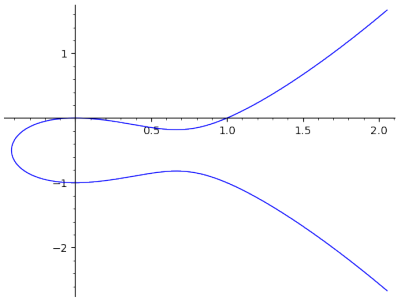
Elliptic Curves and their Endomorphism Rings

1 Elliptic curve as a pointed algebraic curve



The blue curve in the picture contains points $(x, y), x, y \in \mathbb{R}$ satisfying equation $y^2 = x^3 - 432x + 8208$. This picture is obtained from "The L-functions and modular forms database". (LMFDB, https://www.lmfdb.org/) It shows the set of real points on the elliptic curve labelled 11.a3.

By an elliptic curve, we mean a smooth genus 1 algebraic curve with a marked point. Every equation $y^2 = x^3 + Ax + B$ satisfying $4A^3 + 27B^2 \neq 0$ defines an elliptic curve. Namely, there is a smooth projective model corresponding to this affine curve with the marked point the single point at ∞.

Definition 1.1. An *elliptic curve* defined over a field K is a pair (E, O), where E is a smooth curve of genus 1 defined over K and $O \in E(K)$.

When the characteristic of the field K is not 2 or 3, then any elliptic curve (E, O) satisfies an affine defining equation of the form $y^2 = x^3 + Ax + B$, $A, B \in K$, with O placed at ∞. A defining equation of the form $y^2 = f(x)$ with $\deg f = 3$ is called a *Weierstrass equation* for the associated elliptic curve.

Since an elliptic curve E/K is an algebraic curve of genus 1, the set of holomorphic differentials on E is a 1-dimensional K vector space which we simply denote by V.

If E is given by the affine equation $y^2 = x^3 + Ax + B$, then the differential

$$\omega = \frac{dx}{y}$$

is both holomorphic and non-vanishing. Thus, the vector space $V = \{a\omega \mid a \in K\}$.

2 Elliptic curve as an algebraic group

For an algebraic curve C/K, let $\mathrm{Pic}^0(C)$ be its divisor class group, defined as the set of degree 0 divisors over $\overline{K}$ modulo its subset of principal divisors. The Galois group $\mathrm{Gal}(\overline{K}/K)$ acts on $\mathrm{Pic}^0(C)$ via its action on $C(\overline{K})$.

Definition 2.1. The map $\phi : E(\overline{K}) \to \mathrm{Pic}^0(E) : P \mapsto (P - O)$ from the curve to its divisor class group is a bijection. The group law

$$E \times E \to E : (P_1, P_2) \mapsto \phi^{-1}(\phi(P_1) + \phi(P_2))$$

and $E \to E : P \mapsto \phi^{-1}(-\phi(P))$ induced on E is an algebraic morphism defined over K.

This group law makes elliptic curves projective group schemes of dimension 1. Higher dimensional projective varieties with an algebraic group structure are called *abelian varieties* which is the topic of AWS 2024.

Remark 2.2. For any field L/K and an elliptic curve E/K, the group law makes the set $E(L)$ into an abelian group. Then it is natural to ask whether $E(L)$ is a finitely generated abelian group. The Mordell–Weil theorem states that when L is a number field, $E(L)$ is finitely generated. On the other hand, when $L = \overline{\mathbb{Q}}$, even the torsion part of $E(L)$ is not finitely generated. Given an elliptic curve E/K, for which L/K is $E(L)$ finitely generated is a problem among current study in the realm of Diophantine stability.

3 Morphisms between elliptic curves: Isogenies

After introducing the objects which we call elliptic curves, our next goal is to study morphisms between elliptic curves. These morphisms will be regular maps between algebraic curves which are also group homomorphisms. Such a morphism is called an isogeny.

Definition 3.1. An *isogeny* between elliptic curves (E_1, O_1) and (E_2, O_2) is an algebraic map $E_1 \to E_2$ which maps O_1 to O_2. The map $\phi : E_1 \to O_2$ is called the trivial isogeny. Any nontrivial isogeny is a group homomorphism with finite kernel.

Since isogenies are regular maps between algebraic curves, they induces maps between their divisor class groups Pic^0 and their sets of holomorphic differentials V. Both of the induced maps are very important tools in our study of isogenies.

Definition 3.2. Let $\phi : E_1 \to E_2$ be a nontrivial isogeny. Then it induces a map $\phi^* : \mathrm{Pic}^0(E_2) \to \mathrm{Pic}^0(E_1)$. By composing isomorphisms $E_i \simeq \mathrm{Pic}^0(E_i)$, we obtain an isogeny $\hat{\phi} : E_2 \to E_1$ which is called *the dual isogeny* of ϕ.

The next lemma follows from the definition of the group law on elliptic curves and the dual isogeny. It will play an important role in studying the structure of the endomorphism ring $\mathrm{End}(E)$.

Lemma 3.3. $\hat{\phi} \circ \phi = [\deg \phi]$.

4 The structure of the endomorphism ring $\mathrm{End}(E_{\overline{K}})$

We write $\mathrm{Hom}(E_1, E_2)$ to be the set of isogenies between E_1 and E_2 over K and $\mathrm{End}(E)$ the set of isogenies from E to itself over K. We will denote by $\mathrm{End}(E_{\overline{K}})$ the set of endomorphisms from E to itself base changed to the algebraic closure $\overline{K}$. Next we discuss some properties of the set of isogenies between two elliptic curves E_1, E_2.

Lemma 4.1. *The of isogenies* $\mathrm{Hom}(E_1, E_2)$ *is a free abelian group under the addition law* $(\phi + \psi)(P) := \phi(P) + \psi(P)$ *and the identity element being the trivial isogeny.*

Proof. The multiplication by m map (denoted as ϕ_m) is an isogeny and $m\phi = \phi_m \circ \phi$. The composition of two dominant maps is dominant. Thus, $\mathrm{Hom}(E_1, E_2)$ is torsion-free. □

Lemma 4.2. *The endomorphisms ring* $\mathrm{End}(E)$ *with multiplication being composition is an integral domain.*

Proof. The composition of two dominant maps is dominant. □

Let E_1, E_2 be elliptic curves given by Weierstrass equations. Let ω_1, ω_2 be the holomorphic differentials given by dx/y on E_1, E_2 respectively and let V_i be the K-vector space of holomorphic differentials on E_i. For an isogeny $\phi : E_1 \to E_2$, we look at the induced map $\phi^* : V_2 \to V_1$.

Proposition 4.3. *Let E be an elliptic curve given by a Weierstrass equation $y^2 = x^3 + Ax + B$ and let $\omega = dx/y$. The differential ω is invariant under translation maps on E.*

Theorem 4.4. *Let $\phi, \psi : E_1 \to E_2$ be two isogenies and $\phi^*, \psi^* : V_2 \to V_1$ the induced maps, then*

$$(\phi + \psi)^* \omega = \phi^* \omega + \psi^* \omega.$$

Moreover, the map $\mathrm{End}(E) \to \mathrm{End}(V) \simeq K : \phi \to \phi^*$ is a ring homomorphism with kernel being the inseparable morphisms (morphisms whose induced map on the function fields is an inseparable field extension).

Corollary 4.5. *If K is a field of characteristic 0, then $\mathrm{End}(E_{\overline{K}})$ is a **commutative** subring of $\overline{K}$.*

Recall that following the set of isomorphism theorems for groups, every group homomorphism $\phi : G \to H$ is determined by its kernel $\mathrm{Ker}\,\phi$ which is a normal subgroup of G (up to an isomorphism of H).

To study $\mathrm{End}(E_{\overline{K}})$, we next look at the finite subgroups of $E(\overline{K})$.

Lemma 4.6. *When m is coprime to the characteristic of the field K, we have $E(\overline{K})[m] \simeq (\mathbb{Z}/m\mathbb{Z})^2$ where $E(\overline{K})[m]$ denotes the kernel of the multiplication by m map $\phi_m : E \to E,\ P \mapsto mP$.*

Proof. First note that the dual isogeny to the multiplication by m map is itself, $\widehat{\phi}_m = \phi_m$. Since ϕ_m is separable by assumption, we conclude $|E/mE| = \deg \phi_m = m^2$. □

Any isogeny $\phi : E_1 \to E_2$ induces a map $E_1[m] \to E_2[m]$ for any $m \in \mathbb{Z}_{>0}$. For any prime ℓ coprime to the characteristic of the field K, there is an injection

$$\mathrm{Hom}(E_1, E_2) \hookrightarrow \mathrm{Hom}(E_1[\ell^\infty], E_2[\ell^\infty]).$$

Moreover, the following map is also injective.

$$\mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_\ell \hookrightarrow \mathrm{Hom}(E_1[\ell^\infty], E_2[\ell^\infty]).$$

Lemma 4.7. $\mathrm{End}(E_{\overline{K}})$ *is a free $\mathbb{Z}$-module of rank at most 4.*

Proof. Using the injectivity of the above map, we have

$$\mathrm{rank}_{\mathbb{Z}} \mathrm{End}(E_{\overline{K}}) = \mathrm{rank}_{\mathbb{Z}_\ell} \mathrm{End}(E_{\overline{K}}) \otimes \mathbb{Z}_\ell \leq \mathrm{rank}_{\mathbb{Z}_\ell} \mathrm{Hom}(E[\ell^\infty], E[\ell^\infty]) = 4.$$

□

Theorem 4.8. *For an elliptic curve E defined over a field K. The endomorphism ring $\mathrm{End}(E_{\overline{K}})$ is either isomorphic to $\mathbb{Z}$, an order of a quadratic imaginary field, or an order of a quaternion algebra over $\mathbb{Q}$.*

If K is of characteristic 0, then $\mathrm{End}(E_{\overline{K}})$ is commutative.

If K is a finite field, then $\mathrm{End}(E_{\overline{K}})$ strictly contains $\mathbb{Z}$.

Proof. The endomorphism ring $\mathrm{End}(E_{\overline{K}})$ satisfies the following statements:

1. $\mathrm{End}(E_{\overline{K}})$ is a free $\mathbb{Z}$-module of rank at most 4, and an integral domain;
2. there is an involution $\mathrm{End}(E_{\overline{K}}) \to \mathrm{End}(E_{\overline{K}}) : \phi \mapsto \hat{\phi}$;
3. For any isogeny $\phi \in \mathrm{End}(E_{\overline{K}})$, the product $\phi\hat{\phi}$ is a non-negative integer, and $\phi\hat{\phi} = 0 \Rightarrow \phi = 0$.

A ring satisfying these three conditions can only be one of the three types stated above.

When K is of characteristic 0, $\mathrm{End}(E_{\overline{K}})$ is commutative following from Theorem 4.4.

When K is a finite field $\mathbb{F}_q$, the Frobenius morphism is purely inseparable of degree q and it is different from the multiplication by $\sqrt{q}$ map even when q is a square. □

For an elliptic curve E/K where K has characteristic 0, if $\mathrm{End}(E_{\overline{K}})$ strictly contains $\mathbb{Z}$, we say E has **complex multiplication**.