider the case where C does *not* have a rational point, so $n > 1$. We have $\deg(D) = n > 2g-2 = 0$, so the Riemann-Roch theorem implies

$$\ell(D) = \deg(D) + 1 - g = n,$$

and for any positive integer m we have

$$\ell(mD) = \deg(mD) + 1 - g = mn.$$

We now analyze the situation for some specific values of n.

26.1.1 The case $n = 2$

We have $\ell(D) = 2$, so let $\{1, x\}$ be a basis for $\mathcal{L}(D)$. Then $\ell(2D) = 4$, so in addition to $\{1, x, x^2\}$, the Riemann-Roch space $\mathcal{L}(2D)$ contains a fourth linearly independent function y. We then have $\{1, x, x^2, y, xy, x^3\}$ as a basis for $\mathcal{L}(3D)$, but $\mathcal{L}(4D)$ is an 8-dimensional vector space containing the 9 functions $\{1, x, x^2, y, xy, x^3, x^2y, x^4, y^2\}$, so there is a linear relation among them, and this linear relation must have nonzero coefficient on both y^2 and x^4. Assuming we are not in characteristic 2, we can complete the square in y to obtain an equation of the form

$$y^2 = f(x)$$

where f is a quartic polynomial over k. The polynomial f must be squarefree, and it cannot have any k-rational roots (otherwise we would have a rational point). Note that the homegenization of this equation is singular at $(0 : 1 : 0)$, but its desingularization is a curve in $\mathbb{P}^3$. Using the same argument as used on the problem set for hyperelliptic curves, one can show that every curve defined by an equation of this form has genus 1.

26.1.2 The case $n = 3$

We have $\ell(D) = 3$, so let $\{1, x, y\}$ be a basis for $\mathcal{L}(D)$. The 10 functions

$$\{1, x, y, x^2, xy, y^2, x^3, x^2y, xy^2, y^3\}$$

all lie in the 9-dimensional Riemann-Roch space $\mathcal{L}(3D)$, hence there is a linear relation among them that defines a plane cubic curve without any rational points. Conversely, every plane cubic curve has genus 1, since over a finite extension of k we can put the curve in Weierstrass form, which we have already proved has genus 1 (recall that genus is preserved under base extension of a perfect field). An example of a plane cubic curve with no rational points was given on the problem set, and here is another one:

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

Unlike the example on the problem set, this curve has a rational point locally everywhere, that is, over every completion of $\mathbb{Q}$. As noted back in Lecture 3, every geometrically irreducible plane curve has rational points modulo p for all sufficiently large primes p, and in this example the only primes that we need to check are 2, 3, and 5; it is easy to check that there are rational solutions modulo each of these primes, and modulo 3^3. Using Hensel's lemma, solutions modulo p (or p^3, for $p = 3$) can be lifted to $\mathbb{Q}_p$, and there are clearly solutions over $\mathbb{R} = \mathbb{Q}_\infty$

26.1.3 The case $n = 4$

We have $\ell(D) = 4$, so let $\{1, x, y, z\}$ be a basis for $\mathcal{L}(D)$. The 10 functions

$$\{1, x, y, z, x^2, y^2, z^2, xy, xz, yz\}$$

all lie in the 8-dimensional Riemann-Roch space $\mathcal{L}(2D)$, hence there are *two* independent linear relations among them, each corresponding to a quadratic form in $\mathbb{P}^3$, and C is the intersection of two quadric hypersurfaces (its clear that C is contained in the intersection, and one can show that it is equal to the intersection by comparing degrees).

26.2 The case $n > 4$

One can continue in a similar fashion for $n > 4$; indeed, by a theorem of Lang and Tate, over $\mathbb{Q}$ there are genus 1 curves that exhibit every possible value of n. But the situation becomes quite complicated already for $n = 5$: we have $\{1, w, x, y, z\}$ as a basis for $\mathcal{L}(D)$ and in $\mathcal{L}(2D)$ we get 15 functions in a Riemann-Roch space of dimension 10.[1]

26.3 Twists of elliptic curves

A genus one curve C/k with no k-rational points is not an elliptic curve, but for some finite extension L/k the set $C(L)$ will be nonempty; thus if base-extend C to L, we obtain an elliptic curve over L. We will show, this elliptic curve can be defined by a Weierstrass equation whose coefficients actually lie in k, so it is also the base-extension of an elliptic curve E/k. The curves E and C are clearly not isomorphic over k, since E has a k-rational point and C does not, but they become isomorphic when we base-extend to L. In other words, the isomorphism $\varphi\colon C \to E$ is defined over L, but not over k, so the distinguished k-rational point O on E is the image of an L-rational point on C that is not defined over k.

Definition 26.1. Two varieties defined over a field k that are related by an isomorphism defined over $\bar{k}$ are said to be *twists* of each other.

In order to characterize the curves that are twists of a given elliptic curve E/k, we introduce the *j-invariant*. For simplicity, we will assume henceforth that $\mathrm{char}(k) \neq 2, 3$, so that we can put our elliptic curves in short Weierstrass form. But the j-invariant can also be defined in terms of a general Weierstrass equation and except where we explicitly note otherwise, all the theorems we will prove are true in any characteristic.

[1] Note that while every curve can be smoothly embedded in $\mathbb{P}^3$, this embedding will not necessarily be defined over k. Over k, $\mathbb{P}^{n-1}$ is the best we can do.

Definition 26.2. Let E/k be an elliptic curve with Weierstrass equation $y^2 = x^3+a_4x+a_6$. The *j-invariant* of E is

$$j(E) := 1728\frac{4a_4^3}{4a_4^3 + 27a_6^2}.$$

Note that the denominator is always nonzero, since $\Delta(E) = -16(4a^3 + 27a_6^2) \neq 0$.

Theorem 26.3. *For every $j \in k$ there exists an elliptic curve E/k with $j(E) = j$.*

Proof. We define such an E/k via an equation $y^2 = x^3 + a_4x + a_6$ as follows. If $j = 0$, let $a_4 = 0$ and $a_6 = 1$, and if $j = 1728$, let $a_4 = 1$ and $a_6 = 0$. Otherwise, let $a_4 = 3j(1728 - j)$ and $a_6 = 2j(1728 - j)^2$. One can check that $\Delta(E) \neq 0$ and $j(E) = j$ in each case. □

Theorem 26.4. *Two elliptic curves defined over k have the same j-invariant if and only if they are isomorphic over $\bar{k}$.*

Proof. For the forward implication, let $y^2 = x^3 + a_4x + a_6$ and $y^2 = x^3 + a'_4x + a'_6$ be Weierstrass equations for elliptic curve E/k and E'/k, respectively, with $j(E) = j(E') = j$. If $j = 0$ then $a_4 = a'_4 = 0$, and we can make $a_6 = a'_6$ by a linear change of variables defined over a suitable extension of k, hence $E \simeq_{\bar{k}} E'$. If $j = 1728$ then $a_6 = a'_6 = 0$, and we can similarly make $a_4 = a'_4$ via a change of variables over a suitable extension of k. Otherwise, over a suitable extension of k we can make a_4 and a'_4 both equal to 1, and then $j(E) = j(E') \Rightarrow a_6 = a'_6$. Thus in every case, $j(E) = j(E') \Rightarrow E \simeq_{\bar{k}} E'$.

For the reverse implication, we note that the cubic $x^3 + a_4x + a_6$ is uniquely determined by its roots, which are precisely the x-coordinates $\{x_1, x_2, x_3\}$ of the three points of order 2 in $E(\bar{k})$. If $E \simeq_{\bar{k}} E'$, then both curves can be embedded in $\mathbb{P}^2$ so that $E[2] = E'[2]$, and they will then have the same Weierstrass equation, hence the same j-invariant. □

Corollary 26.5. *Let C/k be a genus one curve and let O and O' be any two points in $C(\bar{k})$. Then the elliptic curves (C, O) and (C, O') over $\bar{k}$ have the same j-invariant.*

Proof. The translation-by-O' map on (C, O) is an isomorphism from (C, O) to (C, O'). □

It follows from the corollary that the j-invariant of an elliptic curve (E, O) is independent of the choice of O, it depends only on the curve E.

Definition 26.6. Let C/k be a curve of genus one. The j-invariant $j(C)$ of C is the j-invariant of the elliptic curve (C, O) over $\bar{k}$, for any $O \in C(\bar{k})$.

Theorem 26.7. *Let C/k be a curve of genus one. Then $j(C) \in k$.*

Proof. Let us pick $O \in C(L)$, where L is some finite Galois extension L/k, and let E/L be the elliptic curve (C, O). Then E is isomorphic to the base extension of C to L, so let $\varphi\colon C \to E$ be the isomorphism (which is defined over L). For any $\sigma \in \mathrm{Gal}(L/k)$ there is an isomorphism $\varphi^\sigma\colon C^\sigma \to E^\sigma$. But C is defined over k, so $C^\sigma = C$, and therefore $E^\sigma \simeq_L E$, so $j(E^\sigma) = j(E)$. But then $j(E)^\sigma = j(E^\sigma) = j(E)$ for all $\sigma \in \mathrm{Gal}(L/k)$, so $j(E) \in k$. □

Corollary 26.8. *Every genus one curve C/k is a twist of an elliptic curve E/k.*

The corollary does not uniquely determine E, not even up to k-isomorphism; it is possible for two elliptic curves defined over k to be twists without being isomorphic over k. For example, for any $d \in k^\times$ the elliptic curves defined by the Weierstrass equations

$$E\colon y^2 = x^3 + a_4x + a_6$$

and

$$E_d\colon y^2 = x^3 + d^2a_4x + d^3a_6$$

have the same j-invariant and are related by the isomorphism $(x,y) \mapsto (x/d, y/d^{3/2})$, which is defined over $k(\sqrt{d})$. But unless $d \in k^{\times 2}$, they are not isomorphic over k; the curves E and E_d are said to be *quadratic twists* of each other. More generally, we have the following.

Lemma 26.9. *Let $E\colon y^2 = x^3 + a_4x + a_6$ and $E'\colon y^2 = x^3 + a'_4x + a'_6$ be elliptic curves defined over k, with $j(E) = j(E')$. Then for some $\lambda \in \bar{k}^\times$ we have $a'_4 = \lambda^4 a_4$ and $a'_6 = \lambda^6 a_6$. Moreover, the degree of $k(\lambda)/k$ divides 2,4,6 when $a_4a_6 \neq 0$, $a_6 = 0$, $a_4 = 0$, respectively.*

Proof. We first assume $a_4a_6 \neq 0$. From the definition of the j-invariant, we have

$$\begin{aligned}(4a_4'^3 + 27a_6'^2)a_4^3 &= (4a_4^3 + 27a_6^2)a_4'^3\\ 4 + 27(a_6'^2/a_4'^3) &= 4 + 27(a_6^2/a_4^3)\\ a_6'^2a_4^3 &= a_6^2a_4'^3.\end{aligned}$$

If we let $\lambda = \sqrt{(a'_6a_4)/(a_6a'_4)}$ then we have $a'_4 = \lambda^4 a_4$ and $a'_6 = \lambda^6 a_6$ as desired. When $a_6 = 0$ we may simply take $\lambda = \sqrt[4]{a'_4/a_4}$, and when $a_4 = 0$ we may take $\lambda = \sqrt[6]{a'_6/a_6}$. □

We now want to distinguish (up to k-isomorphism) a particular elliptic curve E/k that is a twist of a given genus one curve C/k. For any twist E/k of C/k we have an isomorphism $\phi\colon C \to E$ that is defined over some extension L/k of k that lies in $\bar{k}$. Every $\sigma \in \mathrm{Gal}(\bar{k}/k)$ defines an isomorphism $\phi^\sigma\colon C^\sigma \to E^\sigma$, and since C and E are both defined over k, we have $C^\sigma = C$ and $E^\sigma = E$, so in fact ϕ^σ is an isomorphism from C to E. The map

$$\varphi_\sigma := \phi^\sigma \circ \phi^{-1}$$

is then an isomorphism from E to itself. Every such isomorphism can be written as

$$\varphi_\sigma = \tau_{P_\sigma} \circ \varepsilon_\sigma,$$

where $P_\sigma = \varphi_\sigma(O)$ and ε_σ is an isomorphism that fixes the distinguished point $O \in E(k)$. Both τ_P and ε_σ are isomorphisms from E to itself, but ε_σ is also an isogeny, which is not true of τ_{P_σ} unless it is the identity map.

Definition 26.10. An *automorphism* of an elliptic curve E is an isomorphism $E \to E$ that is also an isogeny. The set of automorphisms of E form a group $\mathrm{Aut}(E)$ under composition.

Theorem 26.11. *Let k be a field of characteristic not equal to 2 or 3.*[2] *The automorphism group of an elliptic curve E/k is a cyclic group of order 6, 4, or 2, depending on whether $j(E)$ is equal to 0, 1728, or neither, respectively.*

Proof. We may assume E/k is in short Weierstrass form. Any automorphism ε^* of the function field $k(E)$ must preserve the Riemann-Roch space $\mathcal{L}(O)$, which has $\{1, x\}$, as a basis, and also the Weierstrass coefficients a_4 and a_6. It follows from Lemma 26.9 that $\varepsilon^*(x) = \lambda^{-2}x$, where λ is a 6th, 4th, or 2nd root of unity, as $j(E) = 0, 1728$, or neither, and we must then have $\varepsilon^*(y) = \lambda^{-3}y$. This uniquely determines ε^* and therefore ε. □

[2] Over a field of characteristic 2 or 3 one can have automorphism groups of order 24 or 12, respectively; this occurs precisely when $j(E) = 0 = 1728$.

Theorem 26.12. *Let C/k be a genus one curve. There is an elliptic curve E/k related to C/k by an isomorphism $\phi\colon C \to E$ such that for every automorphism $\sigma \in \mathrm{Gal}(\bar{k}/k)$ the isomorphism $\varphi_\sigma\colon E \to E$ defined by $\varphi_\sigma := \phi^\sigma \circ \phi^{-1}$ is a translation-by-P_σ map for some $P_\sigma \in E(\bar{k})$. The curve E is unique up to k-isomorphism.*

Proof. To simplify matters we assume $j(C) \neq 0, 1728$ and $\mathrm{char}(k) \neq 2, 3$. We first pick a point $Q_0 \in C(\bar{k})$ and let E be the elliptic curve (C, Q_0). We have $j(E) = j(C) \in k$, so we can put E in short Weirestrass form with coefficients $a_4, a_6 \in k$, and we have an isomorphism $\phi\colon C \to E$ that sends Q_0 to $O := (0 : 1 : 0)$, but it need not be the case that φ_σ is a translation-by-P_σ map for every $\sigma \in \mathrm{Gal}(\bar{k}/k)$.

We can write each of the isomorphisms $\varphi_\sigma = \phi^\sigma \circ \phi^{-1}$ as

$$\varphi_\sigma = \tau_{P_\sigma} \circ \varepsilon_\sigma,$$

where τ_{P_σ} is translation by $P_\sigma = Q_0^\sigma - Q_0$, and $\varepsilon_\sigma \in \mathrm{Aut}(E)$.

Since $j(E) \neq 0, 1728$, we have $\#\mathrm{Aut}(E) = 2$. The group $\mathrm{Aut}(E)$ clearly contains the identity map $[1]$ and the negation map $[-1]$, so $\mathrm{Aut}(E) = \{[\pm 1]\}$. The Galois group $\mathrm{Gal}(\bar{k}/k)$ acts on $\mathrm{Aut}(E)$ trivially, since both $[1]$ and $[-1]$ are defined over k.

If we apply an automorphism $\rho \in \mathrm{Gal}(\bar{k}/k)$ to φ_σ we obtain

$$\varphi_\sigma^\rho = (\phi^\sigma)^\rho \circ (\phi^{-1})^\rho = (\phi^{\rho\sigma}) \circ \phi^{-1} \circ \phi \circ (\phi^\rho)^{-1} = \varphi_{\rho\sigma} \circ \varphi_\rho^{-1}.$$

Thus

$$\varphi_{\rho\sigma} = \varphi_\sigma^\rho \circ \varphi_\rho = (\tau_{P_\sigma} \circ \varepsilon_\sigma)^\rho \circ (\tau_{P_\rho} \circ \varepsilon_\rho) = \tau_{P_\sigma^\rho + P_\rho} \circ (\varepsilon_\sigma^\rho \circ \varepsilon_\rho) = \tau_{P_{\sigma\rho}} \circ \varepsilon_\sigma \circ \varepsilon_\rho,$$

since ρ fixes ε_σ. But we also have $\varphi_{\rho\sigma} = \tau_{P_{\rho\sigma}} \circ \varepsilon_{\rho\sigma}$, thus $\varepsilon_{\rho\sigma} = \varepsilon_\sigma \circ \varepsilon_\rho = \varepsilon_\rho \circ \varepsilon_\sigma$, since $\mathrm{Aut}(E)$ is commutative. The map $\sigma \to \varepsilon_\sigma$ is thus a group homomorphism $\pi\colon \mathrm{Gal}(\bar{k}/k) \to \mathrm{Aut}(E)$. If the kernel of π is all of $\mathrm{Gal}(\bar{k}/k)$, then every ε_σ is trivial and φ_σ is translation-by-P_σ for all $\sigma \in \mathrm{Gal}(\bar{k}/k)$, as desired.

Otherwise the kernel if π is an index-2 subgroup of $\mathrm{Gal}(\bar{k}/k)$ whose fixed field is a quadratic extension $k(\sqrt{d})/k$ for some $d \in k^\times$. In this case let us consider the quadratic twist E_d of E by d, as defined above, and let $\chi_d\colon E \to E_d$ be the isomorphism $(x, y) \mapsto (x/d, y/d^{3/2})$. We then have an isomorphism $\phi_d = \chi_d \circ \phi$ from C to E_d, and for each $\sigma \in \mathrm{Gal}(\bar{k}/k)$ an isomorphism

$$\tilde{\varphi}_\sigma = \phi_d^\sigma \circ \phi_d^{-1} = (\chi_d \circ \phi)^\sigma \circ (\chi_d \circ \phi)^{-1} = \chi_d^\sigma \circ \phi^\sigma \circ \phi^{-1} \circ \chi_d^{-1} = \chi_d^\sigma \circ \varphi_\sigma \circ \chi_d^{-1}.$$

If $\varepsilon_\sigma = [1]$ then σ fixes $k(\sqrt{d})$ and therefore $\chi_d^\sigma = \chi_d$ and $\tilde{\varphi}_\sigma$ is just translation by $\chi_d(P_\sigma)$, since in this case $\varphi_\sigma = \tau_{P_\sigma}$ and χ_d commutes group operations on E and E_d (since it is an isogeny). If $\varepsilon_\sigma = [-1]$ then $\sigma(\sqrt{d}) = -\sqrt{d}$ and $\chi_d^\sigma = \chi_d \circ [-1]$, and now $\varphi_\sigma = \tau_{P_\sigma} \circ [-1]$. We then have

$$\tilde{\varphi}_\sigma = (\chi_d \circ [-1]) \circ (\tau_{P_\sigma} \circ [-1]) \circ \chi_d^{-1},$$

and now $\tilde{\varphi}_\sigma$ is translation by $\chi_d(-P_\sigma)$. Thus in every case $\tilde{\varphi}_\sigma$ is a translation map, so replacing E by E_d and ϕ by ϕ_d yields the desired result.

If $\phi'\colon C \to E'$ is another isomorphism with the same property then after composing with a suitable translation if necessary we can assume$\phi'(Q_0)$ is the point $O = (0 : 1 : 0)$ on E'. The map $\phi' \circ \phi^{-1}$ is then an isomorphism from E to E' that is fixed by every $\sigma \in \mathrm{Gal}(\bar{k}/k)$, hence defined over k, so E is unique up to k-isomorphism. □

Definition 26.13. The elliptic curve E/k given by Theorem 26.12 is the *Jacobian* of the genus one curve C/k; it is determined only up to k-isomorphism, so we call any elliptic curve that is k-isomorphic to E "the" Jacobian of C.

Note that if C is in fact an elliptic curve, then it is its own Jacobian.

We now want to give an alternative characterization of the Jacobian in terms of the Picard group. We will show that the Jacobian of a genus one curve C/k is isomorphic to $\operatorname{Pic}^0 C$; more precisely, for every algebraic extension L/k we have $E(L) \simeq \operatorname{Pic}^0_L C$ (as abelian groups). This characterization of the Jacobian has the virtue that it applies to curves of any genus; although we will not prove this, for each curve C/k of genus g there is an abelian variety A/k of dimension g such that $A(L) \simeq \operatorname{Pic}^0_L C$ for all algebraic extensions L/k.

In order to to prove this for curves of genus one, we first introduce the notion of a principal homogeneous space.

26.4 Principal homogeneous spaces (torsors)

Recall that an *action* of a group G on a set S is a map $G \times S \to S$ such that the identity acts trivially and the action of gh is the same as the action of h followed by the action of g. With the action written on the left, this means $(gh)s = g(hs)$, or on the right, $s^{(gh)} = (s^h)^g$, where $g, h \in G$ and $s \in S$. Below are various properties that group actions may have:

- *faithful*: no two elements of G act the same way on *every* $s \in S$ ($\forall s(gs = hs) \Rightarrow g = h$).
- *free*: no two elements of G act in the same way on *any* $s \in S$ ($\exists s(gs = hs) \Rightarrow g = h$).
- *transitive*: for every $s, t \in S$ there is a $g \in G$ such that $gs = t$.
- *regular*: free and transitive; for all $s, t \in S$ there is a *unique* $g \in G$ with $gs = t$.

Note that free implies faithful, so long as $S \neq \emptyset$.

Definition 26.14. A nonempty set S equipped with a regular group action by an abelian group G is a *principal homogeneous space for* G, also known as a *G-torsor*.

Since a G-torsor S is being acted upon by an abelian group, it is customary to write the action additively on the right. So for any $s \in S$ and $g \in G$ we write $s + g$ to denote the action of g on S (which is another element t of S). Conversely, for any $s, t \in S$ we write $t - s$ to denote the unique $g \in G$ for which $t = s + g$.

As a trivial example of a G-torsor, we can take G acting on itself. More generally, any G-torsor S is necessarily in bijection with G. In fact, we can make S into a group isomorphic to G as follows: pick any element $s_0 \in S$, and define the bijection $\phi\colon G \to S$ by $\phi(g) = s_0 + g$. Declaring ϕ to be a group homomorphism makes S into a group; the group operation is given by $\phi(g) + \phi(h) = \phi(g + h)$, and ϕ is an isomorphism with the map $s \mapsto s - s_0$ as its inverse.

A good analogy for the relationship between G and S is the relationship between a vector space and affine space. A G-torsor is effectively a group with no distinguished identity element, just as affine space is effectively a vector space with no distinguished origin.

26.5 Principal homogeneous spaces of elliptic curves

The notion of a G-torsor S defined above is entirely generic; we now specialize to the case where $G = E(\bar{k})$ is the group of points on an elliptic curve E/k and $S = C(\bar{k})$ is the set of points on a curve C/k. In this setting we add the additional requirement that the action is given by a morphism of varieties. More formally, we make the following definition.

Definition 26.15. Let E/k be an elliptic curve. A *principal homogeneous space for* E (or *E-torsor*), is a genus one curve C/k such that the set $C(\bar{k})$ is an $E(\bar{k})$-torsor and the map $C \times E \to C$ defined by $(Q, P) \mapsto Q + P$ is a morphism of varieties that is defined over k.

Note that if C/k is an E-torsor and L/k is any algebraic extension over which C has an L-rational point P, then the set $C(L)$ is an $E(L)$-torsor and the elliptic curves (E, O) and (C, P) are isomorphic over L via the translation-by-P map. In particular, we always have $j(C) = j(E)$. If C has a k-rational point then C and E are isomorphic over k, and in general E is the Jacobian of C, as we now prove.

Theorem 26.16. *Let C/k be a curve of genus one and let E/k be an elliptic curve. Then C is an E-torsor if and only if E is the Jacobian of C.*

Proof. Suppose C is an E-torsor, let O be the distinguished point of E and pick any $Q_0 \in C(\bar{k})$. Then we have an isomorphism $\phi\colon C \to E$ that sends to Q_0 to O defined by $Q \mapsto Q - Q_0$, where $Q - Q_0$ denotes the unique element of $E(\bar{k})$ that sends Q to Q_0. For any $\sigma \in \mathrm{Gal}(\bar{k}/k)$, the map $\varphi_\sigma = \phi^\sigma \circ \phi^{-1}$ is given by $P \mapsto (Q_0 + P) - Q_0^\sigma$, and is thus translation by $P_\sigma = Q_0 - Q_0^\sigma$. So E is the Jacobian of C (up to k-isomorphism).

Now suppose E is the Jacobian of C and let $\phi\colon C \to E$ be the isomorphism from C to E given by Theorem 26.12. Then $P \in E(\bar{k})$ acts on $Q \in C(\bar{k})$ via $Q \mapsto \phi^{-1}(\phi(Q) + P)$, and this action is regular, since ϕ and translation-by-P are both isomorphisms. Thus $C(\bar{k})$ is an $E(\bar{k})$-torsor, and the map $\mu\colon C \times E \to C$ given by the action of E is clearly a morphism of varieties, since both ϕ and the group operation $E \times E \to E$ are.

To show that μ is defined over k, we check that $\mu^\sigma = \mu$ for all $\sigma \in \mathrm{Gal}(\bar{k}/k)$. The group operation $E \times E \to E$ is defined over k, hence invariant under the action of σ, and for any $Q \in C$ and $P \in E$ we have

$$\begin{aligned}
\mu^\sigma(Q, P) &= (\phi^{-1})^\sigma(\phi^\sigma(Q) + P) \\
&= (\phi^{-1})^\sigma((\varphi_\sigma \circ \phi)(Q) + P) \\
&= (\phi^{-1})^\sigma(\phi(Q) + P_\sigma + P) \\
&= \phi^{-1}(\phi(Q) + P_\sigma + P - P_\sigma) \\
&= \phi^{-1}(\phi(Q) + P) \\
&= \mu(Q, P),
\end{aligned}$$

where we have used $\varphi_\sigma = \phi^\sigma \circ \phi^{-1}$ to derive $\phi^\sigma = \varphi_\sigma \circ \phi$ and $(\phi^{-1})^\sigma = (\phi^\sigma)^{-1} = \phi^{-1} \circ \varphi_\sigma^{-1}$, and applied $\varphi_\sigma(P) = P + P_\sigma$ and $\varphi_\sigma^{-1}(P) = P - P_\sigma$. □

Theorem 26.17. *Let C/k be an E-torsor and let $Q_0 \in C(\bar{k})$. The map $\pi\colon \mathrm{Div}_{\bar{k}}^0 C \to E(\bar{k})$ defined by*

$$\sum_i n_i P_i \mapsto \sum_i n(P_i - Q_0)$$

is a surjective homorphism whose kernel consists of the principal divisors, and it is independent of the choice of Q_0. Moreover, for any extension L/k in $\bar{k}$ the map π commutes with every element of $\mathrm{Gal}(\bar{k}/L)$ and therefore induces a canonical isomorphism $\mathrm{Pic}_L^0 C \simeq E(L)$.

Note that in the definition of π, the sum on the LHS is a formal sum denoting a divisor, while the sum on the RHS is addition in the abelian group $E(\bar{k})$, where each term $P_i - Q_0$ denotes the unique element of $E(\bar{k})$ whose action sends Q_0 to P_i.

Proof. The map π is clearly a group homomorphism. To see that it is surjective, for any point $P \in E(\bar{k})$, if we let $D = (Q_0 + P) - Q_0 \in \operatorname{Div}^0 C$ then

$$\pi(D) = ((Q_0 + P) - Q_0) - (Q_0 - Q_0) = P.$$

If $\pi(D) = \pi(\sum n_i P_i) = O$ for some $D \in \operatorname{Div}^0_{\bar{k}} C$, then the divisor $\sum_i n_i(P_i - Q_0)$ in $\operatorname{div}^0_{\bar{k}}(E)$ sums to O, hence is linearly equivalent to 0 and therefore a principal divisor. Since $\bar{k}(C) = \bar{k}(E)$, the same is true of D. Conversely, if $D \in \operatorname{div}^0_{\bar{k}} C$ is principal, so is the corresponding divisor in $\operatorname{Div}^0_{\bar{k}} E$, and therefore $\pi(D) = O$. Thus the kernel of π is precisely the group of principal divisors, hence π induces an isomorphism $\operatorname{Pic}^0_{\bar{k}} \to E(\bar{k})$.

Now let $Q_1 \in C(\bar{k})$ and define $\pi'(\sum n_i P_i) = \sum n_i(P_i - Q_1)$. Then

$$\pi(D) - \pi'(D) = \sum_i n_i((P_i - Q_0) - (P_i - Q_1)) = \sum n_i(Q_1 - Q_0) = O,$$

since $\sum n_i = \deg(D) = 0$, thus $\pi' = \pi$ and π is independent of the choice of Q_0.

For any $\sigma \in \operatorname{Gal}(\bar{k}/k)$ and $D = \sum n_i P_i \in \operatorname{Div}^0_{\bar{k}} C$ we have

$$\pi(D)^\sigma = \sum_i n_i(P_i^\sigma - Q_0^\sigma) = \pi(D^\sigma).$$

It follows that $D \in \operatorname{Div}^0_L C$ if and only if $\pi(D) \in E(L)$, for any extension L/k in $\bar{k}$, thus π induces an isomorphism $\operatorname{Pic}^0_L C \to E(L)$ for every L/k in $\bar{k}$. □

26.6 The Weil-Châtelet group

Definition 26.18. Let E/k be an elliptic curve. Two E-torsors C/k and C'/k are *equivalent* if there is an isomorphism $\theta\colon C \to C'$ defined over k that is compatible with the action of E. This means that

$$\theta(Q + P) = \theta(Q) + P$$

holds for all $Q \in C(\bar{k})$ and $P \in E(\bar{k})$. The *Weil-Châtelet group* $\operatorname{WC}(E/k)$ is the set of equivalence classes of E-torsors under this equivalence relation.

The equivalence class of E is simply the set of elliptic curves that are k-isomorphic to E; this is the *trivial class* of $\operatorname{WC}(E/k)$, and it acts as the identity element under the group operation that we will define shortly.

Lemma 26.19. *If $\theta\colon C \to C'$ is an equivalence of E-torsors then*

$$\theta(P) - \theta(Q) = P - Q$$

for all $P, Q \in C$. Conversely, if $\theta\colon C \to C'$ is a k-isomorphism for which the above holds, then θ is an equivalence of E-torsors.

Proof. If θ is an equivalence of E-torsors, then

$$\begin{aligned}\theta(P)-\theta(Q) &= \theta(P)+(Q-P)-\theta(Q)+P-Q\\ &= \theta(P+(Q-P))-\theta(Q)+P-Q\\ &= P-Q.\end{aligned}$$

Conversely, if $\theta(P)-\theta(Q)=P-Q$ for all $P,Q\in C$, then for any $R\in E(\bar{k})$ we have $\theta(Q+R)-\theta(Q)=(Q+R)-Q=R$, and therefore $\theta(Q+R)=\theta(Q)+R$ for all $Q\in C$ and $R\in E(\bar{k})$, so θ is an equivalence of E-torsors. □

Recall from the proof of Theorems 26.12 and 26.16 that if C/k is an E-torsor (and therefore E is the Jacobian of C) then each $\sigma\in\mathrm{Gal}(\bar{k}/k)$ determines an isomorphism $\varphi_\sigma\colon E\to E$ that is a translation-by-P_σ map, where $P_\sigma=Q_0^\sigma-Q_0$ for some fixed $Q_0\in C(\bar{k})$. So we have a map $\alpha\colon\mathrm{Gal}(\bar{k}/k)\to E(\bar{k})$ defined by $\alpha(\sigma)=Q_0^\sigma-Q_0$. For any $\sigma,\tau\in\mathrm{Gal}(\bar{k}/k)$ we have

$$\alpha(\sigma)^\tau=(Q_0^\sigma-Q_0)^\tau=Q_0^{(\tau\sigma)}-Q_0^\tau=(Q_0^{\tau\sigma}-Q_0)-(Q_0^\tau-Q_0)=\alpha(\tau\sigma)-\alpha(\tau),$$

thus

$$\alpha(\tau\sigma)=\alpha(\tau)+\alpha(\sigma)^\tau,$$

and this holds for any choice of Q_0 used to define α. If $\alpha(\sigma)^\tau=\alpha(\sigma)$ then α is a group homomorphism, but in general this is not the case; the map α is known as a *crossed homomorphism*.

Definition 26.20. A map $\alpha\colon\mathrm{Gal}(\bar{k}/k)\to E(\bar{k})$ that satisfies

$$\alpha(\tau\sigma)=\alpha(\tau)+\alpha(\sigma)^\tau$$

for all $\sigma,\tau\in\mathrm{Gal}(\bar{k}/k)$ is called a *crossed homomorphism*.

If α and β are two crossed homomorphism then the map $(\alpha+\beta)(\sigma)=\alpha(\sigma)+\beta(\sigma)$ is also, since

$$(\alpha+\beta)(\tau\sigma)=\alpha(\tau\sigma)+\beta(\tau\sigma)=\alpha(\tau)+\alpha(\sigma)^\tau+\beta(\tau)+\beta(\sigma)^\tau=(\alpha+\beta)(\tau)+(\alpha+\beta)(\sigma)^\tau,$$

and addition of crossed homomorphism is clearly associative. The difference of two crossed homomorphisms is similarly a crossed homomorphism, and the map that sends every element of $\mathrm{Gal}(\bar{k}/k)$ to the distinguished point O acts as an additive identity. Thus the set of all crossed homomorphisms from $\mathrm{Gal}(\bar{k}/k)$ to $E(\bar{k})$ form an abelian group.

The crossed homomorphisms of the form $\sigma\mapsto Q_0^\sigma-Q_0$ that arise from an E-torsor C/k with $Q_0\in C(\bar{k})$ have the property that there is a finite normal extension L/k such that $\mathrm{Gal}(\bar{k}/L)=\alpha^{-1}(O)$; take L to be the normal closure of $k(Q_0)$.[3] Crossed homomorphisms with this property are said to be *continuous*.[4] Sums and negations of continuous crossed homomorphisms are clearly continuous, so they form a subgroup.

Now let us consider what happens when we pick a point $Q_1\in C(\bar{k})$ different from Q_0. Let α_0 be the crossed homomorphism $\sigma\mapsto Q_0^\sigma-Q_0$ and let α_1 be the crossed homomorphism $\sigma\mapsto Q_1^\sigma-Q_1$. Then their difference is defined by

$$\alpha_1(\sigma)-\alpha_0(\sigma)=(Q_1^\sigma-Q_1)-(Q_0^\sigma-Q_0)=(Q_1-Q_0)^\sigma-(Q_1-Q_0).$$

[3] Recall that we assume k to be perfect.

[4] If we give $\mathrm{Gal}(\bar{k}/k)$ the Krull topology and $E(\bar{k})$ the discrete topology this corresponds to the usual notion of continuity.

The crossed homomorphism $\alpha_1 - \alpha_0$ is defined in terms of $Q_1 - Q_0$ which is actually a point on $E(\bar{k})$, rather than $C(\bar{k})$. This is also true if we choose $Q_0 \in C_0(\bar{k})$ and $Q_1 \in C_1(\bar{k})$ where C_0 and C_1 are two equivalent E-torsors.

Definition 26.21. Crossed homomorphisms of the form $\sigma \mapsto P^\sigma - P$ with $P \in E(\bar{k})$ are *principal*. The principal crossed homomorphism form a subgroup, as do the continuous principal crossed homomorphisms.

Given our notion of equivalence for E-torsors, we do not wish to distinguish between principal crossed homomorphisms. This leads to the following definition.

Definition 26.22. Let E/k be an elliptic curve. The group of continuous crossed homomorphisms of E/k modulo its subgroup of principal crossed homomorphisms is the *first Galois-cohomology group* of $E(\bar{k})$. It is denoted by

$$H^1(\mathrm{Gal}(\bar{k}/k), E(\bar{k})).$$

For the sake of brevity we may also write $H^1(k, E)$.

Remark 26.23. More generally, if M is any abelian group on which $\mathrm{Gal}(\bar{k}/k)$ acts, one can define Galois cohomology groups $H^n(k, M)$ for each non-negative integer n. The group $H^0(k, M)$ is simply the subgroup of M fixed by $\mathrm{Gal}(\bar{k}/k)$; in our setting $H^0(k, E) = E(k)$.

We now use the group $H^1(k, E)$ to define a group operation on the $\mathrm{WC}(E/k)$.

Theorem 26.24. *Let E/k be an elliptic curve. There is a bijection between the Weil-Châtelet group $\mathrm{WC}(E/k)$ of E and its first cohomology group $H^1(k, E)$.*

Proof. We have already defined a map from $\mathrm{WC}(E/k)$ to $H^1(k, E)$; given an E-torsor C/k that represents an equivalence class in $\mathrm{WC}(E/k)$, we may pick any point $Q_0 \in C(\bar{k})$ to get a continuous crossed homomorphism $\sigma \mapsto Q_0^\sigma - Q_0$ that is uniquely determined modulo prinicipal crossed homomorphisms, hence it represents an element of $H^1(k, E)$. We just need to show that this map is injective and surjective.

We first prove that it is injective. Let C_1/k and C_2/k be E-torsors, pick $Q_1 \in C_1(\bar{k})$ and $Q_2 \in C_2(\bar{k})$, and suppose that the crossed homomorphism $\sigma \mapsto Q_1^\sigma - Q_1$ and $\sigma \mapsto Q_2^\sigma - Q_2$ are equivalent in $H^1(k, E)$. Then their difference is a principal crossed homomorphism $\sigma \mapsto P^\sigma - P$, for some $P \in E(\bar{k})$. Thus we have

$$(Q_1^\sigma - Q_1) - (Q_2^\sigma - Q_2) = P^\sigma - P$$

for all $\sigma \in \mathrm{Gal}(\bar{k}/k)$. Now define the map $\theta\colon C_1 \to C_2$ by

$$\theta(Q) = Q_1 + (Q - Q_2) - P.$$

It is clear that θ is an isomorphism, since C_1 and C_2 are both E-torsors, and it is defined over k, since for any $\sigma \in \mathrm{Gal}(\bar{k}/k)$ we have

$$\begin{aligned}
\theta(Q)^\sigma &= Q_1^\sigma + (Q^\sigma - Q_2^\sigma) - P^\sigma \\
&= Q_1 - (Q^\sigma - Q_2) - P + (Q_1^\sigma - Q_1) - (Q_2^\sigma - Q_2) - (P^\sigma - P) \\
&= Q_1 - (Q^\sigma - Q_2) - P \\
&= \theta(Q^\sigma)
\end{aligned}$$

Thus C_1 and C_2 lie in the same equivalence class in $\mathrm{WC}(E/k)$; this prove injectivity.

For surjectivity, let α be a continuous crossed homomorphism that represents an element of $H^1(k,E)$. We now define an action of $\mathrm{Gal}(\bar{k}/k)$ on the function field $\bar{k}(E) = \bar{k}(x,y)$ as follows: for any $\sigma \in \mathrm{Gal}(\bar{k}/k)$, the elements x^σ and y^σ are given by

$$(x,y)^\sigma = (x^\sigma, y^\sigma) := (x,y) + \alpha(\sigma),$$

where the $+$ indicates that we apply the algebraic formulas defining the group operation on $E(\bar{k})$ working with points in $\mathbb{P}^2(\bar{k}(E))$. To check that this defines a group action, we note that the identity clearly acts trivially, and for any $\sigma, \tau \in \mathrm{Gal}(\bar{k}/k)$ we have

$$(x,y)^{\tau\sigma} = (x,y) + \alpha(\tau\sigma) = (x,y) + \alpha(\tau) + \alpha(\sigma)^\tau = ((x,y) + \alpha(\sigma))^\tau + \alpha(\tau) = ((x,y)^\sigma)^\tau.$$

The fixed field of this action is is the function field of a curve C that is defined over k and isomorphic to E over $\bar{k}$. By construction, there is an isomorphism $\phi\colon C \to E$ such that for any $\sigma \in \mathrm{Gal}(\bar{k}/k)$ the automorphism $\varphi_\sigma = \phi^\sigma \circ \phi^{-1}$ is a translation by $P_\sigma = -\alpha(\sigma)$, thus E is the Jacobian of C, by Theorem 26.12, and therefore C is an E-torsor, by Theorem 26.16. Thus C represents an equivalence class of $\mathrm{WC}(E/k)$, and if we pick $Q_0 = \phi^{-1}(O)$ then

$$\begin{aligned} Q_0^\sigma - Q_0 &= (\phi^\sigma)^{-1}(O) - \phi^{-1}(O) \\ &= \phi^{-1}(O + \alpha(\sigma)) - \phi^{-1}(O) \\ &= \alpha(\sigma), \end{aligned}$$

So the class of α in $H^1(k,E)$ is the image of the class of C in $\mathrm{WC}(E/k)$. □

The bijection given by the theorem maps the trivial class of $\mathrm{WC}(E/k)$ to the identity element of $H^1(k,E)$, thus we can define a group operation on $\mathrm{WC}(E/k)$ via this bijection.

Corollary 26.25. *The Weil-Châtelet group* $\mathrm{WC}(E/k)$ *is isomorphic to the group* $H^1(k,E)$.

Definition 26.26. Let E/k be an elliptic curve. The *Tate-Shafarevich* group $Ш(E)$ is the kernel of the map

$$\mathrm{WC}(E/k) \to \prod_p \mathrm{WC}(E_p/k_p),$$

where k_p ranges over the completions of k and E_p denotes the base extension of E to k_p.

The Tate-Shafarevich group contains precisely the equivalence classes in $\mathrm{WC}(E/k)$ that are locally trivial everywhere. These are the classes of curves C/k with Jacobian E/k that have a k_p-rational point at every completion k_p.

Definition 26.27. A curve C/k satisfies the *local-global principle* (or *Hasse principle*) if either $C(k) \neq \emptyset$ or $C(k_p) = \emptyset$ for some completion k_p.

Theorem 26.28. *Let C/k be a genus one curve with Jacobian E/k. A genus one curve C/k fails the local-global principle if and only if it represents a non-trivial element of* $Ш(E)$.

References

[1] J. H. Silverman, *The arithmetic of elliptic curves*, Springer, 2009.