Some Notes on Algebraic Maps, Elliptic Curves and Isogenies

Simon Pohmann

May 20, 2022

Contents

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 $S(X) := k[x_0, ..., x_n]/\mathbb{I}(X)$ 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 $X \to Y$ 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 $f_0, ..., f_m \in S(\bar{X})$ of same degree such that

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

- 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 $U \to Y$. 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, rational maps are morphisms $U \to Y$ with maximal domain $U \subseteq X$ open.

In particular, morphisms and rational maps are technically the same thing. The definitions just differ in the domain, not in the key property "locally defined by polynomials". This distinction is mostly an artifact of the definition of varieties via vanishing loci, and is no longer necessary when one uses the "modern" approach to algebraic geometry based on schemes.

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 $k[X] := k[x_1, ..., x_n]/\mathbb{I}(X)$.

This ring has a much tighter connection to the variety.

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

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

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 $k(X) := \mathrm{Frac}(k[X])$. For an irreducible projective variety $X \subseteq \mathbb{P}^n$, define the *function field* as

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

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*

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

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*

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

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 $\mathcal{O}_X(U) \to k(X)$.

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

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

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 $U_1 := U_{p_1}, ..., U_r := U_{p_r}$ with $p_1, ..., p_r \in X$.

As the U_i are an open cover, we see that $\mathbb{V}(\langle h_1, ..., h_r \rangle) = \emptyset$ 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). □

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*

$$\Phi : \{f : X \dashrightarrow \mathbb{P}^m \mid f \text{ rational map}\} \to \mathbb{P}^m_{k(X)},$$
$$f \text{ defined locally by } f_0, ..., f_m \in S(X) \mapsto \left[\frac{f_0}{x_0^d} : \frac{f_1}{x_0^d} : ... : \frac{f_n}{x_0^d}\right]$$

In particular, the restriction

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

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 $[f_0 : ... : f_m]$ 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

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

and similarly for open sets.

Remark 1.10. Note that the bijection Φ 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

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

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

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

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

Proposition 2.3. *Let $f : E \to E'$ 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'. □

Proposition 2.4. *If $\mathrm{char}(k) \neq 2, 3$ 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

$$\begin{aligned}\Delta(E) = &- b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6\\ \text{where}\quad &b_2 = a_1^2 + 4a_2\\ &b_4 = a_1a_3 + 2a_4\\ &b_6 = a_3^2 + 4a_6\\ &b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2\end{aligned}$$

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 $\psi = [\psi_0, \psi_1, 1] : E \to E'$ 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 μ_1, μ_2, μ_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

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

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

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

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. □

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

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

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*

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

Definition 2.11. Define the map

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

Definition 2.12. Define the map

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

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 $E(L) := E \cap \mathbb{P}^2_L = (E \cap L^2) \cup \{O\}$ form a subgroup*

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

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

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

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

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

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

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

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 ψ is surjective, so Algebraic Geometry tells us that ψ^* is injective. We can then define

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

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

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

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

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

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

Using the definition of ϕ we find

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

Explicitly computing the determinant of the multiplication map shows that

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

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 ($\psi(\lambda, \mu) \neq O$ 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

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

Hence

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

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

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

Together, modulo $\psi_1 - \psi_1(\lambda, \mu)$ we get [1]

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

So

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

and the claim follows. □

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-Roche 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 $\psi : E \to E'$ be an isogeny. We define the *degree* of ψ to be the degree of $k(E)|\psi^* k(E')$ and say that ψ 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 $j(E) = j(E')$.*

[1] Strictly speaking, we require $v(\mu, \psi_1(\lambda, \mu)) \neq 0$ here, which I haven't considered. 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

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

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 ψ 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 ψ 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

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

for some $u, v \in k[E]$ with $v^2 = u^3 + A'u + B'$ [2]. 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 ψ 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. □

Remark 2.20. In [Sil09], the above proof was done using the Riemann-Roche 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 $1, x, y$.

[2] 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 $\phi, \psi : E \to E'$ be isogenies on an elliptic curve E. Then $\phi + \psi$ (where addition is defined pointwise) is an isogeny $E \to E$.*

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 $\psi = [\psi_x : \psi_y : 1]$. □

Definition 3.2. For an elliptic curve E, consider the set $\mathrm{End}(E)$ of isogenies $E \to E$ 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 $\mathrm{End}(E)$ is a (possibly noncommutative) ring with unit.*

Proof. The only nontrivial part is to show distributivity, but this directly follows from Prop. 2.15. □

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

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

This is an isogeny by Lemma 3.1.

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

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

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). □

3.1 Constructing Isogenies

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

$$\mathrm{Cl}(k[E]) \to \mathrm{Cl}(k[E'])$$

to $E \to E'$ 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 $\langle x_1 - P_1, ..., x_n - P_n \rangle$. Since C is assumed to be smooth, we see that $\dim T_P C = \dim C = 1$ and so $\dim(\mathfrak{m}_P / \mathfrak{m}_P^2) = 1$. From this, it follows that $\mathfrak{m}_P \cdot k[C_{\text{aff}}]_{\mathfrak{m}_P}$ is principal (this fact requires Nakayama's lemma [3]). Thus there is $\alpha \in k[C_{\text{aff}}]_P := k[C_{\text{aff}}]_{\mathfrak{m}_P}$ [4] such that

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

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 α^{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. □

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

[3] I will not go deeper into that for now, see e.g. [Neu92, Chapter I §11 Exercise 7]

[4] This α is also called *uniformizer*. Note that it is not true that $\mathfrak{m}_P$ is principal, an error I have made before (e.g. consider $E : y^2 = x^3 - x$ and $P = (0, 0)$).

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

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

be a field homomorphism. Then there is a unique morphism

$$\psi : E \to E'$$

such that $\psi^* = f$.

Proof. Consider the rational map $\psi := [f(x) : f(y) : 1] : E \to \mathbb{P}^2$. 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 $\psi : E \to E'$. The uniqueness follows easily from Prop. 1.4. □

3.2 The Frobenius morphism

For this subsection, assume $p = \mathrm{char}(k) > 2$ 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*

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

Note that the Frobenius endomorphism $k \to k,\ \alpha \mapsto \alpha^q$ 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 $\psi : E \to E'$ 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 ψ factors as*

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

where $q = p^t$ and $\tilde{\psi} : E^{(q)} \to E'$ 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 $\mathrm{MiPo}_F(\alpha) = X^{p^l} - a$, for some $l \in \mathbb{N}$ and $a \in F$ since $k(E)|F$ is purely inseparable. Since $\deg(\mathrm{MiPo}_F(\alpha)) \leq [k(E) : F] = t$, 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

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

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

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

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

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

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 ψ and π_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. □

Proposition 3.10. *Let $\tau : E \to E'$ be a separable morphism of degree n between Elliptic Curves $E, E' \subseteq \mathbb{P}^2$. Then $\#\tau^{-1}(\{P\}) = n$ for all but finitely many $P \in E'$.*

Proof. Let $\tau = [\tau_x : \tau_y : 1]$. Consider then the minimal polynomial $f(T, \tau_x, \tau_y) \in \tau^* k(E)[T]$. By assumption, this is separable and has degree n (in T). In particular, it follows that $f(T, \tau_x(P), \tau_y(P))$ is separable of degree n for all but finitely many $P \in E$. Since τ is surjective, find that $f(T, x, y)$ is separable of degree n for all but finitely many $P = (x, y) \in E'$. Hence, it has n distinct roots, say $\beta_1, ..., \beta_n$.

Now write

$$S := \{(u, v) \in E \mid u \in \{\beta_1, ..., \beta_n\}\}, \quad S' = \{(u, v) \in E' \mid u = x\}$$

and find that $\tau(Q) \in S'$ if and only if $Q \in S$. Furthermore, by excluding finitely many P, we can assume that $\#S = 2n$ and $\#S' = 2$ (there are only finitely many cases such that x or β_i give a point of higher multiplicity).

Clearly $\tau^{-1}(\{Q\})$ is a variety of degree n, so $\#\tau^{-1}(\{Q\}) \leq n$ for all Q. Thus we must already have that the map $S \to S'$ is n-to-1 and so $\#\tau^{-1}(\{P\}) = n$. □

Corollary 3.11. *Let $\psi : E \to E'$ be a separable isogeny. Then $\#\ker\psi = \deg(\psi)$.*

Proof. By the previous theorem, there exists a point P' such that $\#\psi^{-1}(\{P'\}) = n$. Now the claim follows, since there is a bijection

$$\ker\psi \to \psi^{-1}(\{P'\}), \quad Q \mapsto Q + P$$

where $P \in E$ such that $\psi(P) = P'$. □

4 Isogeny graphs

This is a quite specialized topic, going further into the methods I am currently studying. Furthermore, it is not present in Silverman anymore.

Definition 4.1. Let E be an Elliptic Curve defined over k. Then denote

$$\begin{aligned}\mathrm{End}_k(E) &:= \{\phi \in \mathrm{End}(E) \mid \phi \text{ defined over } k\}\\ \mathrm{End}^0(E) &:= \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}\end{aligned}$$

4.1 Horizontal and vertical isogenies

Proposition 4.2. *Let E, E' be Elliptic Curves defined over a field k and consider an isogeny $\phi : E \to E'$ of prime degree l. Then* $\mathrm{End}(E)$ *and* $\mathrm{End}(E')$ *have the same rank $r \leq 4$ (as free $\mathbb{Z}$-modules), and*

$$l^2 O \subseteq lO' \subseteq O \subseteq \mathcal{K}$$

via an embedding $\mathrm{End}(E') \to \mathrm{End}^0(E)$.

Proof. Consider the map

$$\Phi_* : \mathrm{End}(E) \to \mathrm{End}(E'), \quad \tau \mapsto \phi \circ \tau \circ \hat{\phi}$$

and

$$\Phi^* : \mathrm{End}(E') \to \mathrm{End}(E), \quad \tau \mapsto \hat{\phi} \circ \tau \circ \phi$$

Then these are injective $\mathbb{Z}$-module homomorphisms with $\Phi_* \circ \Phi^* = [l^2] \circ \cdot$. In particular, find that

$$\frac{\Phi^*}{l} : \mathrm{End}^0(E') \to \mathrm{End}^0(E)$$

is an isomorphism of $\mathbb{Q}$-algebras[5]. In other words, both $\mathcal{O} := \mathrm{End}(E)$ and $\mathcal{O}' := \mathrm{End}(E')$ are orders in $\mathcal{K} := \mathrm{End}^0(E)$.

Now observe that the inclusion $[l^2]\mathcal{O} \to \mathcal{O}$ factors through $\mathcal{O}'$ via

$$l^2\mathcal{O} \overset{\Phi_*/l}{\to} l\mathcal{O}' \overset{\Phi^*/l}{\to} \mathcal{O}$$

and these embeddings are compatible with the embeddings $\mathcal{O}, \mathcal{O}' \to \mathcal{K}$. In other words, have $l^2\mathcal{O} \subseteq l\mathcal{O}' \subseteq \mathcal{O} \subseteq \mathcal{K}$. □

Corollary 4.3. *Let E, E' be Elliptic Curves defined over a field k and consider an isogeny $\phi : E \to E'$ of prime degree l. Suppose that that* $\mathrm{End}(E)$ *has rank 2 (i.e. a CM curve, or an ordinary curve over $k = \mathbb{F}_q$). Then one of the following is true*

- $\mathrm{End}(E) = \mathrm{End}(E')$ *and ϕ is called* horizontal

[5] If it is not completely clear what this means in the non-commutative case, just look at $\mathrm{End}(E)$ resp. $\mathrm{End}(E')$ as a free $\mathbb{Z}$-module of finite rank.

- $[\mathrm{End}(E) : \mathrm{End}(E')] = l$ *and* ϕ *is called* descending
- $[\mathrm{End}(E') : \mathrm{End}(E)] = l$ *and* ϕ *is called* ascending

Proof. Let $\mathcal{O} := \mathrm{End}(E)$ and $\mathcal{O}' := \mathrm{End}(E')$. By the previous proposition, have $l^2\mathcal{O} \subseteq l\mathcal{O}' \subseteq \mathcal{O}$ and clearly $[\mathcal{O} : l^2\mathcal{O}] = l^4$. Since l is prime and $\mathcal{O}' \neq l\mathcal{O}$ resp. $\mathcal{O} \neq l\mathcal{O}'$ (both $\mathcal{O}$ and $\mathcal{O}'$ contain 1), find that either

- $[\mathcal{O}' : l\mathcal{O}] = l^2$ and $[\mathcal{O} : l\mathcal{O}'] = l^2$
- $[\mathcal{O}' : l\mathcal{O}] = l$ and $[\mathcal{O} : l\mathcal{O}'] = l^3$
- $[\mathcal{O}' : l\mathcal{O}] = l^3$ and $[\mathcal{O} : l\mathcal{O}'] = l$

These are exactly the cases that ϕ is horizontal, descending and ascending, respectively. □

4.2 A class group action

Definition 4.4. For any (non-commutative) ring $\mathcal{O}$ write

$$\mathrm{Ell}(\mathcal{O}) := \{E \mid \mathrm{End}(E) \cong \mathcal{O}\}/\cong$$

for the set of isomorphism classes of Elliptic Curves with endomorphism ring $\mathcal{O}$. Write further

$$\mathrm{Ell}_k(\mathcal{O}) := \{[E] \in \mathrm{Ell}(\mathcal{O}) \mid E \text{ defined over } k\}$$

Theorem 4.5. *Let* E, E *be Elliptic Curves such that* $\mathrm{End}(E) \cong \mathrm{End}(E')$. *Then there is a separable isogeny* $E \to E'$.

Lemma 4.6. *Let* E, E' *be Elliptic Curves with* $\mathrm{End}(E) \cong \mathrm{End}(E')$ *and* $\phi, \psi : E_1 \to E_2$ *be nonconstant isogenies. Then* $\Phi_* = \Psi_*$.

Proof. Let $\alpha \in \mathrm{End}(E)$. We have to show that

$$\tau := \frac{\phi \circ \alpha \circ \hat{\phi}}{\deg(\phi)} - \frac{\psi \circ \alpha \circ \hat{\psi}}{\deg(\psi)} = O$$

Assume τ is nonconstant, then so is

$$\tau' := \deg(\phi)(\hat{\psi} \circ \tau \circ \psi) = (\hat{\psi} \circ \phi) \circ \alpha \circ (\hat{\phi} \circ \psi) - \deg(\phi)\deg(\psi)\alpha$$

Note that $\hat{\psi} \circ \phi$ and $\hat{\phi} \circ \psi$ are endomorphisms of E, thus by commutativity of $\mathrm{End}(E)$ we find

$$\tau' = (\hat{\psi} \circ \phi)(\hat{\phi} \circ \psi)\alpha - \deg(\phi)\deg(\psi)\alpha = \deg(\phi)\deg(\psi)\alpha - \deg(\phi)\deg(\psi)\alpha = O$$

since $\hat{\psi} \circ \phi$ is dual to $\hat{\phi} \circ \psi$. So τ must be constant and the claim follows. □

This shows that for any two curves E, E' with $\mathrm{End}(E) \cong \mathrm{End}(E')$ there is a unique canonical isomorphism

$$\Phi_* : \mathrm{End}(E) \to \mathrm{End}(E')$$

Since quadratic number fields always have one nontrivial automorphism, this is not the only isomorphism, but the only one given by isogenies. Furthermore, if $\mathrm{End}(E) \cong \mathrm{End}(E') \cong \mathrm{End}(E'')$ then the diagram of canonical isomorphisms

$$\begin{array}{ccccc} \mathrm{End}(E) & \longrightarrow & \mathrm{End}(E') & \longrightarrow & \mathrm{End}(E'') \\ & \searrow & & \nearrow & \end{array}$$

commutes.

Proposition 4.7. *Let E be an ordinary Elliptic Curve defined over k and assume that $\mathcal{O} := \mathrm{End}(E)$ is an order in a quadratic imaginary number field. For an ideal $\mathfrak{a} \leq \mathcal{O}$ define*

$$E[\mathfrak{a}] := \bigcap_{a \in \mathfrak{a}} \ker(a)$$

Then the map

$$\mathrm{Cl}(\mathcal{O}) \times \mathrm{Ell}(\mathcal{O}) \to \mathrm{Ell}(\mathcal{O}), \quad ([\mathfrak{a}], [E]) \mapsto [E/E[\mathfrak{a}]]$$

defines a (well-defined) group action of $\mathrm{Cl}(\mathcal{O})$ on $\mathrm{Ell}(\mathcal{O})$ (we choose $\mathfrak{a}$ to be an integral ideal representative of the class $[\mathfrak{a}]$)[6]*.*

Proof. First, we show that $\mathrm{End}(E/E[\mathfrak{p}]) \cong \mathcal{O}$ for an invertible ideal $\mathfrak{p} \leq \mathcal{O}$.

Now we show that for (invertible) ideals $\mathfrak{a}, \mathfrak{b} \leq \mathcal{O}$, we have

$$E/E[\mathfrak{b}\mathfrak{a}] \cong E'/E'[\mathfrak{a}] \quad \text{where } E' = E/E[\mathfrak{b}]$$

The tricky part here is that we identified the isomorphic endomorphism rings $\mathrm{End}(E)$ and $\mathrm{End}(E')$, but the isomorphism is only on the level of rings (and we also need the kernel of endomorphisms). So let's be explicit about which ring we are in.

Consider the isogenies

$$\begin{aligned} &\phi : E \to E' = E/E[\mathfrak{b}] \quad \text{with kernel } E[\mathfrak{b}] \\ &\psi : E' \to E'/E'[\mathfrak{a}] \quad \text{with kernel } E'[\mathfrak{a}] \end{aligned}$$

It suffices to show that $\ker(\psi \circ \phi) = E[\mathfrak{b}\mathfrak{a}]$.

[6] Note that for a curve E' that is not E, the notation $E'[\mathfrak{a}]$ means $E'[\Phi_*(\mathfrak{a})]$ where Φ_* is the canonical isomorphism $\mathrm{End}(E) = \mathcal{O} \to \mathrm{End}(E')$.

Consider any $\tau \in \mathfrak{a}$ and let τ' be the image under the isomorphism $\mathrm{End}(E) \cong \mathrm{End}(E')$. Now have that $\tau' \circ \phi = \phi \circ \tau$ (since the isomorphism is Φ_*). Hence

$$\begin{aligned}\ker(\psi \circ \phi) =& \phi^{-1}(\ker \psi) = \phi^{-1}(E'[\mathfrak{a}]) = \phi^{-1}\Big(\bigcap_{\tau \in \mathfrak{a}} \ker(\tau')\Big) \\ =& \bigcap_{\tau \in \mathfrak{a}} \phi^{-1}(\ker(\tau')) = \bigcap_{\tau \in \mathfrak{a}} \ker(\tau' \circ \phi) = \bigcap_{\tau \in \mathfrak{a}} \ker(\phi \circ \tau) = \bigcap_{\tau \in \mathfrak{a}} \tau^{-1}(\ker \phi) \\ =& \bigcap_{\tau \in \mathfrak{a}} \tau^{-1}(E[\mathfrak{b}]) = \bigcap_{\tau \in \mathfrak{a},\ \rho \in \mathfrak{b}} \tau^{-1}(\ker \rho) = \bigcap_{\tau \in \mathfrak{a},\ \rho \in \mathfrak{b}} \ker(\underbrace{\rho \circ \tau}_{= \rho\tau \in \mathrm{End}(E)}) = E[\mathfrak{b}\mathfrak{a}]\end{aligned}$$

The claim now follows, since clearly $E/E[(\alpha)] \cong E$ for a principal ideal $(\alpha) \leq \mathrm{End}(E)$. □

Proposition 4.8. *This action is faithful (even free?) and transitive.*

Proposition 4.9 (CSIDH class group action)**.** *Let E be an Elliptic Curve defined over $k := \mathbb{F}_p$. Denote $\mathcal{O} := \mathrm{End}_k(E)$. Then $\mathrm{Cl}(\mathcal{O})$ acts on $\mathrm{Ell}_k(\mathcal{O})$ via*

$$\mathrm{Cl}(\mathcal{O}) \times \mathrm{Ell}_k(\mathcal{O}) \to \mathrm{Ell}_k(\mathcal{O}), \quad ([\mathfrak{a}], E) \mapsto [E/E[\mathfrak{a}]]$$

Proposition 4.10. *This action is faithful (even free?) and transitive.*

Remark 4.11. If E is a supersingular Elliptic Curve defined over $k := \mathbb{F}_p$, then $\pi^2 = -p$ and so $\mathrm{End}_k(E) \cong \mathbb{Z}[\sqrt{-p}]$. Conversely, if E is ordinary, then $\pi^2 + t\pi + p = 0$ for $t \neq 0$ and so $\mathrm{End}_k(E) \cong \mathbb{Z}[\alpha]$ with $\alpha = \sqrt{t^2/4 - p}$ or $\alpha = 1/2 + \sqrt{t^2/4 - p}$. Hence

$$\mathrm{Ell}_k(\mathbb{Z}[\sqrt{-p}]) = \{E \mid E \text{ supersingular Elliptic Curve defined over } k = \mathbb{F}_p\}/\cong$$

4.3 Summary - Ordinary Elliptic Curves

Theorem 4.12. *Let E be an ordinary Elliptic Curve defined over $\mathbb{F}_q$. Let $\mathcal{O} := \mathrm{End}(E)$ and π be the q-th power Frobenius endomorphism of E. Furthermore, let $t \in \mathbb{Z}$ be the trace of π. Then*

- *$\mathcal{O}$ is an order in the quadratic imaginary number field $\mathbb{Q}[\sqrt{D}]$ where $D = t^2 - 4q$. Note that $\mathbb{Q}[\sqrt{D}] = \mathbb{Q}[\sqrt{D'}]$ if $D = a^2 D'$, and in general D is not square-free.*
- *$\mathbb{Z}[\pi] \subseteq \mathcal{O}$ (in general no equality).*
- *For an integral ideal $\mathfrak{a} \leq \mathcal{O}$ such that $p \nmid [\mathcal{O} : \mathfrak{a}]$, the isogeny $E \to E/E[\mathfrak{a}]$ has degree $[\mathcal{O} : \mathfrak{a}]$.*

There is a faithful and transitive group action of $\mathrm{Cl}(\mathcal{O})$ on $\mathrm{Ell}(\mathcal{O})$ via $[\mathfrak{a}].E = E/E[\mathfrak{a}]$.