

# Some Notes on Algebraic Maps, Elliptic Curves and Isogenies

Simon Pohmann

January 6, 2022

## Contents

<b>1</b>	<b>Maps on varieties</b>	<b>1</b>
1.1	Algebraic maps . . . . .	1
1.2	The coordinate rings . . . . .	2
1.3	Describing rational maps . . . . .	3
<b>2</b>	<b>Elliptic Curves</b>	<b>5</b>
2.1	The group law . . . . .	6
2.2	Isomorphism classes . . . . .	9
<b>3</b>	<b>The Endomorphism ring</b>	<b>11</b>
3.1	Constructing Isogenies . . . . .	12
3.2	The Frobenius morphism . . . . .	13
3.3	Dual Isogenies . . . . .	14

## 1 Maps on varieties

### 1.1 Algebraic maps

First of all, we define the basic notions of algebraic maps, that is maps that are locally defined by polynomials. For simplicity of notation, we already introduce the projective coordinate ring before.

**Definition 1.1.** Let  $X \subseteq \mathbb{P}^n$  be a projective variety. Then the graded ring  $S(X) := k[x_0, \dots, x_n]/\mathbb{I}(X)$  is its projective coordinate ring.

Note that the graded ring is not invariant under isomorphisms of projective varieties.

**Definition 1.2.** Let  $X \subseteq \mathbb{P}^n$  and  $Y \subseteq \mathbb{P}^m$  be quasi-projective varieties, i.e. open subsets of the projective varieties  $\bar{X}, \bar{Y}$ . Then define

- A map  $X \rightarrow Y$  is called *morphism*, if it is given locally by polynomials, so for each  $p \in X$  there is an open neighborhood  $U$  of  $p$  and homogeneous polynomials  $f_0, \dots, f_m \in S(\bar{X})$  of same degree such that

$$(f_0(a), \dots, f_m(a)) \neq 0 \text{ and } f(a) = [f_0(a) : \dots : f_m(a)] \text{ for all } a \in U$$

- A map  $X \rightarrow k$  is called *regular* at  $p \in X$ , if it is given by polynomials near  $p$ , i.e. there is an open neighborhood  $U$  of  $p$  such that the restriction  $U \rightarrow k$  is a morphism. Denote the regular maps on  $X$  by  $\mathcal{O}_{\bar{X}}(X)$ . We remark that this is a  $k$ -algebra.
- A partial map  $X \dashrightarrow Y$  on an irreducible quasi-projective variety  $X$  is called *rational*, if its set of definition is an open subset  $U \subseteq X$  and it is a morphism  $U \rightarrow Y$ . We identify rational maps  $f, g : X \dashrightarrow Y$  defined on  $U, V \subseteq X$  if  $f|_{U \cap V} = g|_{U \cap V}$ . In other words, regular maps are morphisms  $U \rightarrow Y$  with maximal domain  $U \subseteq X$  open.

In particular, morphisms, rational maps and regular maps are technically all the same thing. The definitions just differ in the domain and the codomain, not in the key property “locally defined by polynomials”. However, they are usually used in a different way. One often works with morphisms between varieties of the same type (e.g. morphisms between projective varieties), and then they differ fundamentally from regular maps (we only have the above equivalence by taking  $Y = k$  to be an affine variety).

## 1.2 The coordinate rings

We have already introduced the projective coordinate ring, which is a not totally natural object, because it is not invariant under isomorphisms. Affine varieties have a much nicer coordinate ring.

**Definition 1.3.** For an affine variety  $X \subseteq \mathbb{A}^n$ , define the affine coordinate ring  $k[X] := k[x_1, \dots, x_n]/\mathbb{I}(X)$ .

This ring has a much tighter connection to the variety.

**Theorem 1.4.** Let  $\mathcal{V}$  be the category of affine varieties  $\subseteq \mathbb{A}_k^n$  with affine morphisms, and  $\mathcal{A}$  the category of finitely generated, reduced (commutative, unital)  $k$ -algebras. Then

$$\Phi : \mathcal{V}^{\text{op}} \rightarrow \mathcal{A}, \quad V \mapsto k[V], \quad \phi \mapsto \phi^*$$

is an equivalence of categories.

Further, each irreducible affine and projective (and even quasi-projective) variety has a function field.

**Definition 1.5.** For an irreducible affine variety  $X \subseteq \mathbb{A}^n$ , define the *function field* as the field of fractions  $k(X) := \text{Frac}(k[X])$ . For an irreducible projective variety  $X \subseteq \mathbb{P}^n$ , define the *function field* as

$$k(X) := \{f/g \in \text{Frac}(S(X)) \mid f, g \text{ homogeneous polynomials of same degree}\}$$

Note that we can evaluate an element  $\frac{f}{g} \in k(X)$  at all points  $a \in X \setminus \mathbb{V}(g)$  and get a well-defined value in  $k$ . To get the function field of an arbitrary quasi-projective variety, one can define it as the function field of an affine chart. We will not pursue that path further. However, the following lemma is important.

**Lemma 1.6.** *Let  $X \subseteq \mathbb{P}^n$  be an irreducible projective variety. Then for all embeddings  $\mathbb{A}^n \subseteq \mathbb{P}^n$  get*

$$k(X \cap \mathbb{A}^n) \cong k(X) \quad \text{via} \quad \frac{f}{g} \mapsto \frac{x_0^d f(x_1/x_0, \dots, x_n/x_0)}{x_0^d g(x_1/x_0, \dots, x_n/x_0)}, \quad d = \max\{\deg f, \deg g\}$$

*Further, find that  $k(X)$  is invariant under isomorphisms. If the embedding  $\mathbb{A}^n \subseteq \mathbb{P}^n$  is clear, we will sometimes identify both fields.*

Hence, the function field is again a natural property of varieties.

### 1.3 Describing rational maps

The function field is more or less equal to all regular maps defined on *some* open subset of  $X$ . Namely

**Proposition 1.7.** *Let  $X \subseteq \mathbb{P}^n$  be an irreducible projective variety. Have a well-defined and injective  $k$ -algebra homomorphism*

$$\mathcal{O}_X(U) \rightarrow k(X), \quad f : U \rightarrow k \text{ defined locally at } p \in U \text{ by } f = g/h \mapsto \frac{g}{h}$$

*Further, this is in some sense surjective, meaning that for each  $f \in k(X)$  there is some open  $U \subseteq X$  such that  $f$  is contained in the image of  $\mathcal{O}_X(U) \rightarrow k(X)$ .*

If we only consider regular maps that are defined on the whole of  $X$ , we get the following statement.

**Theorem 1.8.** *If  $X \subseteq \mathbb{P}^n$  is a projective variety, find  $\mathcal{O}_X(X) \cong k$ . If  $X \subseteq \mathbb{A}^n$  is an affine variety, find  $\mathcal{O}_X(X) \cong k[X]$ .*

*Proof.* Consider the map

$$k[X] \rightarrow \mathcal{O}_X(X), \quad f \mapsto (a \mapsto f(a))$$

which is clearly a well-defined, injective  $k$ -algebra homomorphism. So for the second part, it is left to show that it is surjective.

Let  $f \in \mathcal{O}_X(X)$ . Then for each  $p \in X$  there is an open neighborhood  $U_p \subseteq X$  and polynomials  $g_p, h_p \in S(X)$  with  $f = g_p/h_p$  on  $U_p$  with  $h_p(a) \neq 0$  for all  $a \in U_p$ . As  $X \subseteq \mathbb{A}^n$ , we can assume  $g_p, h_p \in k[X]$ . Obviously, there is a finite subcover  $U_1 := U_{p_1}, \dots, U_r := U_{p_r}$  with  $p_1, \dots, p_r \in X$ .

As the  $U_i$  are an open cover, we see that  $\mathbb{V}(\langle h_1, \dots, h_r \rangle) = \emptyset$  and so by Hilbert's Nullstellensatz, find

$$1 = \sum_i \alpha_i h_i$$

Thus

$$f_i := \frac{g_i}{h_i} = \frac{g_i}{h_i} \sum_j \alpha_j h_j = \alpha_i g_i + \sum_{j \neq i} \alpha_j h_j \in k[X] \subseteq k(X)$$

So on each  $U_i$ , the regular map  $f$  is given by a polynomial  $f_i \in k[X]$ . It is left to show that those glue together to one global polynomial (this is only trivial in the case  $X$  irreducible).  $\square$

Describing rational maps and morphisms can be done similarly, but they also allow a relatively nice definition using the function field.

**Theorem 1.9.** *Let  $X \subseteq \mathbb{P}^n$  be an irreducible projective variety. Then there is a well-defined bijection*

$$\begin{aligned} \Phi : \{f : X \dashrightarrow \mathbb{P}^m \mid f \text{ rational map}\} &\rightarrow \mathbb{P}_{k(X)}^m, \\ f \text{ defined locally by } f_0, \dots, f_m \in S(X) &\mapsto \left[ \frac{f_0}{x_0^d} : \frac{f_1}{x_0^d} : \dots : \frac{f_m}{x_0^d} \right] \end{aligned}$$

*In particular, the restriction*

$$\Phi|_{\{f : X \rightarrow \mathbb{P}^m \mid f \text{ morphism}\}} : \{f : X \rightarrow \mathbb{P}^m \mid f \text{ morphism}\} \rightarrow \mathbb{P}_{k(X)}^m$$

*is a well-defined injection.*

We sometimes will identify those two representations of rational maps. Note that  $k[X \cap \mathbb{A}^n] \subseteq k(X \cap \mathbb{A}^n) \cong k(X)$ , and using this makes the notation of rational maps as  $[f_0 : \dots : f_m]$  even more convenient, because we do not even require fractions then.

Furthermore, the rational maps  $X \dashrightarrow Y$  to a projective variety  $Y$  are then exactly the elements of

$$\mathbb{V}_{k(X)}(\mathbb{I}_k(Y)) \subseteq \mathbb{P}_{k(X)}^m$$

and similarly for open sets.

**Remark 1.10.** Note that the bijection  $\Phi$  from Theorem 1.9 is compatible with evaluation maps in the following sense. For  $f : X \dashrightarrow Y$  and  $g : Y \dashrightarrow \mathbb{P}^r$  such that the composition  $g \circ f$  is well-defined, have

$$\Phi(g \circ f) = \text{ev}_{\Phi(f)}(\Phi(g))$$

**Definition 1.11.** Let  $f = [f_0 : \dots : f_m] : X \dashrightarrow Y$  be a rational map with  $f_0, \dots, f_m \in k(X)$ . Then

$$f^* : k(Y) \rightarrow k(X), \quad y_i \mapsto f_i$$

is called the *pullback* of  $f$ .

## 2 Elliptic Curves

**Definition 2.1** (Elliptic Curve). An elliptic curve  $E \subseteq \mathbb{P}^2$  is a nonsingular curve given by an equation of the form

$$E = \mathbb{V}(Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3)$$

We write  $O := [0 : 1 : 0]$  for the unique point of  $E$  on the hyperplane at infinity. Further, write  $k[E]$  for the affine coordinate ring  $k[E \cap \mathbb{A}^2]$ .

We will often use dehomogenized equations to specify an elliptic curve.

**Definition 2.2** (Isogeny). An isogeny  $f : E \rightarrow E'$  between elliptic curves is a morphism with  $f(O) = O$ . An isogeny that is an isomorphism in the sense of Algebraic Geometry is also called isomorphism.

**Proposition 2.3.** *Let  $f : E \rightarrow E'$  be a nonconstant isogeny. Then  $f$  is surjective.*

*Proof.* It is a fact from Algebraic Geometry that the image of a projective variety under a morphism is a projective variety. So the image of  $f$  must be an irreducible projective subvariety of  $E'$ , hence either a single point or  $E'$ .  $\square$

**Proposition 2.4.** *If  $\text{char}(k) \neq 2, 3$  then each elliptic curve is isomorphic to an elliptic curve of the form*

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

**Definition 2.5** (Discriminant). For an elliptic curve  $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ , define the discriminant

$$\Delta(E) = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

$$\text{where } b_2 = a_1^2 + 4a_2$$

$$b_4 = a_1a_3 + 2a_4$$

$$b_6 = a_3^2 + 4a_6$$

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$$

Note that for elliptic curves  $E$  given by the simpler equation  $E : y^2 = x^3 + Ax + B$  have

$$\Delta(E) = -16(4A^3 - 27B^2)$$

**Proposition 2.6.** *A cubic curve*

$$C = \mathbb{V}(Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3)$$

*is an elliptic curve (i.e. nonsingular), if and only if  $\Delta(C) \neq 0$ .*

**Lemma 2.7.** *Let  $\psi = [\psi_0, \psi_1, 1] : E \rightarrow E'$  be a morphism between elliptic curves. Then  $k(\psi_0, \psi_1, x) = k(x, y)$ .*

*Proof.* Assume that we have  $E' : y^2 = x^3 + Ax + B$ . Then clearly

$$\psi_1^2 = \psi_0^3 + A\psi_0 + B$$

Now assume for a contradiction that  $\psi_0, \psi_1 \in k(x)$ . Since  $k$  is algebraically closed, have  $x^3 + Ax + B = (x - \mu_1)(x - \mu_2)(x - \mu_3)$  and so

$$(\psi_0 - \mu_1)(\psi_0 - \mu_2)(\psi_0 - \mu_3)$$

is a perfect square in  $k(x)$ . Note that  $\Delta(E')$  is a constant multiple of the discriminant of the polynomial  $x^3 + Ax + B$  and since  $\Delta(E') \neq 0$ , we see that  $\mu_1, \mu_2, \mu_3$  are pairwise distinct. With  $\phi_0 = f/g$  and  $f, g \in k[x], f \perp g$  we see that then the factors  $f - \mu_1 g, f - \mu_2 g$  and  $f - \mu_3 g$  are pairwise coprime, so each must already be a perfect square, say

$$f - \mu_1 g = h_1^2, \quad f - \mu_2 g = h_2^2, \quad f - \mu_3 g = h_3^2$$

with pairwise coprime  $h_1, h_2, h_3$ . Then

$$\begin{aligned} (\mu_2 - \mu_1)g &= (h_1 - h_2)(h_1 + h_2), \\ (\mu_3 - \mu_1)g &= (h_1 - h_3)(h_1 + h_3) \end{aligned}$$

Since  $h_2 \perp h_3$ , find  $(h_1 + h_2) \perp (h_1 + h_3)$  and  $(h_1 - h_2) \perp (h_1 - h_3)$ , so

$$h_1 - h_2 = \epsilon(h_1 + h_3), \quad h_1 + h_2 = \epsilon'(h_1 - h_3)$$

for some  $\epsilon, \epsilon' \in k^*$ . Thus  $(1 - \epsilon)h_1 = \epsilon h_3 + h_2$  with  $\epsilon - 1 \in k^*$ . So

$$2h_1 = (\epsilon + \epsilon')h_1 + (\epsilon - \epsilon')h_3$$

thus

$$(2 - \epsilon - \epsilon')h_1 = (\epsilon - \epsilon')h_3$$

and so  $\epsilon = \epsilon' = 1$  since  $h_1 \perp h_3$ . However then  $h_3 = -h_2$ , a contradiction.  $\square$

## 2.1 The group law

**Proposition 2.8.** *Let  $E$  be an elliptic curve. Then each projective line meets  $E$  at exactly three points, with multiplicity.*

**Definition 2.9.** Define a map

$$+_{\text{geo}} : E \times E \rightarrow E$$

that for  $P, Q \in E$  is given by the following geometric construction:

- Let  $L$  be the line through  $P, Q$  (with multiplicity)
- Let  $R$  be the third point of intersection of  $E$  with  $L$  (exists by 2.8)

- Let  $L'$  be the line through  $R, O$
- Set  $P +_{\text{geo}} Q$  to be the third point of intersection of  $E$  with  $L'$

**Proposition 2.10.** *Let  $E : y^2 = x^3 + Ax + B$  be an elliptic curve. Then the affine coordinate ring  $k[E]$  is a Dedekind domain and there is a bijection*

$$\phi : E \rightarrow \text{Cl}(k[E]), \quad (\lambda, \mu) \mapsto \overline{\langle x - \lambda, y - \mu \rangle}, \quad O \mapsto \overline{\langle 1 \rangle}$$

**Definition 2.11.** Define the map

$$+_{\text{alg}} : E \times E \rightarrow E, \quad (P, Q) \mapsto \phi^{-1}(\phi(P)\phi(Q))$$

**Definition 2.12.** Define the map

$$\begin{aligned} +_{\text{poly}} : E \times E \rightarrow E, \quad ((x_1, y_1), (x_2, y_2)) &\mapsto (x_3, y_3), \\ ((x, y), (x, -y)) &\mapsto O \\ (O, P), (P, O) &\mapsto P \end{aligned}$$

where for  $P = (x_1, y_1)$ ,  $Q = (x_2, y_2) \neq (x_1, -y_1)$  we set

$$\begin{aligned} \lambda &:= \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } x_1 \neq x_2 \\ \frac{3x_1^2 + A}{2y_1} & \text{otherwise} \end{cases} \\ x_3 &:= -x_1 - x_2 + \lambda^2 \\ y_3 &:= -y_1 + \lambda(x_1 - x_3) \end{aligned}$$

**Proposition 2.13** (The group law). *Let  $E$  be an elliptic curve. Then  $+$  :=  $+_{\text{geo}} = +_{\text{alg}} = +_{\text{poly}}$ .*

**Corollary 2.14.** *Let  $E : Y^2 = X^3 + AX + B$  be an elliptic curve. Then*

- $E$  together with the binary operation  $+$  from 2.13 is a group.
- $E$  has neutral element  $O$
- $E$  is abelian
- for a field tower  $k|L|K$ , the so-called  $L$ -rational points  $E(L) := E \cap \mathbb{P}_L^2 = (E \cap L^2) \cup \{O\}$  form a subgroup

**Proposition 2.15.** *Let  $E, E' : y^2 = x^3 + A'x + B'$  be elliptic curves and  $\psi : E \rightarrow E'$  an isogeny. Then  $\psi$  is a group homomorphism.*

*Proof.* Wlog assume that  $\psi$  is nonconstant. Have  $\psi = [\psi_1 : \psi_2 : 1]$  with  $\psi_1, \psi_2 \in k(E)$  and consider the field homomorphism

$$\psi^* : k(E') \rightarrow k(E), \quad \bar{f} \mapsto \overline{f(\psi_1, \psi_2)}$$

This is well-defined, because if  $\bar{f} = \bar{g}$  then

$$f(\psi_1, \psi_2) \equiv g(\psi_1, \psi_2) \pmod{\underbrace{\psi_2^2 - \psi_1^3 + A'\psi_1 + B'}_{=(0)}}$$

Now we look at the field extension

$$k(E) = k(x, y) \mid \psi^* k(E') = k(\psi_1, \psi_2)$$

As  $\psi(O) = O$  we see that there are homogeneous polynomials  $f, g, h \in k[R, S, T]$  of same degree with

$$f(0, 1, 0) = h(0, 1, 0) = 0, \quad g(0, 1, 0) = 1, \quad \psi_1 = \frac{f^{\text{deh}}(x, y)}{h^{\text{deh}}(x, y)}, \quad \psi_2 = \frac{g^{\text{deh}}(x, y)}{h^{\text{deh}}(x, y)}$$

Since  $f, h$  are homogeneous of same degree, we see that  $f(0, y, 0) = h(0, y, 0) = 0$  for all  $y \in k$ . It follows that  $\psi_1 \in k(x)$ . Furthermore, if  $\psi_1 = f(x)/h(x)$  for  $f, h \in k[T]$  we can then assume wlog that  $f - \psi_1 h \in \psi^* k(E')[T]$  is the minimal polynomial of  $x$  over  $\psi^* k(E')$  or over  $k(\psi_1)$ .

By 2.3 we see that  $\psi$  is surjective, so Algebraic Geometry tells us that  $\psi^*$  is injective. We can then define

$$\psi_* := (\psi^*)^{-1} \circ N_{k(E)|\psi^* k(E')} : k(E) \rightarrow k(E')$$

This map is a (multiplicative) group homomorphism, as  $\psi^*$  is a field homomorphism and the norm map  $N$  is multiplicative. Thus it induces a well-defined group homomorphism

$$\overline{\psi_*} : \text{Cl}(k[E]) \rightarrow \text{Cl}(k[E']), \quad \bar{I} \mapsto \overline{(\psi_* I)}$$

Now we show that the following diagram is commutative and the claim follows by 2.10 and 2.13.

$$\begin{array}{ccc} E & \xrightarrow{\psi} & E' \\ \phi \downarrow & & \downarrow \phi \\ \text{Cl}(k[E]) & \xrightarrow{\overline{\psi_*}} & \text{Cl}(k[E']) \end{array}$$

Clearly this holds for  $O$ , so consider  $(\lambda, \mu) \in E$  with  $\psi(\lambda, \mu) \neq O$ . As  $\psi^*$  is injective, it suffices to show that  $(\psi^* \circ \phi \circ \psi)(\lambda, \mu) = (\psi^* \circ \overline{\psi_*} \circ \phi)(\lambda, \mu)$ .

Using the definition of  $\phi$  we find

$$\begin{aligned} (\psi^* \circ \psi_* \circ \phi)(\lambda, \mu) &= (N(x - \lambda), N(y - \mu)) \quad \text{and} \\ (\psi^* \circ \phi \circ \psi)(\lambda, \mu) &= \psi^*((x - \psi_1(\lambda, \mu), y - \psi_2(\lambda, \mu))) = (\psi_1 - \psi_1(\lambda, \mu), \psi_2 - \psi_2(\lambda, \mu)) \end{aligned}$$

Explicitly computing the determinant of the multiplication map shows that

$$N_{L(\alpha)|L}(\alpha - \lambda) = \text{MiPo}_L(\alpha)(\lambda) \quad \text{so} \quad N(x - \lambda) = \text{MiPo}_{k(\psi_1)}(x)(\lambda)$$



By the above, find  $f, h \in k[T]$  such that  $\psi_1 = f(x)/h(x)$  and  $f(T) - \psi_1 h(T)$  is the minimal polynomial of  $x$ . Now we see that  $(\psi(\lambda, \mu) \neq 0$  so  $h(\lambda) \neq 0)$

$$N(x - \lambda) = f(\lambda) - \psi_1 h(\lambda) = -h(\lambda)(\psi_1 - \psi_1(\lambda, \mu))$$

As  $\psi_2^2 = u(\psi_1)$  for some  $u \in k[T]$  we find  $u, v \in k[S, T]$  such that

$$\text{MiPo}_{\psi^*k(E')}(Y) = v(T, \psi_1)\psi_2 - u(T, \psi_1) \in k(\psi_1, \psi_2)(T)$$

Hence

$$N(y - \mu) = v(\mu, \psi_1)\psi_2 - u(\mu, \psi_1)$$

As  $\text{MiPo}(y)(y) = 0$  have

$$\text{MiPo}(y)(y)(\lambda, \mu) = v(\mu, \psi_1(\lambda, \mu))\psi_2(\lambda, \mu) - u(\mu, \psi_1(\lambda, \mu)) = 0$$

Together, modulo  $\psi_1 - \psi_1(\lambda, \mu)$  we get <sup>1</sup>

$$\frac{1}{v(\mu, \psi_1(\lambda, \mu))}N(y - \mu) \equiv \psi_2 - \frac{u(\mu, \psi_1)}{v(\mu, \psi_1)} \equiv \psi_2 - \underbrace{\frac{u(\mu, \psi_1(\lambda, \mu))}{v(\mu, \psi_1(\lambda, \mu))}}_{=\psi_2(\lambda, \mu)} = \psi_2 - \psi_2(\lambda, \mu)$$

So

$$(N(x - \lambda), N(y - \mu)) = (\psi_1 - \psi_1(\lambda, \mu), \psi_2 - \psi_2(\lambda, \mu)) \in \text{Cl}(k[E])$$

and the claim follows.  $\square$

**Remark 2.16.** In [Sil09], the above proof was done using the Picard group (which is naturally isomorphic to the ideal class group, but working with it uses different tools). Riemann-Roch is not cited (as far as I think) for that proof, but already relies heavily on the theory of divisors.

Note that the field extension  $k(E)|\psi^*k(E')$  is quite important. In particular, we say

**Definition 2.17.** Let  $\psi : E \rightarrow E'$  be an isogeny. We define the *degree* of  $\psi$  to be the degree of  $k(E)|\psi^*k(E')$  and say that  $\psi$  is *separable* if  $k(E)|\psi^*k(E')$  is.

## 2.2 Isomorphism classes

**Definition 2.18** (j-invariant). Let  $E : y^2 = x^3 + Ax + B$  be an elliptic curve. Then define the j-invariant of  $E$  as

$$j(E) := \frac{(-48A)^3}{\Delta(E)} = 1728 \frac{4A^3}{27B^2 + 4A^3}$$

**Proposition 2.19.** Let  $E, E'$  be two elliptic curves. Then  $E \cong E'$  if and only if  $j(E) = j(E')$ .

---

<sup>1</sup>Strictly speaking, we use require  $v(\mu, \psi_1(\lambda, \mu)) \neq 0$  here. At least we have  $v(y, \psi_1) \neq 0$  here, which follows from Lemma 2.7.

*Proof.* First, assume  $j(E) = j(E')$  and consider the isogeny  $\psi = [u^2x, u^3y, 1]$  where  $u^4 = A/A'$ . Then

$$\begin{aligned} (u^3y)^2 &= u^6y^2 \quad \text{and} \\ (u^2X)^3 - A(u^2X) - B &= u^6\left(X^3 - \frac{1}{u^4}AX - \frac{1}{u^6}B\right) \\ &= u^6\left(X^3 - A'X - \frac{1}{u^6}B\right) \end{aligned}$$

From  $j(E) = j(E')$  we get

$$A^3(27B'^2 + 4A'^3) = A'^3(27B^2 + 4A^3)$$

Thus

$$A^3\left(27B'^2 + 4\frac{1}{u^{12}}A^3\right) = \frac{1}{u^{12}}A'^3(27B^2 + 4A^3)$$

and so

$$B'^2 = \frac{1}{u^{12}}B^2 + \frac{1}{27u^{12}}(4A^3 - 4A'^3) = \frac{1}{u^{12}}B^2$$

It follows that  $u^6 = B/B'$  and so  $\psi$  maps  $E$  to  $E'$ . It is only a linear transformation, hence also an isomorphism.

For the other direction, assume there is an isomorphism  $\psi = [u, v, 1]$  from  $E$  to  $E'$  where  $E' : Y^2 = X^3 + A'X + B'$  and  $x, y \in k(E)$ . As  $\psi$  is an isomorphism, it is also an isomorphism of the affine varieties  $E \cap \mathbb{A}^2$  resp.  $E' \cap \mathbb{A}^2$  and so we find the pullback

$$\psi^* : k[E'] \rightarrow k[E], \quad x' \mapsto u, y' \mapsto v$$

for some  $u, v \in k[E]$  with  $v^2 = u^3 + A'u + B'$ . We want to show that  $u, v$  are linear in  $x, y \in k[E]$ , and the claim follows more or less by reversing the computation above.

As  $\psi$  maps  $O$  to  $O$ , we see as before in Prop. 2.15 that  $u \in k[x]$ . Since  $u$  is transcendental over  $k$ , we see that  $k[x]$  is a finitely generated  $k[u]$ -module. Now we find

$$[k[u] : k[x]] \underbrace{[k[x] : k[x, y]]}_{=2} = [k[u] : k[x, y]] = \underbrace{[k[u] : k[u, v]]}_{\leq 2} \underbrace{[k[u, v] : k[x, y]]}_{=1 \text{ by assumption}}$$

and so  $k[u] = k[x]$ . Clearly this implies that  $u$  is linear in  $x$ . It is easy to see that now  $v$  must also be linear in  $x$  and  $y$ .  $\square$

**Remark 2.20.** In [Sil09], the above proof was done using the Riemann-Roch theorem, from which it directly follows that a certain vector space containing  $1, x, u$  is 2-dimensional, and so  $u$  is linear in  $1$  and  $x$ . Similarly, one again finds that  $v$  is linear in  $1, x, y$ .

---

<sup>2</sup>Note that we use a result discussed at the beginning here. Namely, the crucial point is that a birational equivalence between affine varieties that is defined everywhere is already an isomorphism.

### 3 The Endomorphism ring

**Lemma 3.1.** *Let  $\phi, \psi : E \rightarrow E'$  be isogenies on an elliptic curve  $E$ . Then  $\phi + \psi$  (where addition is defined pointwise) is an isogeny  $E \rightarrow E$ .*

*Proof.* Clearly  $(\phi + \psi)(O) = O$  and the map is given locally by polynomials, as

$$\begin{aligned} \frac{\phi_y - \psi_y}{\phi_x - \psi_x} &= \frac{\phi_y^2 - \psi_y^2}{(\phi_x - \psi_x)(\phi_y + \psi_y)} = \frac{\phi_x^3 + A'\phi_x + B' - \psi_x^3 - A'\psi_x - B'}{(\phi_x - \psi_x)(\phi_y + \psi_y)} \\ &= \frac{(\phi_x^2 + \phi_x\psi_x + \psi_x^2 + A')(\phi_x - \psi_x)}{(\phi_x - \psi_x)(\phi_y + \psi_y)} = \frac{\phi_x^2 + \phi_x\psi_x + \psi_x^2 + A'}{\phi_y + \psi_y} \end{aligned}$$

in  $k[E]$  where  $\phi = [\phi_x : \phi_y : 1]$  and  $\psi = [\psi_x : \psi_y : 1]$ .  $\square$

**Definition 3.2.** For an elliptic curve  $E$ , consider the set  $\text{End}(E)$  of isogenies  $E \rightarrow E$  together with pointwise addition  $+$  and composition  $\cdot$ . This is called the *Endomorphism ring* of  $E$ .

**Proposition 3.3.** *Let  $E$  be an elliptic curve. Then  $\text{End}(E)$  is a (possibly noncommutative) ring with unit.*

*Proof.* The only nontrivial part is to show distributivity, but this directly follows from Prop. 2.15.  $\square$

**Definition 3.4.** Let  $E$  be an elliptic curve. For  $m \in \mathbb{Z}$  denote by  $[m]$  the multiplication isogeny

$$E \rightarrow E, \quad P \mapsto \text{sgn}(m) \sum_{i=1}^{|m|} P$$

This is an isogeny by Lemma 3.1.

**Proposition 3.5.** *Let  $E$  be an elliptic curve. Then the ring homomorphism*

$$[\cdot] : \mathbb{Z} \rightarrow \text{End}(E), \quad m \mapsto [m]$$

*is injective.*

*Proof.* As  $[\cdot]$  is a ring homomorphism, it suffices to show  $[m] \neq 0$  for  $m \neq 0$ . For  $P = [x : y : 1] \in E$  we see that the  $x$ -coordinate of  $[2]P$  is

$$\begin{aligned} -2x + \lambda^2 &= \left( \frac{3x^2 + A}{2y} \right)^2 - 2x = \frac{9x^4 + 6Ax^2 + A^2 - 8x^4 - 8Ax^2 - 8xB}{4x^3 + 4Ax + 4B} \\ &= \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4x^3 + 4Ax + 4B} \end{aligned}$$

In particular, there are only finitely many  $x$  such that

$$x^4 - 2Ax^2 - 8Bx + A^2 = 0$$

and so only finitely many  $P \in E$  with  $P + P = O$ . Thus  $[2] \neq 0$ .

Consider now any  $m \in \mathbb{Z}$  with  $m = 2^k n, n \perp 2$  and assume  $[m] = 0$ . Then  $[2^k]$  annihilates only finitely many points, so  $[n]$  must annihilate infinitely many points. Hence  $[n] = 0$  as the fiber  $[n]^{-1}(O)$  is a subvariety of  $E$ . Now we show that  $E$  contains a 2-torsion point  $P$ , then  $[n]P = [(n-1)/2]O + P = P \neq O$  and we get a contradiction.

However, this is easy to see as there is some  $x$  with  $x^3 + Ax + B = 0$  and so  $(x, 0) + (x, 0) = O$  (we use that  $k$  is algebraically closed).  $\square$

### 3.1 Constructing Isogenies

The proof of Prop. 2.15 via the ideal class group is quite nice. However, using  $\text{Cl}(k[E])$  will stop to work when we want to construct new isogenies, as it is unclear that transferring a group homomorphism

$$\text{Cl}(k[E]) \rightarrow \text{Cl}(k[E'])$$

to  $E \rightarrow E'$  will result in an isogeny, i.e. a map given locally by polynomials. Now we will look at related ways to construct an isogeny.

**Lemma 3.6.** *Let  $f : C \dashrightarrow \mathbb{P}^m$  be a rational map on a smooth projective curve in  $\mathbb{P}^2$  (i.e. a 1-dimensional nonsingular projective variety). Then  $f$  is a morphism.*

*Proof.* wlog assume the set of definition of  $f$  is  $U \subseteq C$ . Now fix a point  $P \in C \setminus U$  and consider an affine chart  $\mathbb{A}^2 \subseteq \mathbb{P}^2$  such that  $P \in C_{\text{aff}} := C \cap \mathbb{A}^2$ .

It is a statement of Algebraic Geometry that for  $P \in C$ , we have for the tangent space  $T_P C$  of  $C$  at  $P$  that

$$T_P C \cong (\mathfrak{m}_P / \mathfrak{m}_P^2)^*$$

where  $\mathfrak{m}_P \subseteq k[C_{\text{aff}}]$  is the maximal ideal  $\langle x_1 - P_1, \dots, x_n - P_n \rangle$ . Since  $C$  is assumed to be smooth, we see that  $\dim T_P C = \dim C = 1$  and so  $\dim(\mathfrak{m}_P / \mathfrak{m}_P^2) = 1$ . Thus there is  $\alpha \in k[C_{\text{aff}}]_{\mathfrak{m}_P}^3$  such that

$$\mathfrak{m}_P = (\alpha) \subseteq k[C_{\text{aff}}]_{\mathfrak{m}_P}$$

Now let  $f = [f_0 : f_1 : f_2]$ . By assumption,  $P \notin U$  and so the rational map  $f_i(P) = 0$  for all  $i \leq 3$ . In other words, we have  $f_0, f_1, f_2 \in \mathfrak{m}_P$ . Now let  $d_i > 0$  be the greatest integer such that  $\alpha^{d_i}$  divides  $f_i$  and set  $d = \min\{d_0, d_1, d_2\}$ .

Now find that  $[f_0/\alpha^d : f_1/\alpha^d : f_2/\alpha^d] = [f_0 : f_1 : f_2]$  but for some  $i$ , have  $f_i/\alpha^d \notin \mathfrak{m}_P$ , so  $(f_i/\alpha^d)(P) \neq 0$ . This contradicts the assumption that  $f$  cannot be defined at  $P$ .  $\square$

Interestingly, this statement is the main reason why we require elliptic curves to be nonsingular.

**Lemma 3.7.** *Let  $E, E'$  be elliptic curves and*

$$f : k(E') \rightarrow k(E)$$

---

<sup>3</sup>This  $\alpha$  is also called *uniformizer*.

be a field homomorphism. Then there is a unique morphism

$$\psi : E \rightarrow E'$$

such that  $\psi^* = f$ .

*Proof.* Consider the rational map  $\psi := [f(x) : f(y) : 1] : E \rightarrow \mathbb{P}^2$ . By the previous lemma, this is a morphism.

Assume that  $E$  is given by  $E : y^2 = x^3 + Ax + B$ . Then, in  $k(E)$  we have that  $y^2 = x^3 + Ax + B$  and since  $f$  is a field homomorphism, we see that

$$f(y)^2 = f(x)^3 + Af(x) + B$$

It follows that  $\psi : E \rightarrow E'$ . The uniqueness follows easily from Prop. 1.4.  $\square$

### 3.2 The Frobenius morphism

For this subsection, assume  $p = \text{char}(k) > 2$  is an odd prime.

**Definition 3.8.** For an elliptic curve  $E : y^2 = x^3 + Ax + B$  and  $t \in \mathbb{N}$  define the elliptic curve  $E^{(q)}$  by

$$E^{(q)} : y^2 = x^3 + A^q x + B^q$$

where  $q = p^t$ . Further, define the *Frobenius morphism*

$$\pi_q := [x^q, y^q, 1] : E \rightarrow E^{(q)}$$

Note that the Frobenius endomorphism  $k \rightarrow k$ ,  $\alpha \mapsto \alpha^q$  has trivial kernel, and so the curve  $E^{(q)}$  has discriminant  $\Delta(E)^q \neq 0$  and is nonsingular, i.e. an elliptic curve.

**Lemma 3.9.** Let  $\psi : E \rightarrow E'$  be an isogeny. With the inseparability degree  $t := [k(E') : \psi^*k(E)]_i$  of the field extension  $k(E')|\psi^*k(E)$  we find that  $\psi$  factors as

$$E \xrightarrow{\pi_q} E^{(q)} \xrightarrow{\tilde{\psi}} E'$$

where  $q = p^t$  and  $\tilde{\psi} : E^{(q)} \rightarrow E'$  is some separable isogeny. Write  $\pi = \pi_p$ , so  $\pi_q = \pi^t$ .

*Proof.* Consider the field tower  $k(E)|F|\psi^*k(E')$  where  $F$  is the field of separable elements in  $k(E)$  (over  $\psi^*k(E')$ ). Now we will give a description of  $F$ .

For  $\alpha \in k(E)$  have that  $\text{MiPo}_F(\alpha) = X^{p^l} - a$ , for some  $l \in \mathbb{N}$  and  $a \in F$  since  $k(E)|F$  is purely inseparable. Since  $\deg(\text{MiPo}_F(\alpha)) \leq [k(E) : F] = t$ , we see that  $\alpha^q \in F$ . In particular,  $x^q, y^q \in F$ .

Now observe that  $k(x)|k(x^q)$  is obviously a field extension of degree  $q$ , and since 2 does not divide  $p$ , it follows that also  $k(x, y)|k(x^q, y^q)$  has degree  $q$ . Since  $x^q, y^q \in F$ , we find  $k(E)|F|k(x^q, y^q)$  and as  $[k(E) : F] = q$ , it already follows that  $F = k(x^q, y^q)$ .

Now observe that

$$k(E^{(q)}) \rightarrow k(E), \quad u \mapsto x^q, \quad v \mapsto y^q$$

is a well-defined field homomorphism with image  $k(x^q, y^q)$ . Hence  $k(E^{(q)}) \cong F$  and we have the field tower

$$k(E) \mid k(E^{(q)}) \mid \psi^*k(E')$$

which induces a field homomorphism  $k(E') \rightarrow k(E^q)$ ,  $a \mapsto \psi^*(a)$  (using  $k(E^{(q)}) \subseteq k(E)$ ). The previous lemma now gives us a morphism

$$\tilde{\psi} : E^{(q)} \rightarrow E'$$

with  $\tilde{\psi}^* = \psi^*$ . Further have that

$$\pi_q^* : k(E^{(q)}) \rightarrow E, \quad u = x^q \mapsto x^q, \quad v = y^q \mapsto y^q$$

is the identify on  $k(E^{(q)})$ . Hence  $(\tilde{\psi} \circ \pi_q)^* = \pi_q^* \circ \tilde{\psi}^* = \psi^*$  and the uniqueness in the previous lemma shows that

$$\psi = \tilde{\psi} \circ \pi_q$$

Since  $\psi$  and  $\pi_q$  map  $O$  to  $O$ , this must also be the case for  $\tilde{\psi}$ . So  $\tilde{\psi}$  is a separable isogeny and the claim follows.  $\square$

### 3.3 Dual Isogenies

**Lemma 3.10.** *Let  $\psi : E \rightarrow E'$  be a nonconstant morphism between elliptic curves such that  $k(E)|\psi^*k(E')$  is separable. Then  $\#\psi^{-1}(\{O\}) = \deg \psi$ .*

*Proof.* Let  $\psi = [\psi_0 : \psi_1 : 1]$  and consider

$$F := \text{MiPo}_{\psi^*k(E')}(x) = \sum_{n=0}^m a_n(\psi_0, \psi_1)T^n \in k(\psi_0, \psi_1)[T]$$

where  $a_n \in k(X, Y)$ . Note that  $m = \deg \psi$  as  $k(\psi_0, \psi_1, x) = k(x, y)$  by Lemma 2.7.

As  $k$  is infinite, we can now find  $(\lambda, \mu) \in E$  such that

$$F_{\lambda, \mu} = \sum_{n=0}^m a_n(\psi_0(\lambda, \mu), \psi_1(\lambda, \mu))T^n \in k[T]$$

is a separable polynomial of degree  $m$ . Hence, it has  $m$  distinct roots, say  $x_1, \dots, x_m$  in  $k$ .  $\square$

## Notes

Let  $p$  be a prime. Consider the category EC defined by

$$\begin{aligned} \text{Ob}(\text{EC}) &:= \{E \text{ elliptic curve over } \mathbb{F}_{p^2}\} \\ \text{Hom}_{\text{EC}}(E, E') &:= \{\psi : E \rightarrow E' \text{ isogeny}\} \end{aligned}$$

Have a functor

$$\begin{aligned} & \cdot^{(p)} : \mathbf{EC} \rightarrow \mathbf{EC} \\ & E \text{ defined by } y^2 = x^3 + Ax + B \mapsto E' \text{ defined by } y^2 = x^3 + A^p x + B^p \\ & \left[ \sum_{i,j} a_{ij} x^i y^j : \sum_{i,j} b_{ij} x^i y^j : \sum_{i,j} c_{ij} x^i y^j \right] \mapsto \left[ \sum_{i,j} a_{ij}^p x^i y^j : \sum_{i,j} b_{ij}^p x^i y^j : \sum_{i,j} c_{ij}^p x^i y^j \right] \end{aligned}$$

and a functor

$$\hat{\cdot} : \mathbf{EC} \rightarrow \mathbf{EC}^{\text{op}}, \quad E \mapsto E, \quad \phi \mapsto \hat{\phi}$$

$(d, \epsilon)$ -structures and their isogenies are given by the category  $\mathcal{C}$  defined by

$$\begin{aligned} \text{Ob}(\mathcal{C}) &:= \{(E, \psi) \mid E \in \mathbf{EC}, \psi : E \rightarrow E^{(p)}, \hat{\psi} = \epsilon \psi^{(p)}\} \\ \text{Hom}_{\mathcal{C}}((E, \psi), (E', \psi')) &:= \{\phi : E \rightarrow E' \mid \psi' \circ \phi = \phi^{(p)} \circ \psi\} \end{aligned}$$