As usual, a curve is a smooth projective (geometrically irreducible) variety of dimension one and k is a perfect field.

23.1 Genus zero curves with a rational point

Earlier in the course we showed that all plane conics with a rational point are isomorphic to $\mathbb{P}^1$. We now show that this applies to any genus zero curve with a rational point.

Theorem 23.1. *Let C/k be a curve with a rational point. Then C has genus zero if and only if it is isomorphic to $\mathbb{P}^1$ (over k).*

Proof. Every curve that is isomorphic to $\mathbb{P}^1$ has genus zero; this follows from Lemma 21.13 and the Riemann-Roch theorem. Conversely, for a curve of genus $g = 0$ with a rational point P, the Riemann-Roch theorem implies

$$\ell(P) = \deg(P) + 1 - g = 1 + 1 - 0 = 2,$$

since $\deg P = 1 > 2g - 2 = -2$. Thus there exists a non-constant function $f \in \mathcal{L}(P)$, and such an f has a simple pole at P and no other poles. It follows that $\operatorname{div}_\infty f = \deg P = 1$, hence f gives a degree-one morphism from C to $\mathbb{P}^1$ that is defined over k, since $f \in k(C)$, and this is an isomorphism (here we use Corollaries 19.3 and 19.5). □

Remark 23.2. If C/k does not have a rational point, we might instead let P be any closed point (these always exist). Everything in the above proof works except that now we have $\operatorname{div}_\infty f = \deg P > 1$. The function f still defines a morphism to $\mathbb{P}^1$, but it is not an isomorphism because its degree is greater than one. But if we base extend C/k to a finite extension k'/k over which the place P splits into degree one places, then we can show that C/k' is isomorphic to $\mathbb{P}^1$. So every curve of genus zero is isomorphic to $\mathbb{P}^1$ over a finite extension of its ground field.

23.2 Genus one curves with a rational point

Theorem 23.3. *Let C/k be a curve with a rational point. Then C has genus one if and only if it is isomorphic to a plane curve of the form*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1}$$

with $a_1, a_2, a_3, a_4, a_6 \in k$.

Proof. Let C/k be a curve of genus one with a rational point P. For any positive integer n we have $\deg nP = n > 2g - 2 = 0$, so by the Riemann-Roch theorem,

$$\ell(nP) = \deg(nP) + 1 - g = n + 1 - 1 = n.$$

In particular, $\mathcal{L}(2P)$ has dimension 2. Clearly $k \in \mathcal{L}(2P)$, since $0 \geq -2P$, so $\mathcal{L}(2P)$ has a k-basis of the form $\{1, x\}$ for some $x \in k(C) - k$. The space $\mathcal{L}(3P)$ contains $\mathcal{L}(2P)$ and has dimension 3, so it has a basis of the from $\{1, x, y\}$ for some $y \in k(C)^\times$. The functions $1, x, y, x^2$ all belong to $\mathcal{L}(4P)$ and have poles of distinct orders $0, 2, 3, 4$ at P, respectively,

thus they are linearly independent and form a basis for $\mathcal{L}(4P)$. By the same argument, $(1, x, y, x^2, xy)$ is a basis for $\mathcal{L}(5P)$.

But $\mathcal{L}(6P)$ contains both x^3 and y^2, as well as $1, x, y, x^2, xy$. Thus we have 7 elements in a k-vector space of dimension 6, and these must satisfy a linear equation. This equation must contain terms ax^3 and by^2 with $a, b \neq 0$ (otherwise we are left with a linearly independent set of terms), and if we replace x by ax/b and y by by/a, after multiplying through by b^3/a^4 and homogenizing we obtain an equation in the desired form (1).

Now suppose we have a curve C/k defined by an equation of the form (1). If we homogenize (1) and use projective coordinates $(x : y : z)$, then $P = (0 : 1 : 0)$ is a rational point, and it is clearly the only point on C (rational or otherwise) with $z = 0$, since $z = 0$ forces $x = 0$ and all points $(0 : y : 0)$ are projectively equivalent.

The function x (projectively represented as x/z) defines a morphism $(x : z)$ from C to $\mathbb{P}^1$ of degree $[k(C) : k(x)] = 2$, since $k(C) = k(x, y)$ and the minimal equation of y over $k(x)$ has degree 2 (note that C is a curve, and in particular an irreducible algebraic set, so equation (1) must be irreducible). It follows that $\operatorname{div}_\infty x = 2$ (by Corollary 19.23), and since the function x has a pole only at points with z-coordinate 0, it must have a double pole at P. By the same argument, the function y has a pole of order 3 at P. The set of functions $\{x^i y^j\}$ contains elements with poles of order $n = 2i + 3j$ at P for $n = 0$ and all $n \geq 2$, and none of these functions has any other poles. Thus we can construct a set of n linearly independent functions with poles of order $0, 2, 3, \ldots, n$, all of which lie $\mathcal{L}(nP)$. Applying the Riemann-Roch theorem with n sufficiently large yields

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

so the genus g of C is at most 1.

To show that $g \neq 0$, consider the rational map ι defined by $(x : -y - a_1x - a_3z : z)$. The map ι leaves the RHS of (1) unchanged, and on the LHS we have

$$y(y + a_1x + a_3z) \mapsto (-y - a_1x - a_3z)(-y - a_1x - a_3z + a_1x + a_3z) = (y + a_1x + a_3z)y,$$

which is also unchanged, so ι is a morphism from C to itself. The morphism ι is clearly invertible (it is its own inverse), so it is an automorphism. Let us now determine the points fixed by ι. Clearly $(0 : 1 : 0)$ is fixed, and a point with $z \neq 0$ is fixed if and only if $y = -y - a_1x - a_3z$. Assuming $\operatorname{char}(k) \neq 2$, this is equivalent to $y = -(a_1x + a_3z)/2$. There are then three possibilities for x, corresponding to the roots of the cubic

$$x^3 + a_2x^2 + a_4x + a_6z + (a_1x + a_3z)^2/4.$$

These roots are distinct, since a repeated root would correspond to a singularity on the smooth curve C. Thus ι fixes exactly 4 points in $\bar{k}(C)$. If $g = 0$, then C is isomorphic to $\mathbb{P}^1$, by Theorem 23.1, and the only automorphism of $\mathbb{P}^1$ that fixes four points in $\mathbb{P}^1$ is the identity map, by Lemma 23.7 below. But ι is clearly not the identity map on $\bar{k}(C)$, indeed, it fixes only the 4 points already mentioned, thus $g \neq 0$.

If $\operatorname{char}(k) = 2$ one needs a different argument to show $g \neq 0$; see [2]. □

Corollary 23.4. *Every genus one curve C/k with a rational point is isomorphic to a plane cubic curve.*

Remark 23.5. It is also true that every (smooth) plane cubic has genus one, but we won't prove this here. The fact that genus one curves with a rational point can always be embedded in $\mathbb{P}^2$ is noteworthy; the corresponding statement is already false in genus 2.

Remark 23.6. The automorphism ι used in the proof of Theorem 23.3 is an example of an *involution*, an automorphism whose composition with itself is the identity map.

We now prove the lemma used in the proof of Theorem 23.3.

Lemma 23.7. *Suppose ϕ is an automorphism of $\mathbb{P}^1$ that fixes more than 2 points in $\mathbb{P}^1(\bar{k})$. Then ϕ is the identity map.*

Proof. Without loss of generality, we assume ϕ fixes the point $\infty = (1 : 0)$; if not we can apply a linear transformation to $\mathbb{P}^1$ that moves a point fixed by ϕ to ∞. The restriction ϕ_a of ϕ to $\mathbb{A}^1(\bar{k}) = \mathbb{P}^1(\bar{k}) - \{\infty\}$ is then a bijection, and also a morphism of affine varieties. As a morphism from $\mathbb{A}^1 \to \mathbb{A}^1$ the map ϕ_a is a polynomial map, say $\phi_a = (f)$, and f must have degree one since ϕ_a is a bijection. If the equation $f(x) = x$ has more than one solution, then both sides must be equal as polynomials of degree one (two points uniquely determine a line), but then ϕ_a is the identity map. □

Remark 23.8. One can extend the argument above to show that every automorphism of $\mathbb{P}^1$ is a rational function of the form $(ax + by)/(cx + dy)$ with $ad - bc \neq 0$, also known as a *Möbius transformation*. It is easy to see that every non-trivial Möbius transformation fixes exactly 2 points (over $\bar{k}$); they correspond to rotations of the Riemann sphere.

Definition 23.9. Equation (1) in Theorem 23.3 is called a *Weierstrass equation*.

Remark 23.10. There is no a_5 in a Weierstrass equation. As can be seen from the proof of Theorem 23.3, each coefficient a_i appears in front of a function with a pole of order $6 - i$ at the given rational point (and no other poles). There are no functions with only a single pole of order $6 - 5 = 1$ on a curve of genus one (indeed, such a function would give an isomorphism to $\mathbb{P}^1$).

Lemma 23.11. *Let C/k be a curve defined by a Weierstrass equation*

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

If the characteristic of k is not 2 (resp. not 2 or 3) then a_1 and a_3 (resp. a_1, a_2, and a_3) can be made zero via a linear change of coordinates.

Proof. If $\mathrm{char}(k) \neq 2$ then we can complete the square on the LHS, writing it as

$$(y + (a_1x + a_3)/2)^2 - (a_1x + a_3)^2/4.$$

Setting $u = y + (a_1x + a_3)/2)$ and moving the remaining terms to the RHS yields

$$u^2 = x^3 + a_2'x^2 + a_4'x + a_6',$$

for some $a_2', a_4', a_6' \in k$. If we also have $\mathrm{char}(k) \neq 3$, we can depress the cubic on the RHS by setting $v = x + a_2'/3$, yielding

$$u^2 = v^3 + a_4''v + a_6''$$

with $a_4'', a_6'' \in k$. □

Definition 23.12. A Weierstrass equation with $a_1a_2a_3 = 0$ is a *short Weierstrass equation*.

Lemma 23.13. *The short Weierstrass equation $y^2 = x^3 - a_4x - a_6$ defines a genus one curve if and only if $4a_4^3 + 27a_6^2 \neq 0$.*

Proof. The partial derivatives of $f(x, y, z) = y^2z - x^3 - a_4xz^2 - a_6z^3$ are

$$\begin{aligned}\partial f/\partial x &= -3x^2 - a_4z^2,\\ \partial f/\partial y &= 2yz,\\ \partial f/\partial z &= y^2 - 2a_4xz - 3a_6z^2.\end{aligned}$$

Let X be the zero locus of f in $\mathbb{P}^2$. If $P = (x_0 : y_0 : z_0)$ is a singular point of X, then $z_0 \neq 0$ (otherwise we must have $x_0 = y_0 = 0$, but this is not a valid projective point). We then have $y_0 = 0$, (a) $3x_0^2 + a_4z_0^2 = 0$, and (b) $2a_4x_0z_0 + 3a_6z_0^2 = 0$. Writing $x_0 = -3a_6z_0/(2a_4)$ via (b) and plugging into (a) gives

$$\begin{aligned}3(-3a_6z_0)^2/(2a_4)^2 + a_4z_0^2 &= 0\\ 27a_6^2 + 4a_4^3 &= 0.\end{aligned}$$

The calculations above are reversible, so X has a singular point if and only if $4a_4^3+27a_6^2 = 0$. If X has no singular points then it must be irreducible; it is a hypersurface in $\mathbb{P}^2$ and it were the union of two or more curves, then the intersection points would be singular. Thus X is a curve defined by a Weierstrass equation with the rational point $(0 : 1 : 0)$, so by Theorem 23.3 it has genus one. □

In what follows we may assume for the sake of simplicity, that the characteristic of k is not 2 or 3 so that we can work with short Weierstrass equations; everything we do can be extended to the general case, the equations are just more complicated to write down.

23.3 Elliptic curves

Definition 23.14. An *elliptic curve* E/k is a genus one curve with a distinguished rational point O. Equivalently, an elliptic curve is a curve E/k defined by a Weierstrass equation with the distinguished rational point $O = (0 : 1 : 0)$.

Notice that an elliptic curve E/k is, strictly speaking, more than just the curve E, it is the pair (E, O). If E has two rational points, say O_1 and O_2, then (E, O_1) and (E, O_2) are two different elliptic curves. In practice one typically works with elliptic curves given by Weierstrass equations, in which case the point O is always taken to be the point $(0 : 1 : 0)$ at infinity; thus we may refer to E/k as an elliptic curve without explicitly mentioning O.

Remark 23.15. Elliptic curves are obviously *not ellipses* (ellipses are curves of genus zero), but there is a connection. If one attempts to compute the circumference of an ellipse with semi-major axis a and eccentricity e by applying the arc-length formula, one finds that the circumference is given by

$$4a\int_0^1 \sqrt{\frac{1-e^2t}{1-t^2}}\,dt.$$

This is known as an *elliptic integral* (incomplete, and of the second kind), and it does not have a simple closed form. However, the integrand $u(t)$ satisfies the equation

$$u^2(1-t^2) = 1 - e^2t^2,$$

and this defines a genus one curve with a rational point, an elliptic curve.[1] The theory of elliptic curves originated in the study of solutions to integrals like the one above, leading to the notion of *elliptic functions* that arise in complex analysis as solutions to non-linear differential equations that correspond to Weierstrass equations.

Theorem 23.16. *Let E/k be an elliptic curve with distinguished point O. The map ϕ that sends the point $P \in E(k)$ to the class of the divisor $P - O$ in $\mathrm{Pic}^0_k(E)$ is a bijection. This induces a commutative group operation on $E(k)$ defined by*

$$P_1 + P_2 := \phi^{-1}(\phi(P_1) + \phi(P_2)),$$

in which O acts as the identity element.

Proof. We first show that ϕ is injective. If $P - O \sim Q - O$ then $P \sim Q$. We then have $\operatorname{div} f = P - Q$ for some $f \in k(E)$. If f is nonzero then it gives an isomorphism $E \to \mathbb{P}^1$, which is impossible, since E has genus one. So $P = Q$ and ϕ is injective.

Now suppose D is any divisor of degree 0. Then $D + O$ has degree $1 \geq 2g - 1 = 1$, and by the Riemann-Roch theorem

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

so there is a nonzero $f \in \mathcal{L}(D+O)$ such that $\operatorname{div} f + D + O \geq 0$. But $\deg(\operatorname{div} f + D + O) = 1$, so we must have $\operatorname{div} f + D + O = P$ for some $P \in E(k)$. Thus $D \sim P - O$. □

Thus the set of rational points $E(k)$ form an abelian group. The same applies to every base extension of E, so we the set $E(k')$ is also an abelian group (also with O as the identity), for any extension k'/k; this follows from the fact that the genus of a curve is preserved under base extension (of a perfect field), so E/k' is also an elliptic curve.[2]

We now want to describe the group operation more explicitly. For this purpose we use the following construction. Let us assume our elliptic curve E/k is given by a Weierstrass equation, hence embedded in $\mathbb{P}^2$. If L is a line in $\mathbb{P}^2$ defined by a linear form (a homogeneous polynomial of degree one) with coefficients in k, then the intersection $(L \cap E)$ corresponds to a divisor in $D_L = \mathrm{Div}_k E$ of degree 3. This follows from Bezout's Theorem, and the fact that $(L \cap E)$ is fixed by the action of $G_k = \mathrm{Gal}(\bar{k}/k)$; the set $(L \cap E)$ is a union of Galois orbits, each a closed point of E/k, and each occurs in D_L with multiplicity corresponding to the intersection number of E and L at each $\bar{k}$-point in the orbit (these all must coincide).

Lemma 23.17. *Let E/k be an elliptic curve in $\mathbb{P}^2$, and let L_1, L_2 be lines in $\mathbb{P}^2$ defined by linear homogeneous polynomials $\ell_1, \ell_2 \in k[x, y, z]$. Let $f \in k(E)$ be image of ℓ_1/ℓ_2 under the map $k(\mathbb{P}^2) \to k(E)$ induced by the inclusion $E \subseteq \mathbb{P}^2$. Then*

$$\operatorname{div} f = (L_1 \cap E) - (L_2 \cap E).$$

Proof. This follows from Bezout's theorem and the discussion above. □

We now give an explicit description of the group operation on an elliptic curve $E(k)$ defined by a Weierstrass equation. Any two points P and Q in $E(k)$ uniquely determine a line L_1 that is defined over k (if $P = Q$ then take the line tangent to E at $P = Q$). By Bezout's Theorem, $L \cap E$ contains a third point R, and this point must lie in $E(k)$ because

[1] The given equation is singular at $u = 0$ and $t = \pm 1$, but its desingularization is an elliptic curve.

[2] This is not always true when k is not perfect.

P, Q, and $L_1 \cap E$ are all fixed by G_k. If we now let L_2 be the line $z = 0$ at infinity, and let ℓ_1 and ℓ_2 be the linear forms defining L_1 and L_2, then

$$\operatorname{div} \ell_1/\ell_2 = (L_1 \cap E) - (L_2 \cap E) = P + Q + R - 3O = (P - O) + (Q - O) + (R - O)$$

since O is the only point on E with $z = 0$ (so by Bezout's Thoerem, the intersection number $I_P(L_2 \cap E)$ must be 3). This divisor is principal, hence equivalent to the zero divisor, and in terms of the group operation on $E(K)$ this implies

$$P \oplus Q \oplus R = O,$$

where the symbol $\oplus$ denotes the group operation on $E(k)$.[3] and we recall that O is the identity element of the group operation. This is summed up in the following corollary.

Corollary 23.18. *Let E/k be an elliptic curve defined by a Weierstrass equation. The sum of any three points in $E(k)$ that lie on a line is zero under the group law on $E(k)$.*

Corollary 23.18 completely determines the group operation on $E(k)$. To avoid ambiguity, we will temporarily use $\oplus$ to denote the group operation on $E(k)$, in order to distinguish it from addition in $\operatorname{Div}_k E$. Given any two points P and Q we compute their sum $R = P \oplus Q$ by noting that $P \oplus Q = R$ holds if and only if $P \oplus Q \ominus R = O$, so we may compute the negation of R as the third point on the line determined by P and Q. To get R itself, we use the fact that $R \ominus R = O$ if and only if $O \oplus R \ominus R = O$, so we obtain R as the third point on the line determined O and the negation of R. To sum up, the group law on $E(k)$ can be defined as follows.

Corollary 23.19 (Geometric group law)**.** *Let P and Q be rational points on elliptic curve embedded in $\mathbb{P}^2$. Then $P \oplus Q$ is the negation of the third point in the intersection of E and the line uniquely determined by P and Q.*

For explicit computations, we can use the Weierstrass equation for E to compute the coordinates of the point $P \oplus Q$ as rational functions of the coordinates of P and Q. The case where either P or Q is equal to O is obvious, so we assume otherwise, in which case neither P nor Q lies on the line $z = 0$ at infinity and we can work in the affine patch $z \neq 0$.

In order to simplify the formulas, let us assume that $\operatorname{char}(k) \neq 2, 3$ so that E/k can be defined by a short Weierstrass equation

$$y^2 = x^3 + a_4 x + a_6. \tag{2}$$

The additive inverse of any affine point $P = (x_0 : y_0 : 1)$ is $(x_0 : -y_0 : 1)$, since the third point on the line $x - x_0 z$ determined by P and O (and of course O is its own inverse).

We now consider how to compute the sum of two affine points $P_1 = (x_1 : y_1 : z_1)$ and $P_2 = (x_2 : y_2 : z_2)$. Let us first dispose of some easy cases. If $x_1 = x_2$ then $y_1 = \pm y_2$, and if $y_1 = -y_2$ then P_2 is the negation of P_1 and their sum is O, so we assume this is not the case. We then have two possibilities, either $x_1 \neq x_2$, or $P_1 = P_2$. In the latter case, if $y_1 = 0$ then $P_1 = P_2$ is its own negation (a point of order two) and $P_1 \oplus P_2 = O$.

In every other case the slope λ of the line L determined by P_1 and P_2 is given by

$$\lambda = \frac{y_2 - y_2}{x_2 - x_1} \quad (x_1 \neq x_2), \qquad \lambda = \frac{3x_1^2 + a_4}{2y_1} \quad (P_1 = P_2 \text{ and } y_1 \neq 0),$$

[3]We use $\oplus$ here to avoid confusion with the symbol $+$ used to denote addition of divisors (and to write divisors as formal sums of closed points); later, when there is no risk of confusion we will simply use $+$ to denote the group operation on $E(k)$.

and $(y - y_1) = \lambda(x - x_1)$ is the equation for L.

Substituting this into (2) gives the cubic equation

$$\begin{aligned}(\lambda(x - x_1) + y_1)^2 &= x^3 + a_4x + a_6\\ 0 &= x^3 - \lambda^2x^2 + \cdots,\end{aligned}$$

whose solutions are precisely x_1, x_2, and x_3. We now observe that the sum of the roots of any cubic polynomial are equal to the negation of its quadratic coefficient, so $x_1 + x_2 + x_3 = \lambda^2$. This determines x_3; plugging x_3 into the equation for L and negating the result gives y_3.

Theorem 23.20 (Algebraic group law)**.** *Let E/k be an elliptic curve given by the short Weierstrass equation $y^2 = x^3 + a_4x + a_6$. If $P_1 = (x_1 : y_1 : 1)$ and $P_2 = (x_2 : y_2 : 1)$ are affine points whose sum is an affine point $P_3 = (x_3 : y_3 : z_3)$, then*

$$\begin{aligned}x_3 &= \lambda^2 - x_1 - x_2,\\ y_3 &= \lambda(x_1 - x_3) - y_1,\end{aligned}$$

where $\lambda = (y_2 - y_1)/(x_2 - x_1)$ if $P_1 \neq P_2$ and $\lambda = (3x_1^2 + a_4)/(2y_1)$ if $P_1 = P_2$.

Remark 23.21. One can define the group operation on $E(k)$ directly via either Corollary 23.19 or Theorem 23.20 (and one can extend Theorem 23.20 to general Weierstrass equations). But in order to show that this actually makes $E(k)$ a group, one must verify that the group operation is associative, and this is a surprisingly non-trivial exercise. The advantage of using the bijection between $E(k)$ and $\mathrm{Pic}^0_k E$ given by Theorem 23.16 to define the group operation is that it is clear that this defines a group!

It follows from Theorem 23.20 that for any fixed point $P \in E(\bar{k})$, the *translation-by-P map* τ_P that sends Q to $P \oplus Q$ can be defined as a rational map (hence a morphism) from E to itself; it clearly has an inverse (replace P with its negation), so τ_P is an automorphism. The same is true of the *negation map* that sends P to its additive inverse. See [2, III.3.6] for details.

23.4 Abelian varieties

A variety whose points form a group such that the group operations are defined by morphisms, is called an *algebraic group*. More generally, this terminology is also applied to any open subset of a variety (a *quasi-variety*). Examples include $\mathbb{A}^1$, with the group operation given by addition of coordinates, and the general linear group GL_n, which can be viewed as an open subset of $\mathbb{A}^{n^2}$ corresponding to matrices with nonzero determinant.

It follows from Theorem 23.20 that an elliptic curve is an algebraic group, and in fact an *abelian variety*.

Definition 23.22. An *abelian variety* is a projective algrebraic group.

It follows from Theorem 23.20 that an elliptic curve is an abelian variety of dimension one. In fact, one can show that every abelian variety of dimension one is isomorphic to an elliptic curve. It might seem strange that the definition of an abelian variety does not include the requirement that group actually be abelian. This turns out to be a necessary consequence of requiring the algebraic group to be a *projective* variety. We will only prove this for abelian varieties of dimension one, but it is true in general.

Theorem 23.23. *An abelian variety is an abelian group.*

Proof in dimension one. Let G be an abelian variety of dimension one, and for any $h \in G$ consider the morphism $\phi_h \colon G \to G$ defined by $\phi_h(g) = g^{-1}hg$. Since G is a projective variety (hence complete), the image of ϕ_h is also a projective variety, which must be either a point or all of G. Let e be the identity element of G. For $h = e$ image of ϕ_h is clearly just the point $h = e$. For $h \neq e$ the image of ϕ_h cannot contain e, because $g^{-1}hg = e$ implies $hg = g$ and $h = e$. So the image of ϕ_h is a always a point, and it must be the point h, since $\phi_h(e) = h$. Thus for all $g, h \in G$ we have $\phi_h(g) = g^{-1}hg = h$, equivalently, $hg = gh$, so G is abelian.

The proof of Theorem 23.23 in the general case is essentially the same; one first shows that the dimension of $\operatorname{im} \phi_h$ must be the same for every $h \in G$, and since $\dim \operatorname{im} \phi_e = 0$, the image ϕ_h is a point for every $h \in G$ and the proof then proceeds as above; see [1, §4.3]. □

Now that we know abelian varieties are in fact abelian, we will write the group operation additively. When working with morphisms of abelian varieties it is natural to distinguish morphisms ϕ that preserve the group structure, that is, we would like $\phi(g+h) = \phi(g)+\phi(h)$. An obvious necessary condition is $\phi(0) = 0$. This turns out to be sufficient.

Theorem 23.24. *Let $\phi \colon G \to H$ be a morphism of abelian varieties for which $\phi(0) = 0$. Then ϕ is a group homomorphism.*

Proof. For each $h \in G$ let $\phi_h \colon G \to H$ be the morphism $\phi_h(g) = \phi(g) + \phi(h) - \phi(g + h)$. Then $\phi_0(g) = \phi(0) + \phi(g) - \phi(g + 0) = 0$ for all $g \in G$. As in the proof of Theorem 23.23, the image of ϕ_h is a single point for all $h \in G$, and since $\phi_h(0) = \phi(0) + \phi(h) - \phi(0 + h) = 0$, that point must be 0. It follows that $\phi_h(g) = 0$ for all $g, h \in G$, therefore we always have $\phi(g) + \phi(h) = \phi(g + h)$ and ϕ is a group homomorphism. □

References

[1] I. R. Shafarevich, *Basic algebraic geometry*, 2nd edition, Springer-Verlag, 1994.

[2] J.H. Silverman, *The arithmetic of elliptic curves*, 2nd edition, Springer, 2009.