Mathematics of Isogeny-based Cryptography

Luca De Feo

IBM Research, Zürich

September 16, 2019
Isogeny-based Cryptography Workshop
Birmingham

Slides online at https://defeo.lu/docet

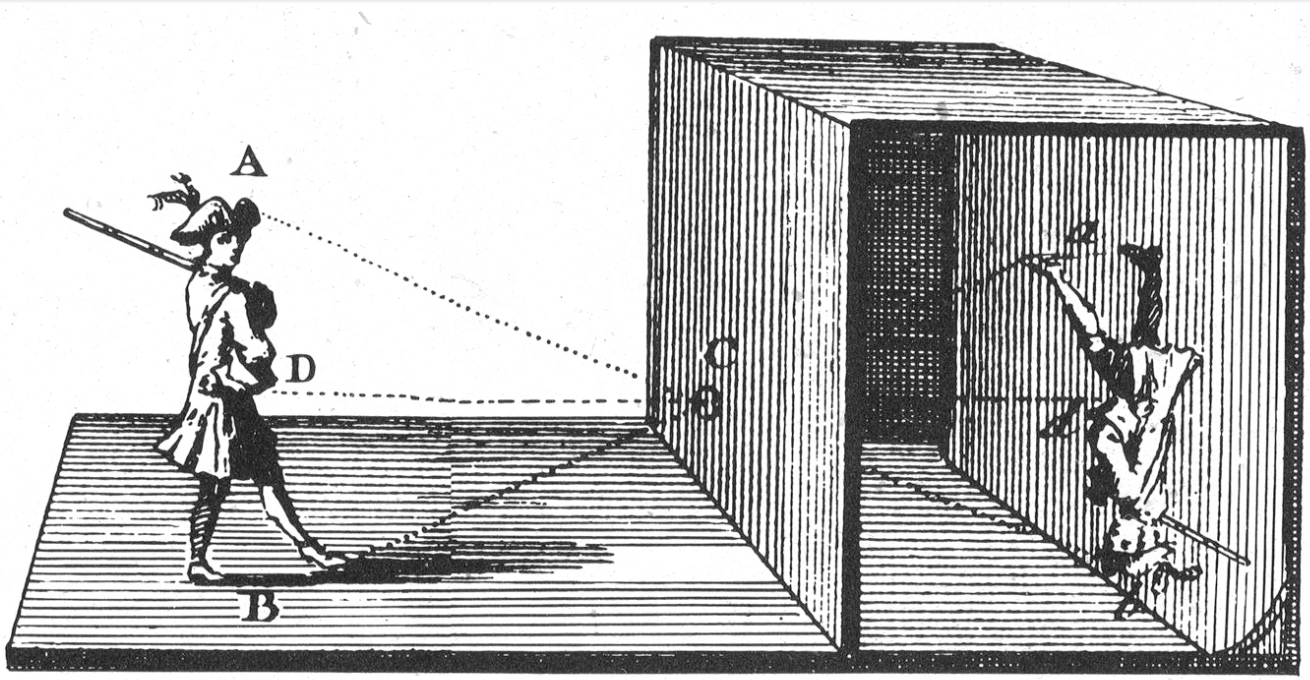
Projective space

Definition (Projective space)

Let $\bar{k}$ an algebraically closed field, the projective space $\mathbb{P}^n(\bar{k})$ is the set of non-null $(n+1)$-tuples $(x_0, \ldots, x_n) \in \bar{k}^n$ modulo the equivalence relation

$$(x_0, \ldots, x_n) \sim (\lambda x_0, \ldots, \lambda x_n) \qquad \text{with } \lambda \in \bar{k} \setminus \{0\}.$$

A class is denoted by $(x_0 : \cdots : x_n)$.

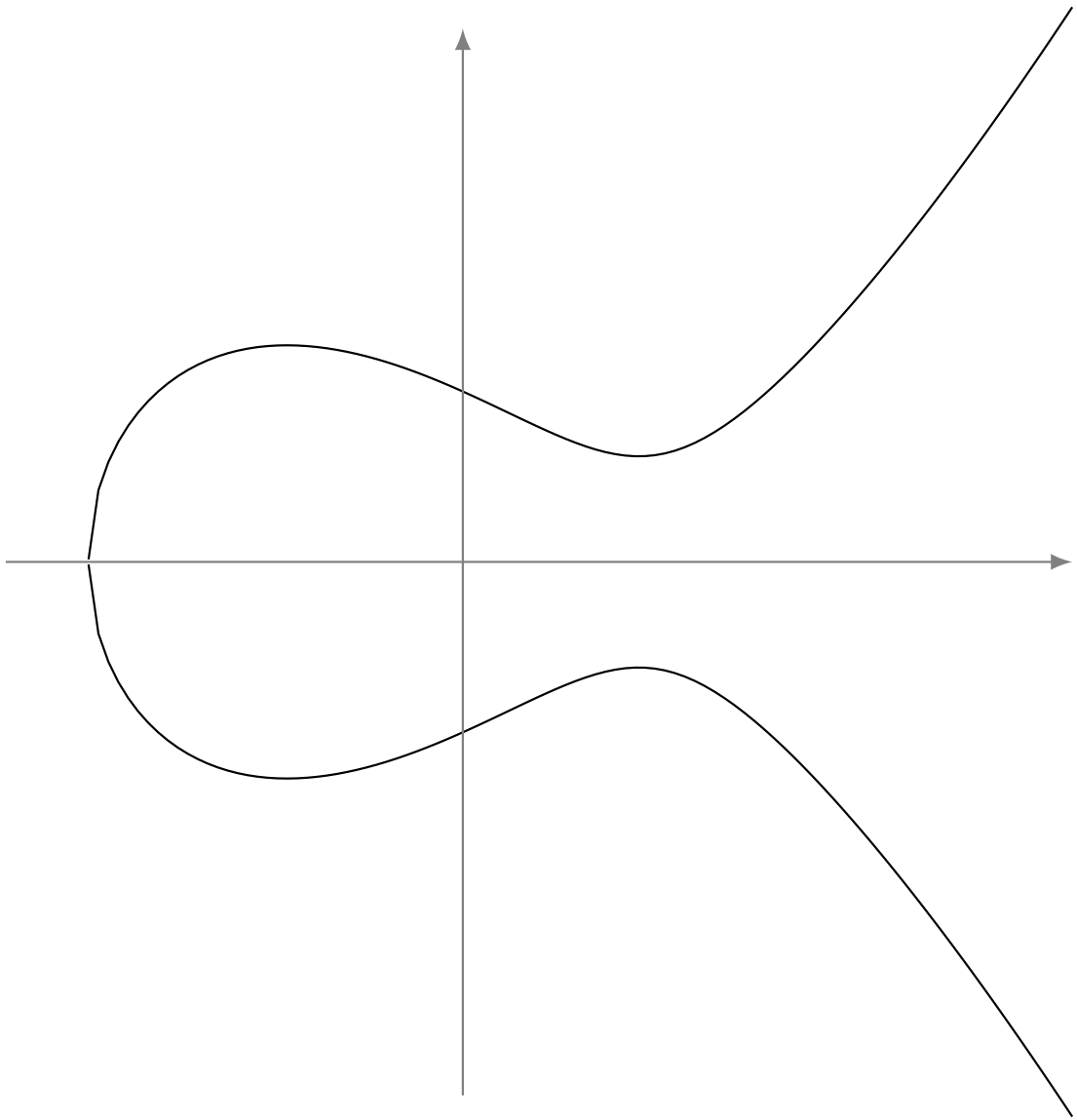


Weierstrass equations

Let k be a field of characteristic $\neq 2, 3$.
An elliptic curve *defined over* k is the locus in $\mathbb{P}^2(\bar{k})$ of an equation

$$Y^2Z = X^3 + aXZ^2 + bZ^3,$$

where $a, b \in k$ and $4a^3 + 27b^2 \neq 0$.



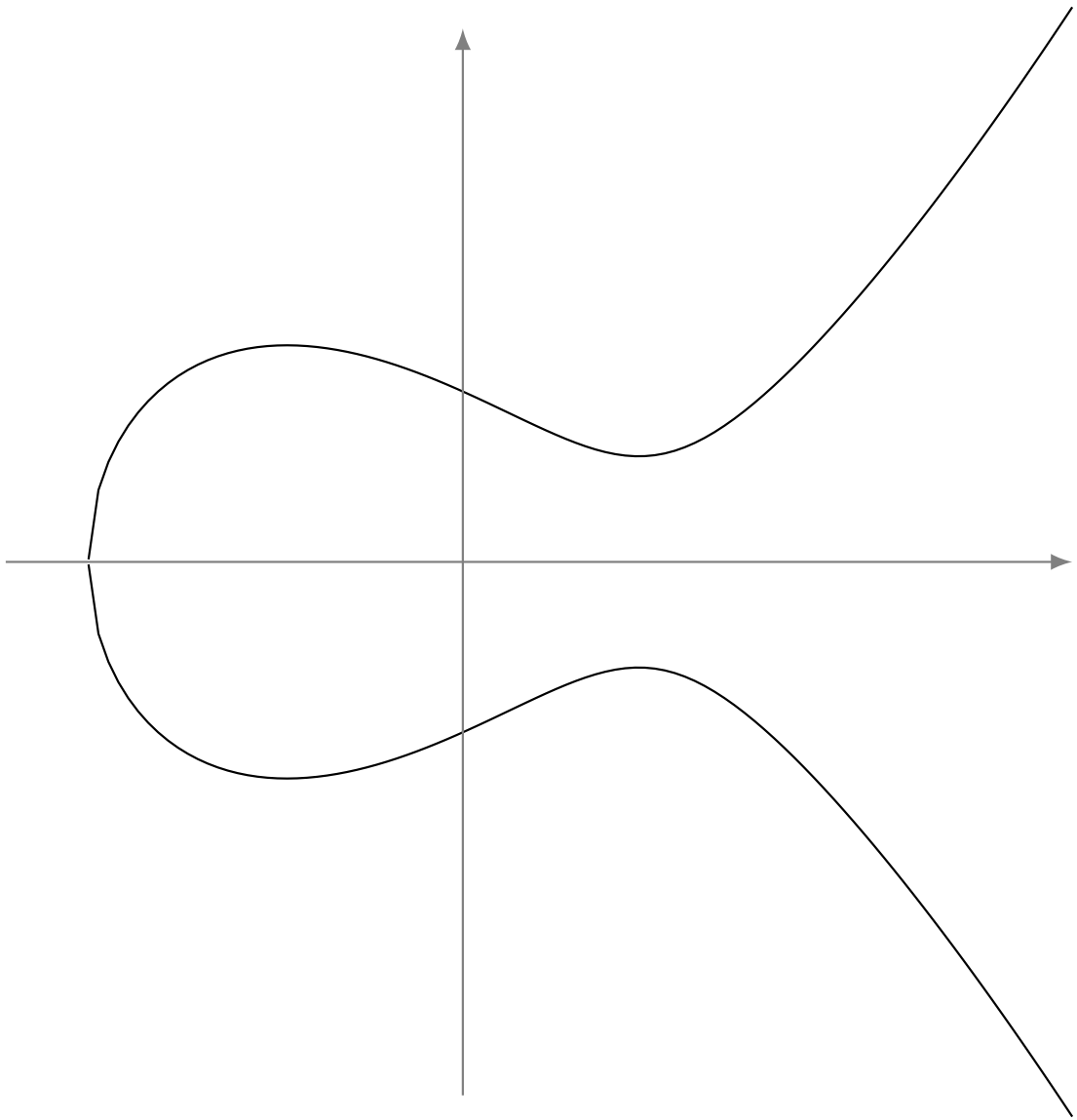
Weierstrass equations

Let k be a field of characteristic $\neq 2, 3$.
An elliptic curve *defined over* k is the locus in $\mathbb{P}^2(\bar{k})$ of an equation

$$Y^2Z = X^3 + aXZ^2 + bZ^3,$$

where $a, b \in k$ and $4a^3 + 27b^2 \neq 0$.

- $\mathcal{O} = (0 : 1 : 0)$ is the point at infinity;



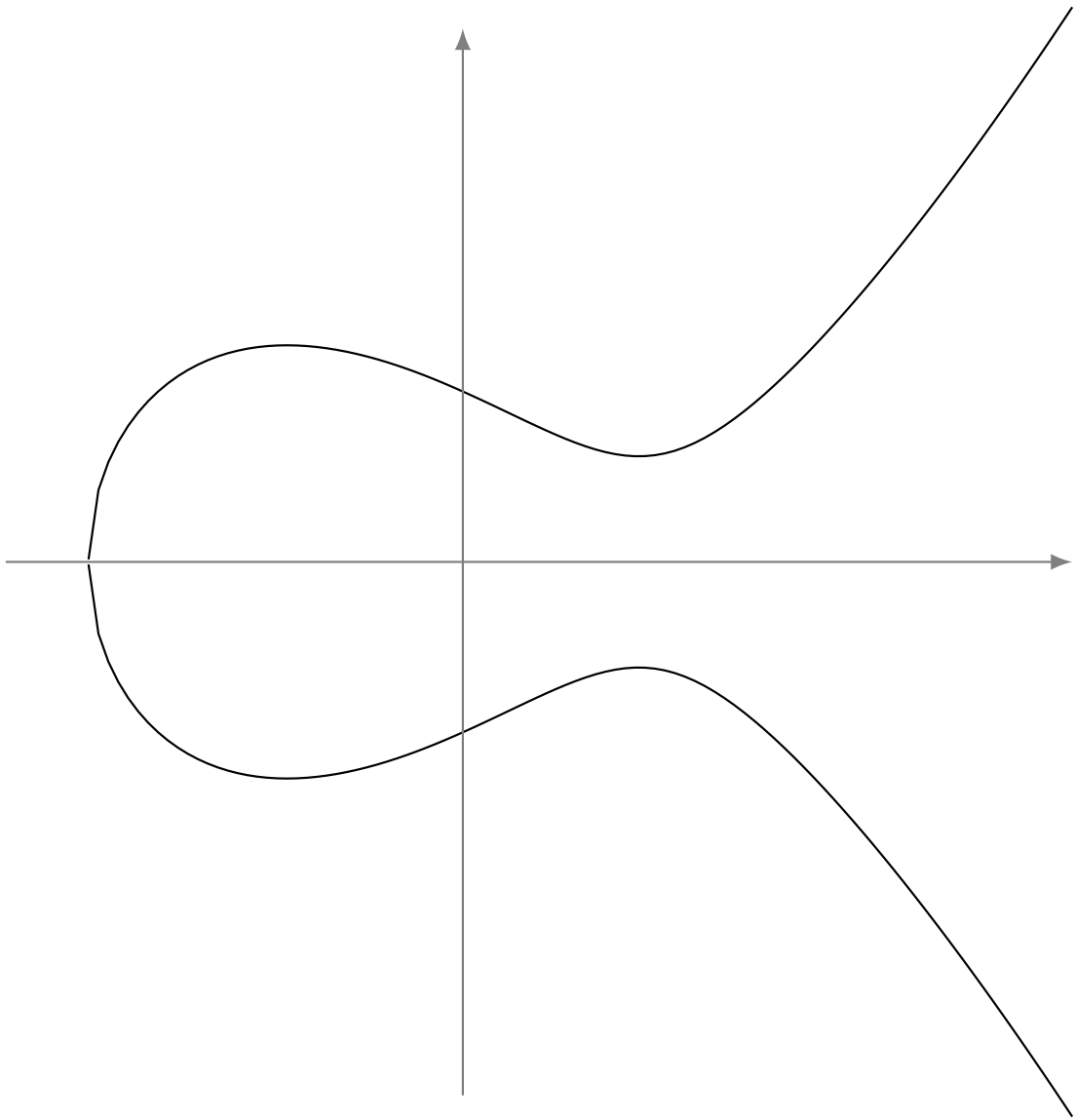
Weierstrass equations

Let k be a field of characteristic $\neq 2, 3$.
An elliptic curve *defined over* k is the locus in $\mathbb{P}^2(\bar{k})$ of an equation

$$Y^2Z = X^3 + aXZ^2 + bZ^3,$$

where $a, b \in k$ and $4a^3 + 27b^2 \neq 0$.

- $\mathcal{O} = (0 : 1 : 0)$ is the point at infinity;
- $y^2 = x^3 + ax + b$ is the affine equation.

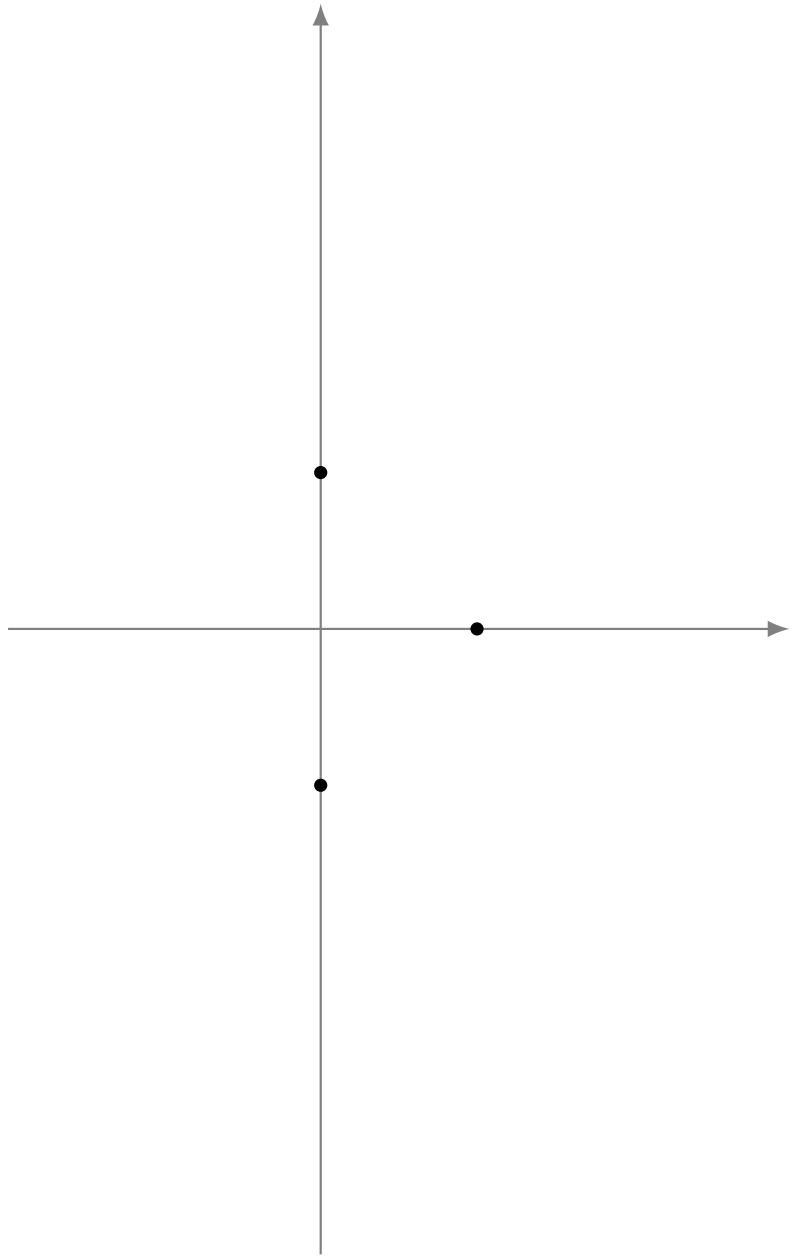


Attention: arithmetic geometry!

$$E \ : \ y^2 = x^3 - 2x + 1$$

Rational points:

- $E(\mathbb{Q}) = \{(1,0), (0,1), (0,-1), \mathcal{O}\}$,

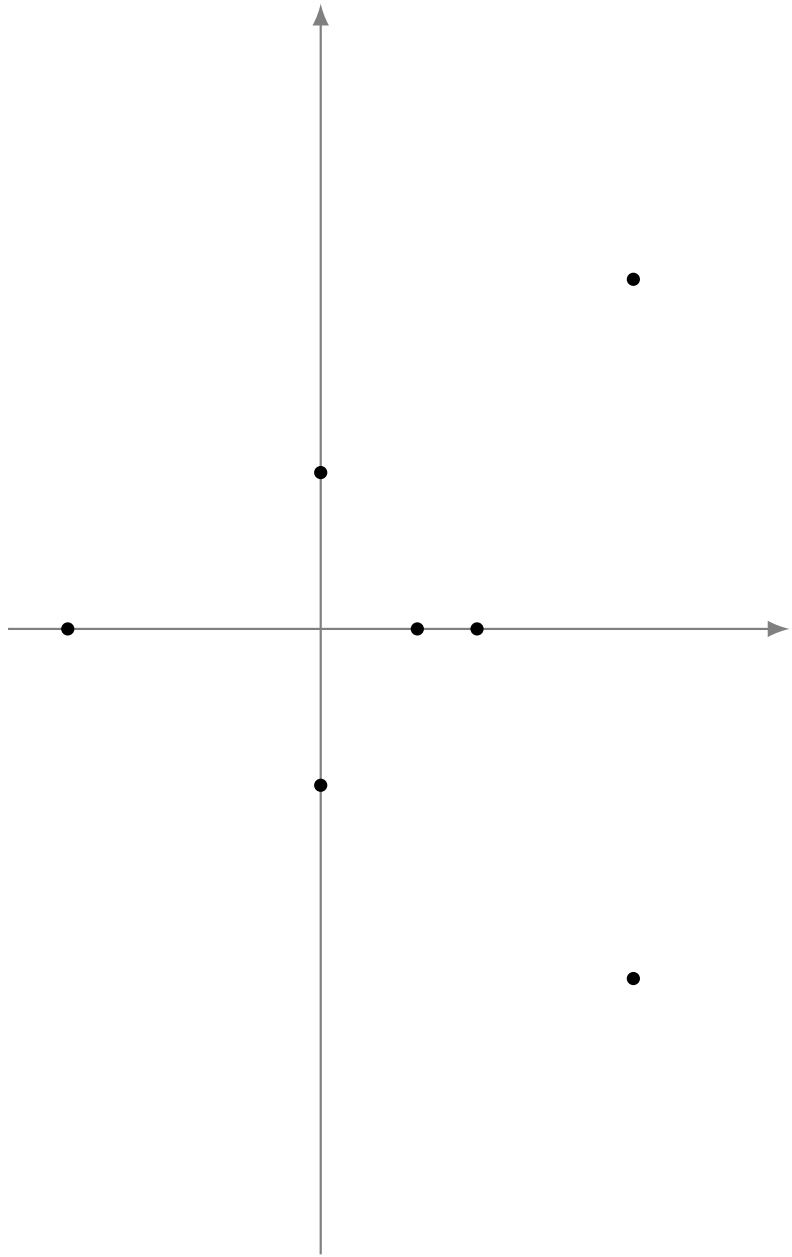


Attention: arithmetic geometry!

$$E \ : \ y^2 = x^3 - 2x + 1$$

Rational points:

- $E(\mathbb{Q}) = \{(1,0),(0,1),(0,-1),\mathcal{O}\}$,
- $\#E(\mathbb{Q}(\sqrt{5})) = 8$,

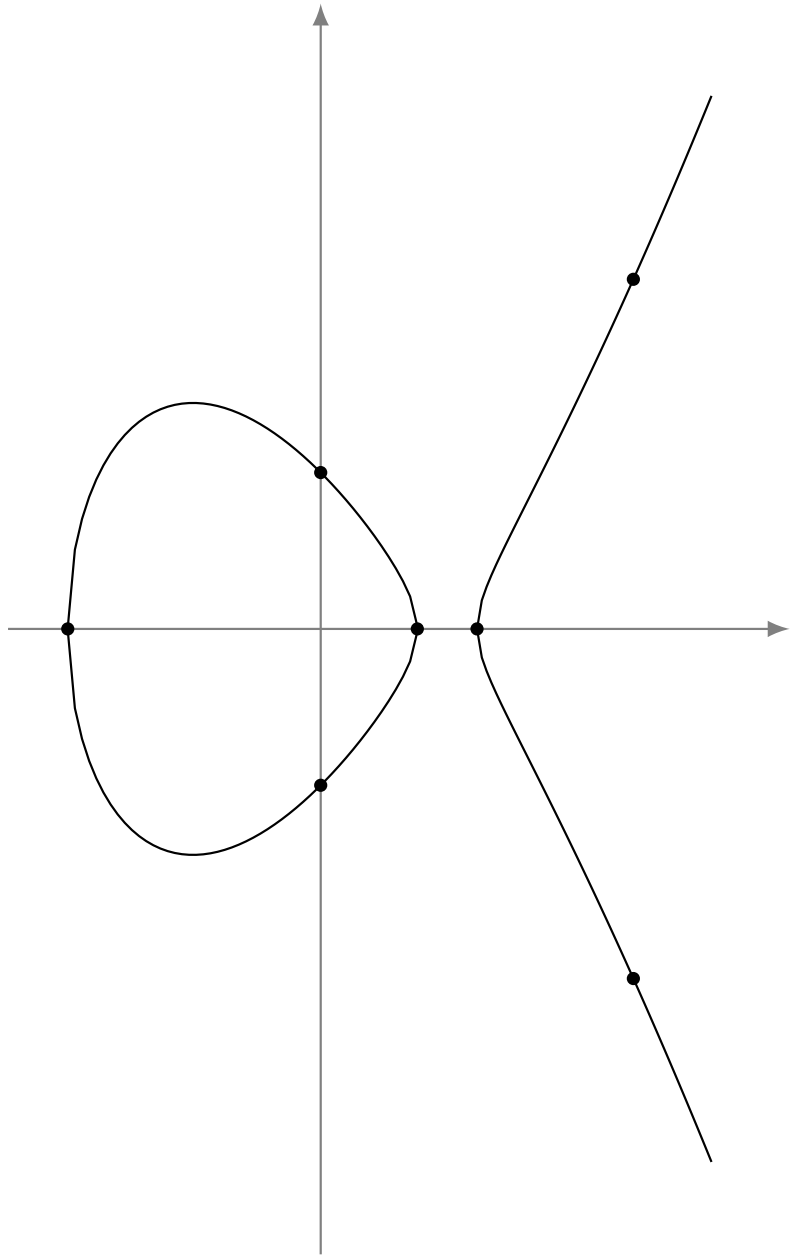


Attention: arithmetic geometry!

$$E \ : \ y^2 = x^3 - 2x + 1$$

Rational points:

- $E(\mathbb{Q}) = \{(1,0),(0,1),(0,-1),\mathcal{O}\}$,
- $\#E(\mathbb{Q}(\sqrt{5})) = 8$,
- ...
- $\#E(\mathbb{R}) = \infty$.

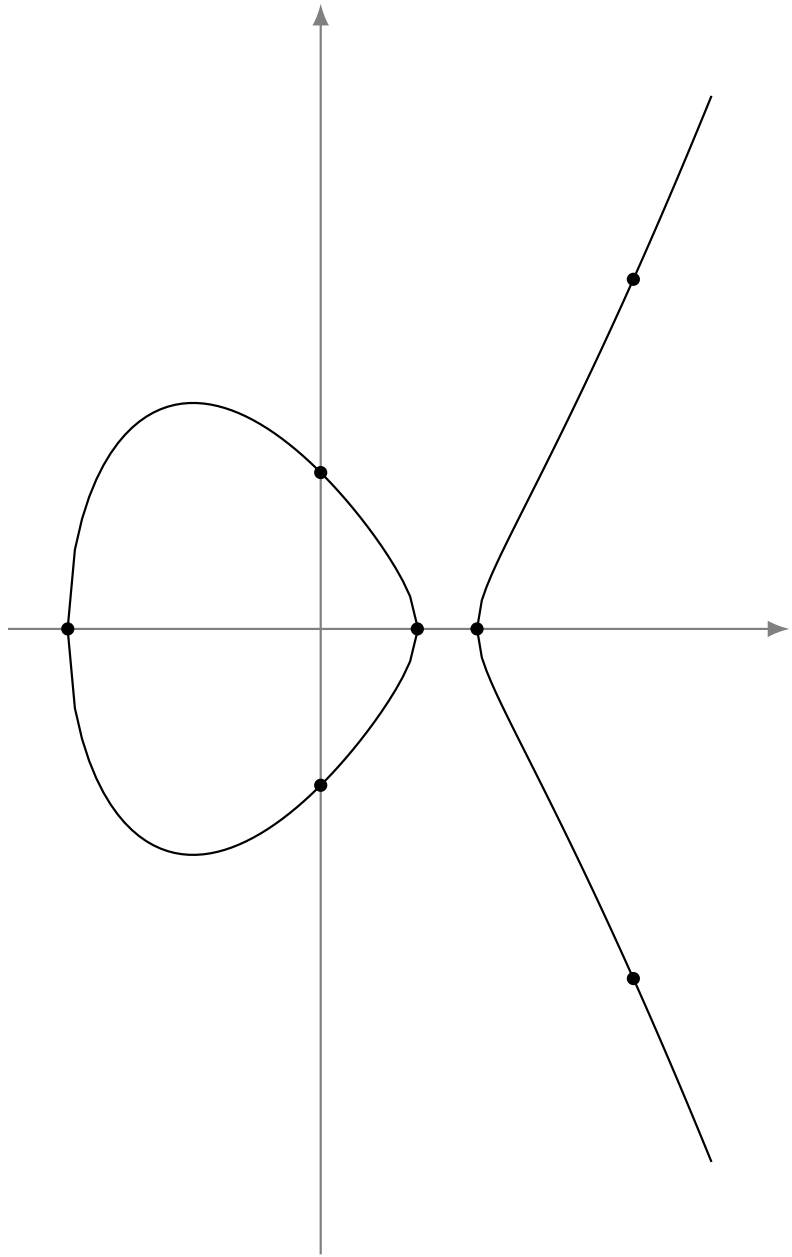


Attention: arithmetic geometry!

$$E \ : \ y^2 = x^3 - 2x + 1$$

Rational points:

- $E(\mathbb{Q}) = \{(1,0),(0,1),(0,-1),\mathcal{O}\}$,
- $\#E(\mathbb{Q}(\sqrt{5})) = 8$,
- ...
- $\#E(\mathbb{R}) = \infty$.
- $\#E(\mathbb{C}) = \infty$.

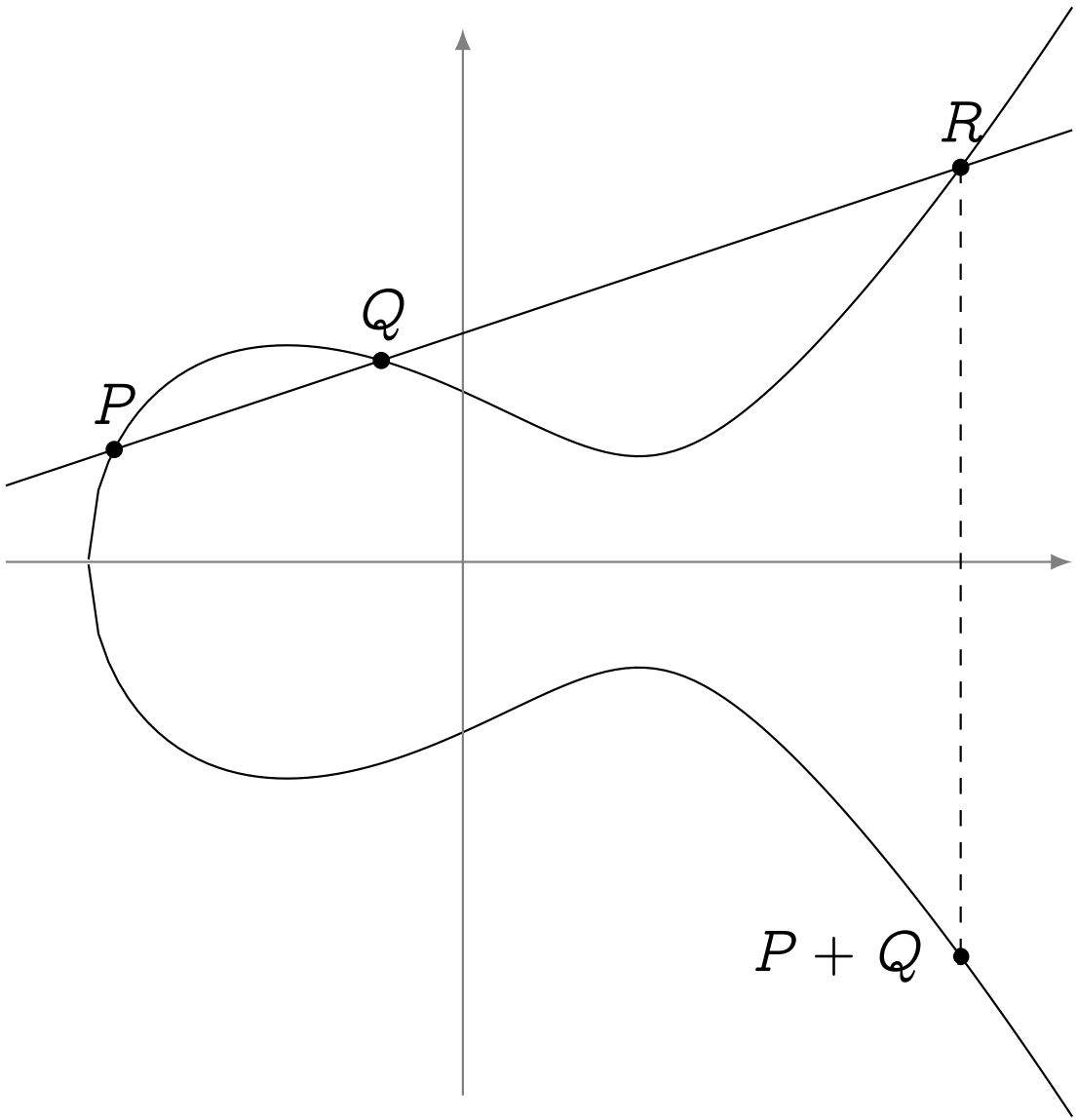


The group law

Bezout's theorem

Every line cuts E in exactly three points (counted with multiplicity).

Define a group law such that any three colinear points add up to zero.



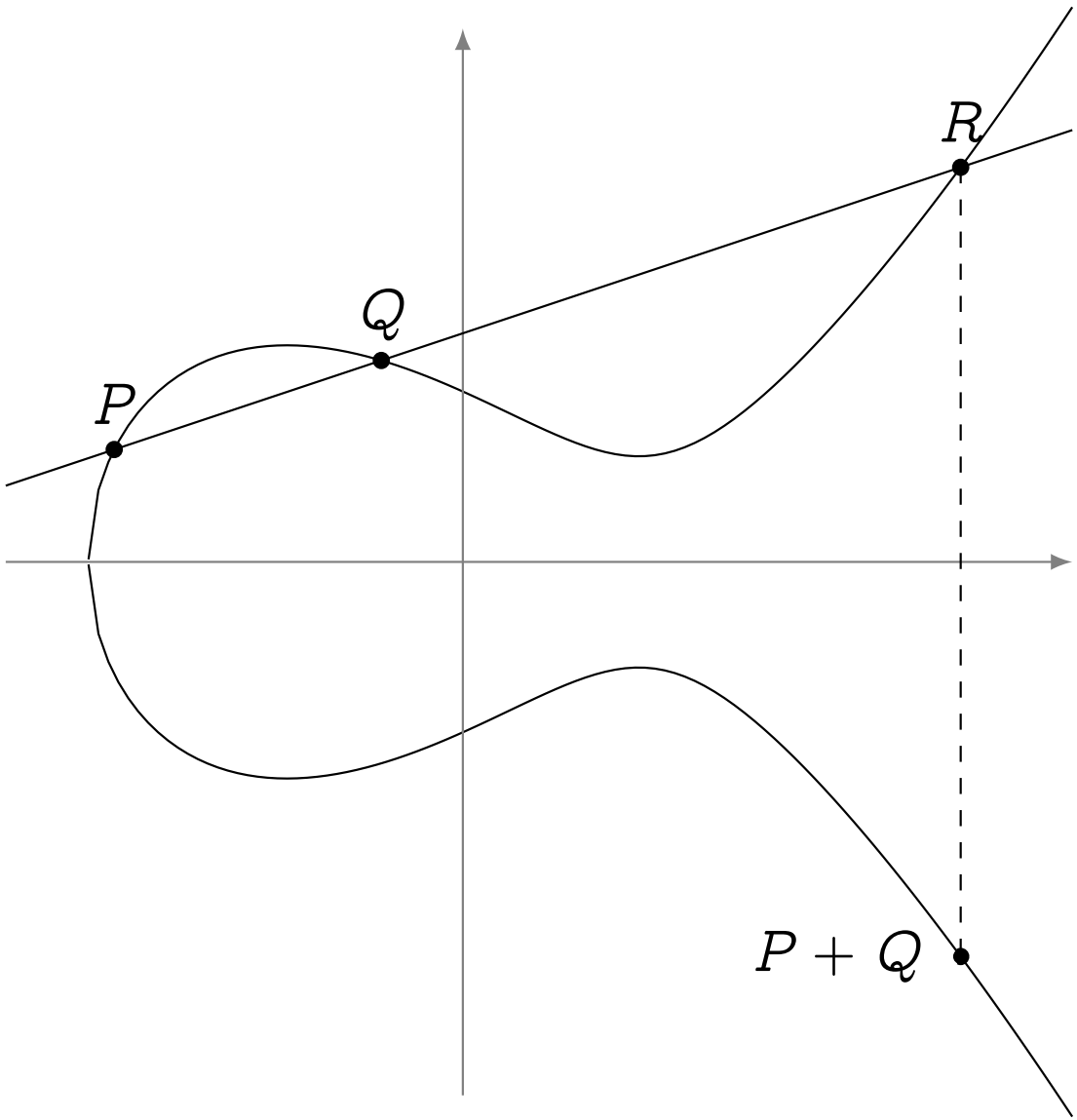
The group law

Bezout's theorem

Every line cuts E in exactly three points (counted with multiplicity).

Define a group law such that any three colinear points add up to zero.

- The law is algebraic (it has *formulas*);



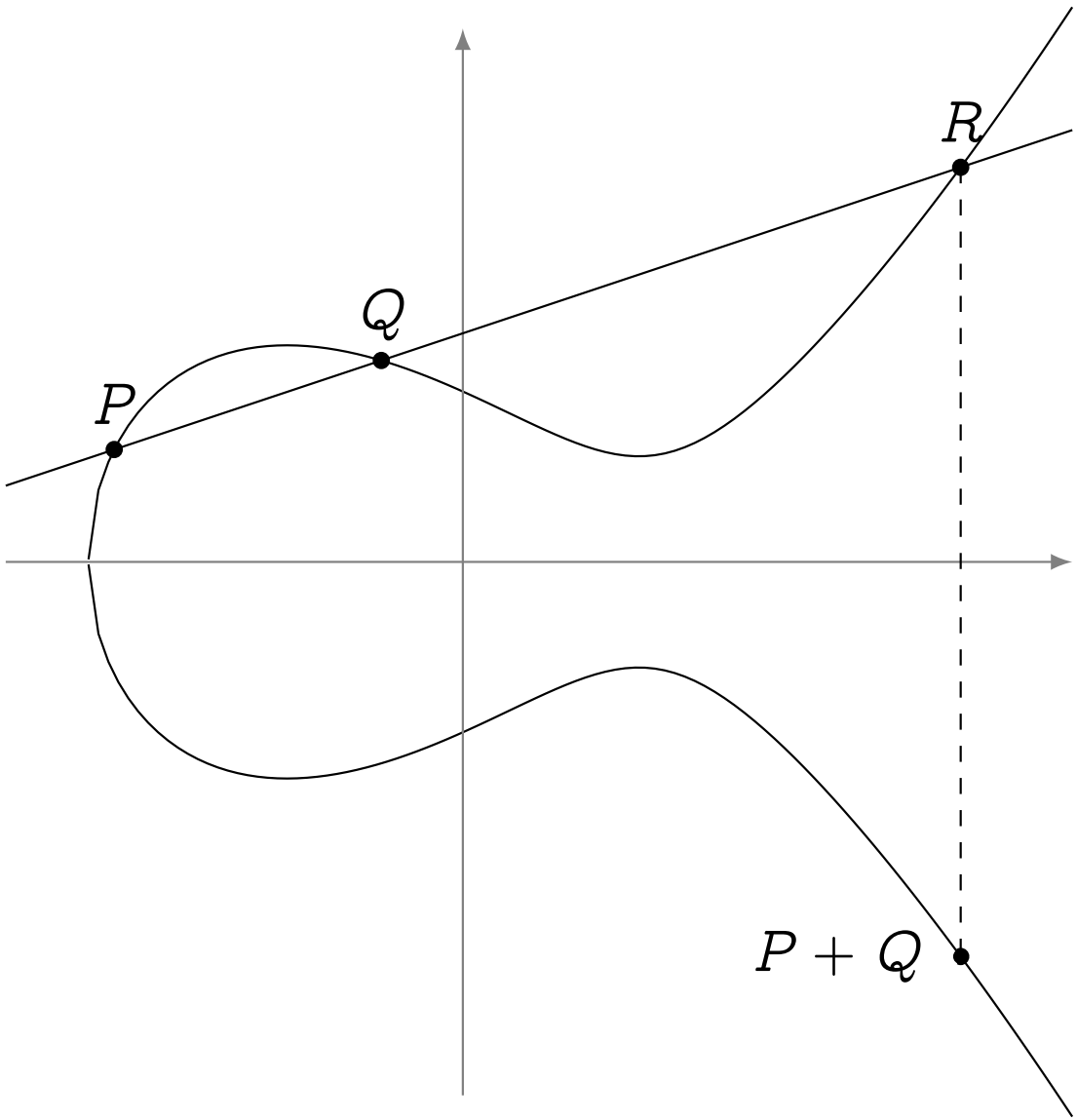
The group law

Bezout's theorem

Every line cuts E in exactly three points (counted with multiplicity).

Define a group law such that any three colinear points add up to zero.

- The law is algebraic (it has *formulas*);
- The law is commutative;
- $\mathcal{O}$ is the group identity;
- Opposite points have the same x-value.



What are elliptic curves?

For mathematicians

- The smooth projective curves of genus 1 (with a distinguished point);
- The simplest abelian varieties (dimension 1);
- Finitely generated abelian groups of mysterious free rank (aka BSD conjecture);
- What you use to make examples.

What are elliptic curves?

For mathematicians

- The smooth projective curves of genus 1 (with a distinguished point);
- The simplest abelian varieties (dimension 1);
- Finitely generated abelian groups of mysterious free rank (aka BSD conjecture);
- What you use to make examples.

For cryptographers

- Finite abelian groups (often cyclic);
- Easy to compute the order;
- "2-dimensional" generalizations of μ_k (the roots of unity of k)…
- …with bilinear maps (aka pairings)!

Maps: isomorphisms

Isomorphisms

The only invertible algebraic maps between elliptic curves are of the form

$$(x, y) \mapsto (u^2 x, u^3 y)$$

for some $u \in \bar{k}$.
They are group isomorphisms.

j-Invariant

Let $E : y^2 = x^3 + ax + b$, its j-invariant is

$$j(E) = 1728 \frac{4a^3}{4a^3 + 27b^2}.$$

Two elliptic curves E, E' are isomorphic if and only if $j(E) = j(E')$.

Group structure

Torsion structure

Let E be defined over an algebraically closed field $\bar{k}$ of characteristic p.

$$E[m] \simeq \quad \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \qquad \text{if } p \nmid m,$$

$$E[p^e] \simeq \begin{cases} \mathbb{Z}/p^e\mathbb{Z} & \text{ordinary case,} \\ \{\mathcal{O}\} & \text{supersingular case.} \end{cases}$$

Finite fields (Hasse's theorem)

Let E be defined over a finite field $\mathbb{F}_q$, then

$$|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}.$$

In particular, there exist integers n_1 and $n_2 | \gcd(n_1, q-1)$ such that

$$E(\mathbb{F}_q) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}.$$

Maps: what's scalar multiplication?

$$[n] \ : \ P \mapsto \underbrace{P + P + \cdots + P}_{n \text{ times}}$$

- A map $E \to E$,
- a group morphism,
- with finite kernel
  (the torsion group $E[n] \simeq (\mathbb{Z}/n\mathbb{Z})^2$),
- surjective (in the algebraic closure),
- given by rational maps of degree n^2.

Maps: what's ~~scalar multiplication~~ an isogeny?

$$[n] \; : \; P \mapsto \underbrace{P + P + \cdots + P}_{n \text{ times}}$$

- A map $E \to E$,
- a group morphism,
- with finite kernel
  (the torsion group $E[n] \simeq (\mathbb{Z}/n\mathbb{Z})^2$),
- surjective (in the algebraic closure),
- given by rational maps of degree n^2.

Maps: what's ~~scalar multiplication~~ an isogeny?

$$\phi \ : \ P \mapsto \phi(P)$$

- A map $E \to E$,
- a group morphism,
- with finite kernel
  (the torsion group $E[n] \simeq (\mathbb{Z}/n\mathbb{Z})^2$),
- surjective (in the algebraic closure),
- given by rational maps of degree n^2.

Maps: what's ~~scalar multiplication~~ an isogeny?

$$\phi \ : \ P \mapsto \phi(P)$$

- A map $E \to E'$,
- a group morphism,
- with finite kernel
  (the torsion group $E[n] \simeq (\mathbb{Z}/n\mathbb{Z})^2$),
- surjective (in the algebraic closure),
- given by rational maps of degree n^2.

Maps: what's scalar multiplication an isogeny?

$$\phi \ : \ P \mapsto \phi(P)$$

- A map $E \to E'$,
- a group morphism,
- with finite kernel (the torsion group $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$ any finite subgroup $H \subset E$),
- surjective (in the algebraic closure),
- given by rational maps of degree n^2.

Maps: what's scalar multiplication an isogeny?

$$\phi \ : \ P \mapsto \phi(P)$$

- A map $E \to E'$,
- a group morphism,
- with finite kernel (the torsion group $E[m] \simeq (\mathbb{Z}/m\mathbb{Z})^2$ any finite subgroup $H \subset E$),
- surjective (in the algebraic closure),
- given by rational maps of degree m^2 $\#H$.

Maps: what's scalar multiplication an isogeny?

$$\phi \ : \ P \mapsto \phi(P)$$

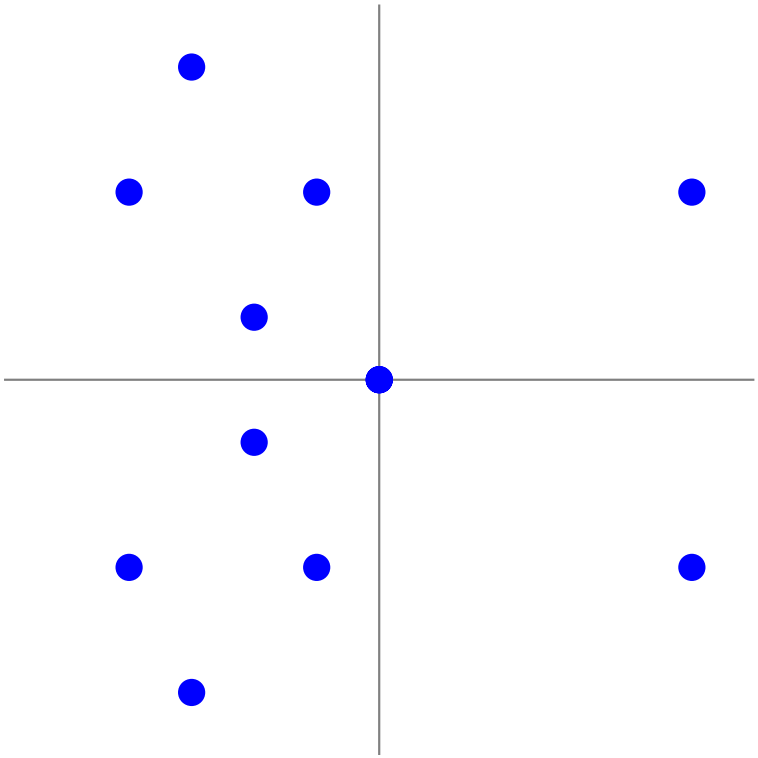
- A map $E \to E'$,
- a group morphism,
- with finite kernel (the torsion group $E[m] \simeq (\mathbb{Z}/m\mathbb{Z})^2$ any finite subgroup $H \subset E$),
- surjective (in the algebraic closure),
- given by rational maps of degree m^2 $\#H$.

(Separable) isogenies $\Leftrightarrow$ finite subgroups:

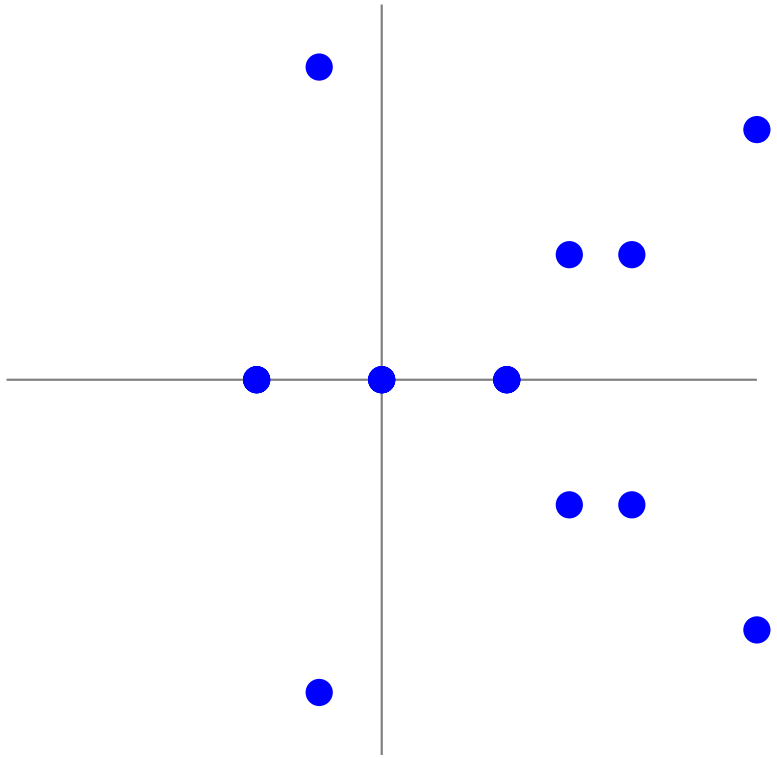
$$0 \to H \to E \xrightarrow{\phi} E' \to 0$$

Isogenies: an example over $\mathbb{F}_{11}$

$$E \ : \ y^2 = x^3 + x$$



$$E' \ : \ y^2 = x^3 - 4x$$

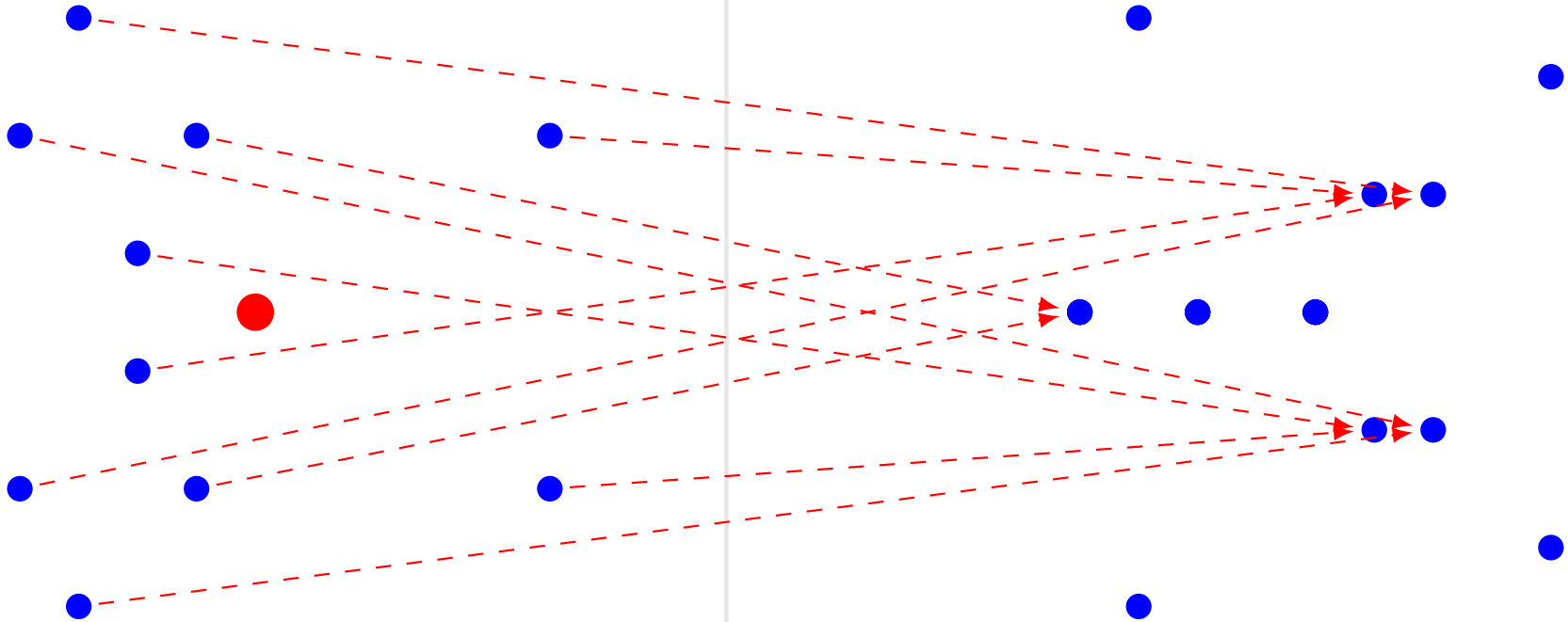


$$\phi(x, y) = \left(\frac{x^2 + 1}{x}, \quad y \frac{x^2 - 1}{x^2} \right)$$

Isogenies: an example over $\mathbb{F}_{11}$

$E : y^2 = x^3 + x$

$E' : y^2 = x^3 - 4x$



$$\phi(x, y) = \left(\frac{x^2 + 1}{x}, \quad y \frac{x^2 - 1}{x^2} \right)$$

- Kernel generator in red.
- This is a degree 2 map.
- Analogous to $x \mapsto x^2$ in $\mathbb{F}_q^*$.

Maps: isogenies

Theorem

Let $\phi : E \to E'$ be a map between elliptic curves. These conditions are equivalent:

- *ϕ is a surjective group morphism,*
- *ϕ is a group morphism with finite kernel,*
- *ϕ is a non-constant algebraic map of projective varieties sending the point at infinity of E onto the point at infinity of E'.*

If they hold ϕ is called an isogeny.

Two curves are called isogenous if there exists an isogeny between them.

Example: Multiplication-by-m

On any curve, an isogeny from E to itself (i.e., an endomorphism):

$$\begin{aligned} [m] \ : \ & E \to E, \\ & P \mapsto [m]P. \end{aligned}$$

Isogeny lexicon

Degree

- $\approx$ degree of the rational fractions defining the isogeny;
- Rough measure of the information needed to encode it.

Separable, inseparable, cyclic

An isogeny ϕ is separable iff $\deg \phi = \# \ker \phi$.

- Given $H \subset E$ finite, write $\phi : E \to E/H$ for the unique separable isogeny s.t. $\ker \phi = H$.
- ϕ inseparable $\Rightarrow p$ divides $\deg \phi$.
- Cyclic isogeny $\equiv$ separable isogeny with cyclic kernel.
  - Non-example: the multiplication map $[m] : E \to E$.

Rationality

Given E defined over k, an isogeny ϕ is rational if $\ker \phi$ is Galois invariant.

$\Rightarrow$ ϕ is represented by rational fractions with coefficients in k.

The dual isogeny

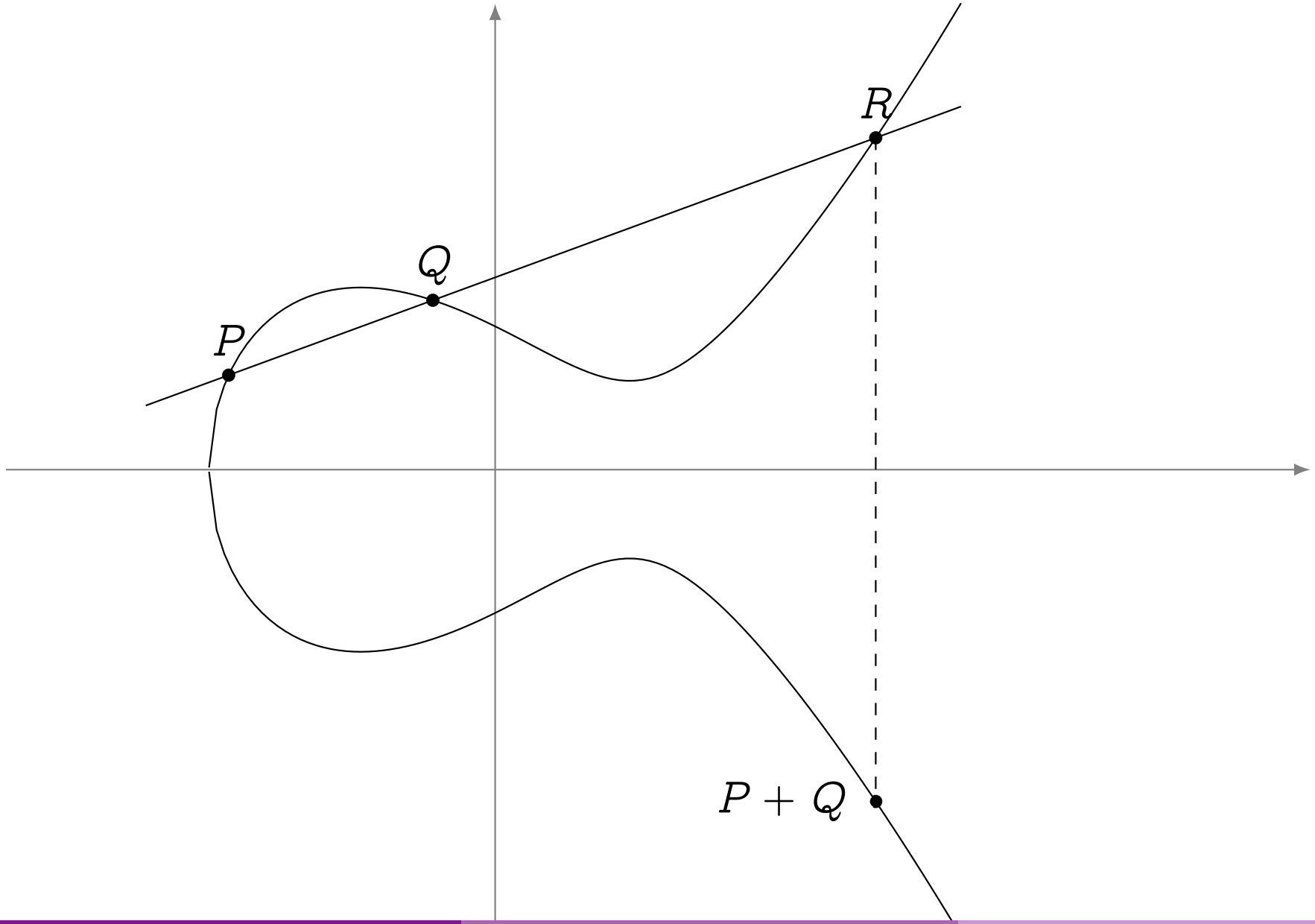
Let $\phi : E \to E'$ be an isogeny of degree m. There is a unique isogeny $\hat{\phi} : E' \to E$ such that

$$\hat{\phi} \circ \phi = [m]_E, \quad \phi \circ \hat{\phi} = [m]_{E'}.$$

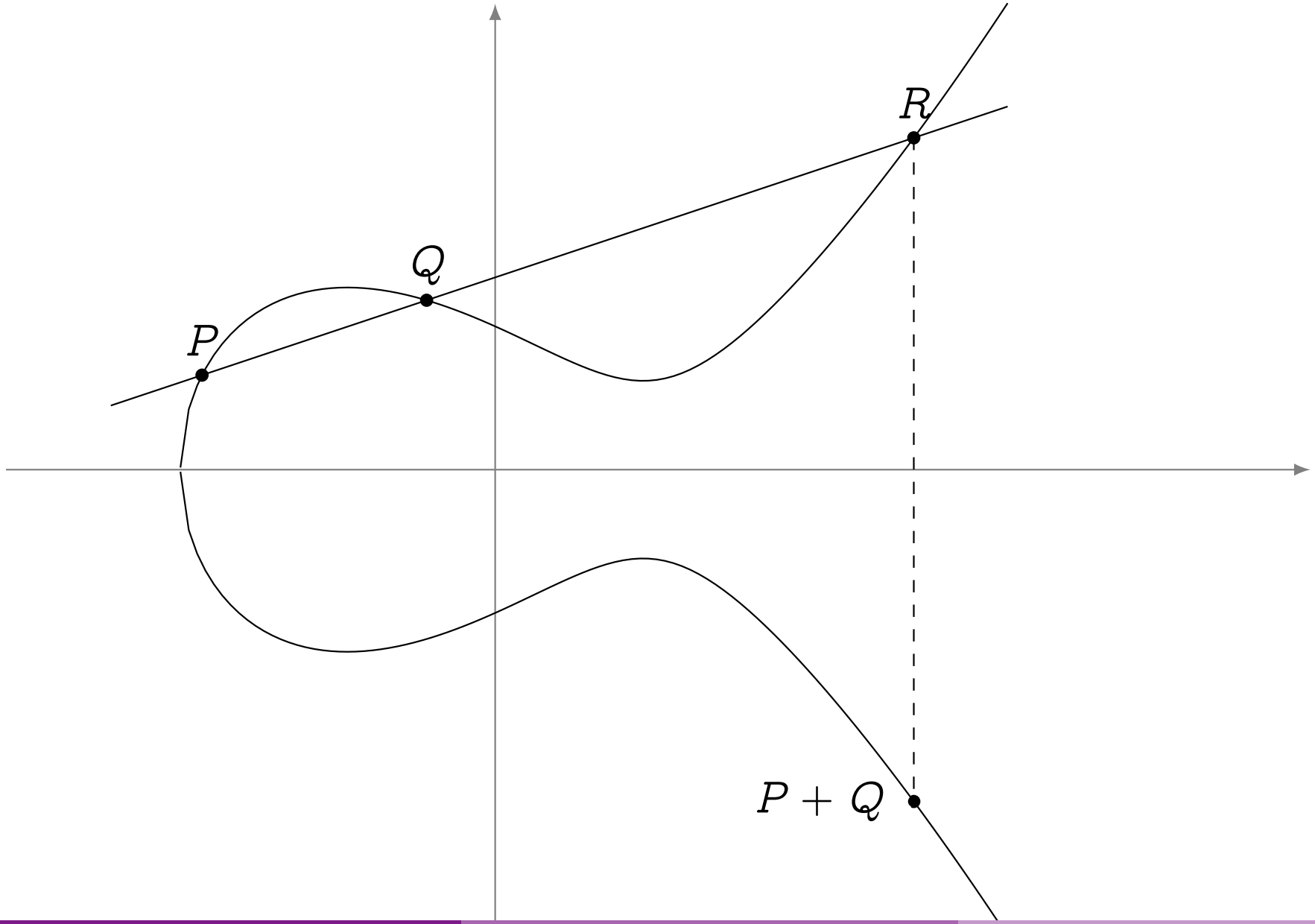
$\hat{\phi}$ is called the dual isogeny of ϕ; it has the following properties:

1. $\hat{\phi}$ is defined over k if and only if ϕ is;
2. $\widehat{\psi \circ \phi} = \hat{\phi} \circ \hat{\psi}$ for any isogeny $\psi : E' \to E''$;
3. $\widehat{\psi + \phi} = \hat{\psi} + \hat{\phi}$ for any isogeny $\psi : E \to E'$;
4. $\deg \phi = \deg \hat{\phi}$;
5. $\hat{\hat{\phi}} = \phi$.

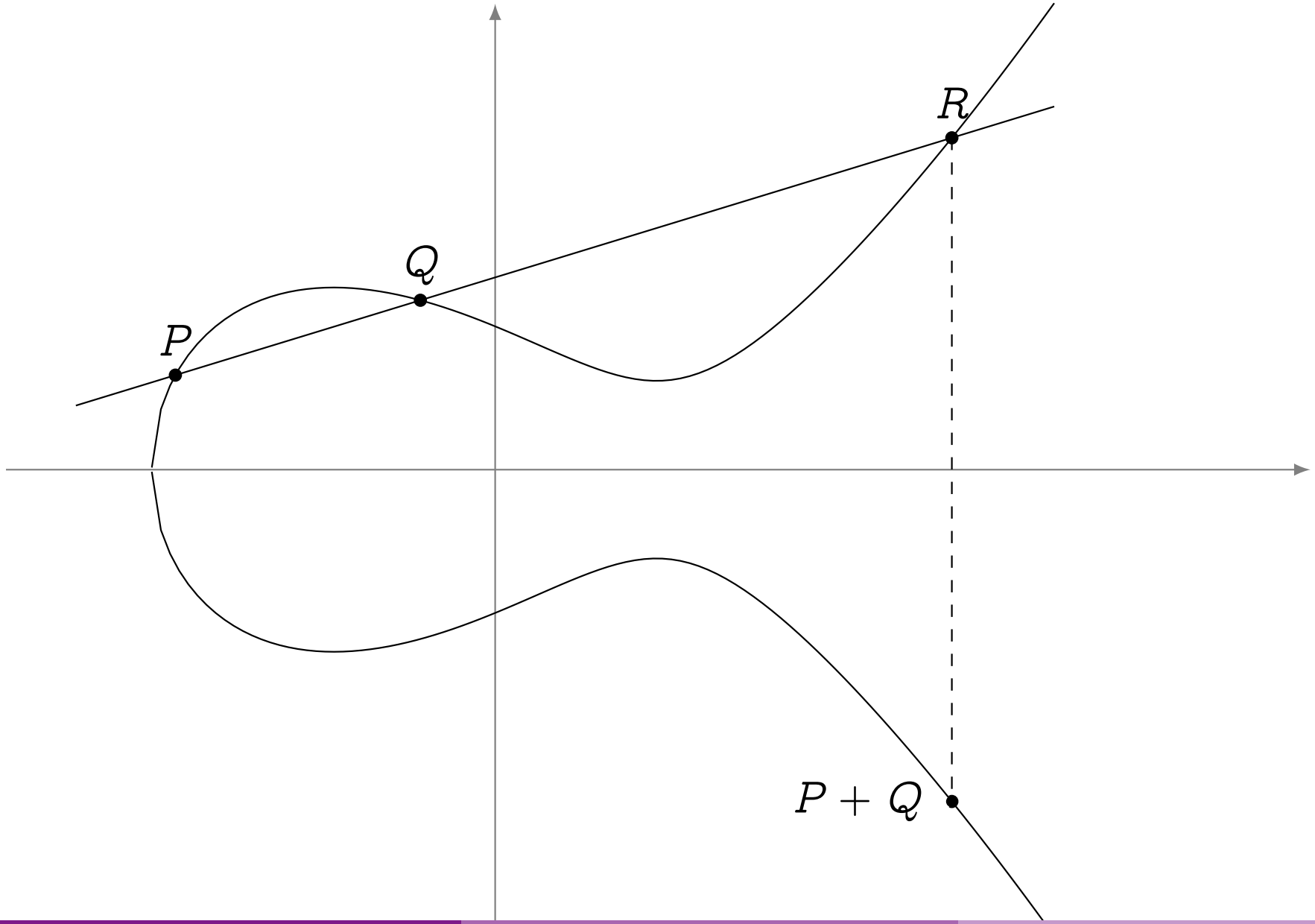
Up to isomorphism



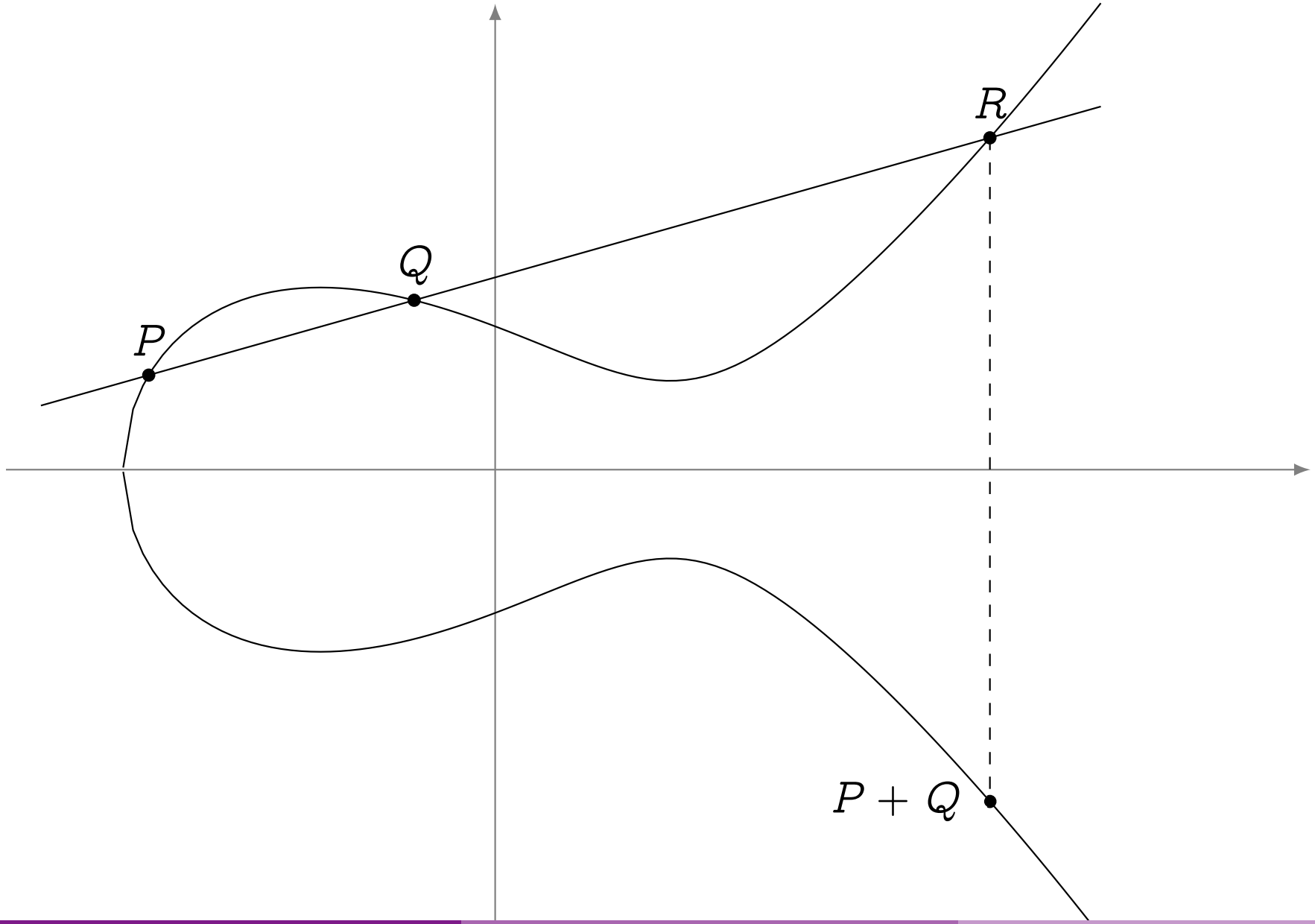
Up to isomorphism



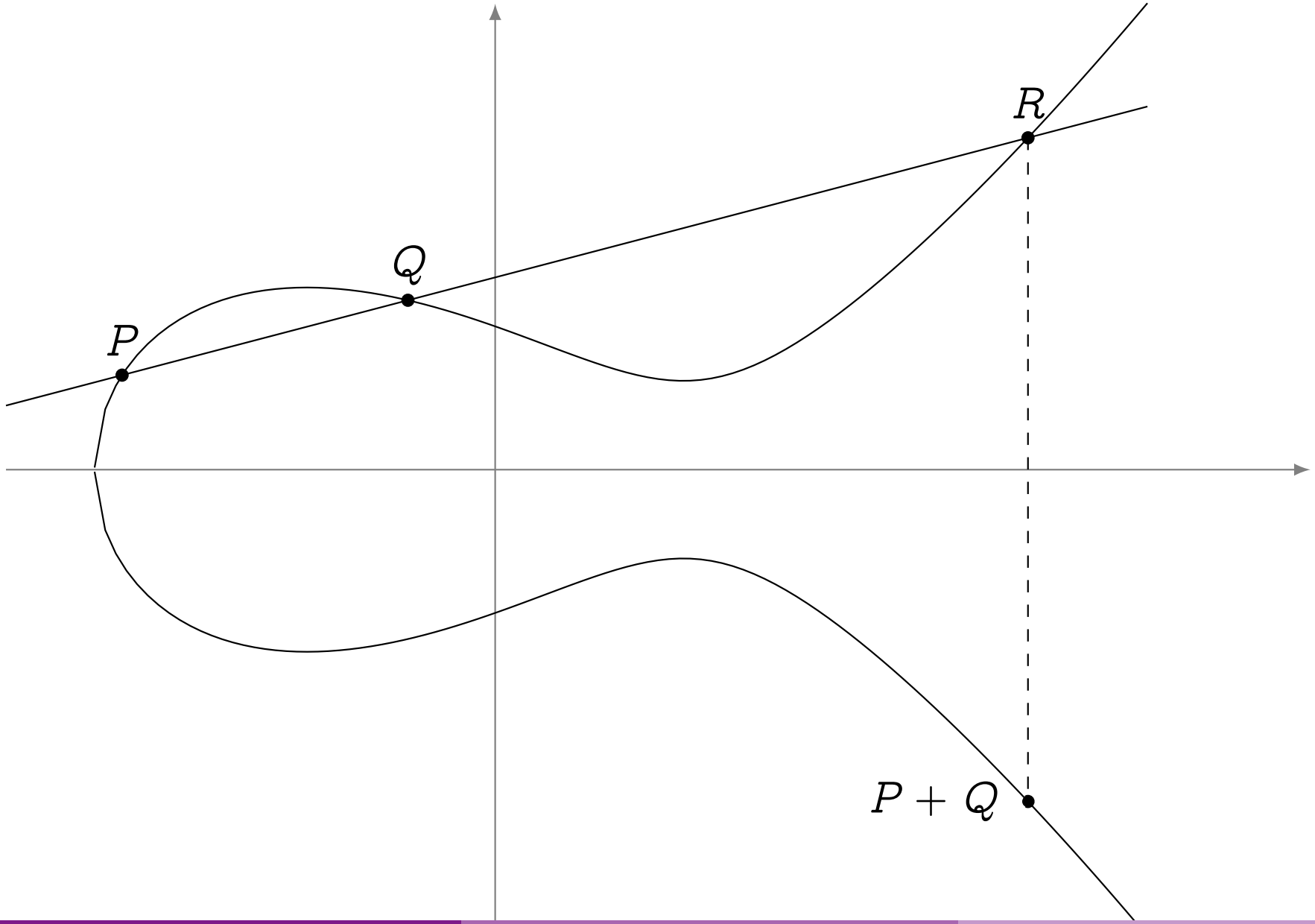
Up to isomorphism



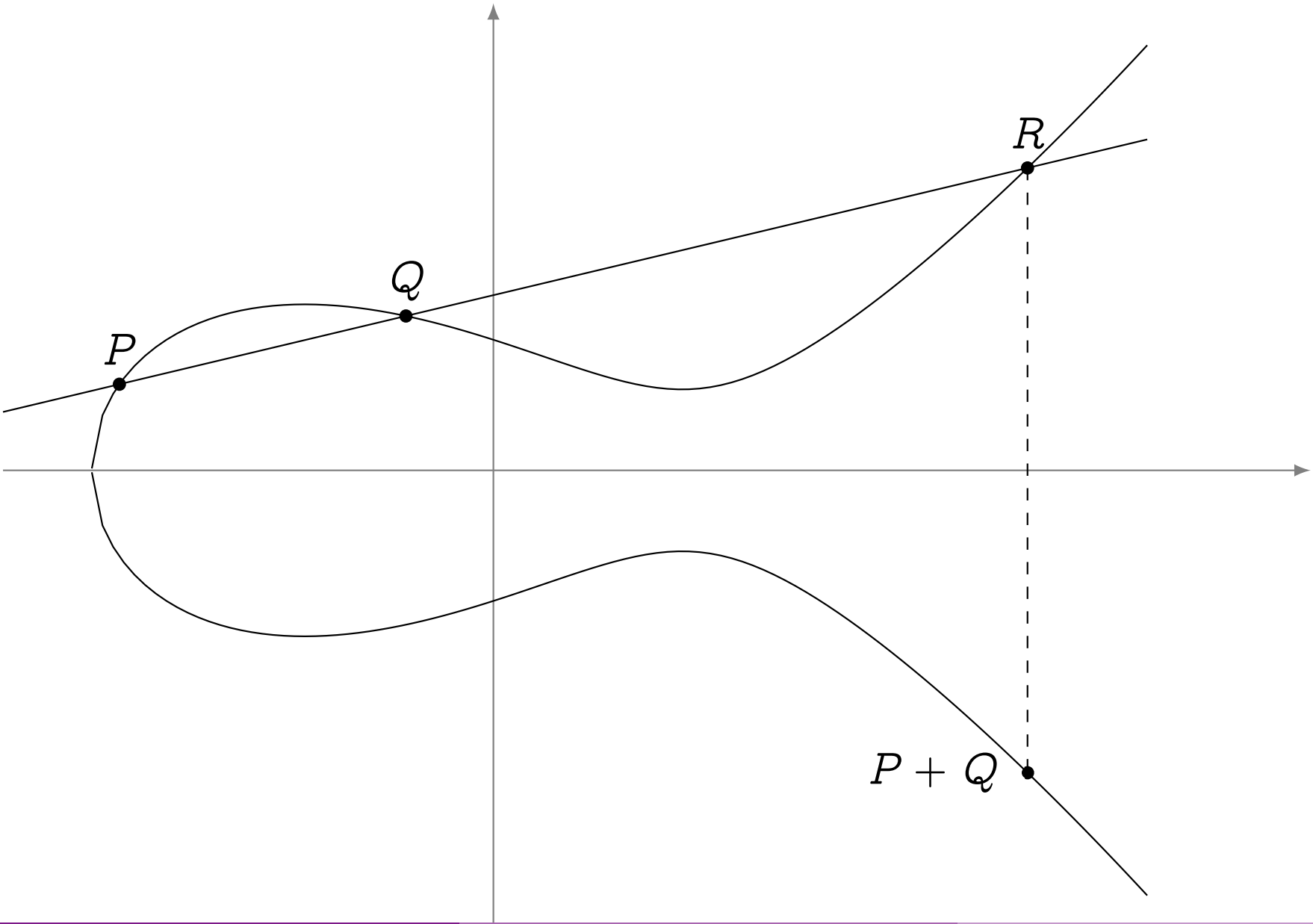
Up to isomorphism



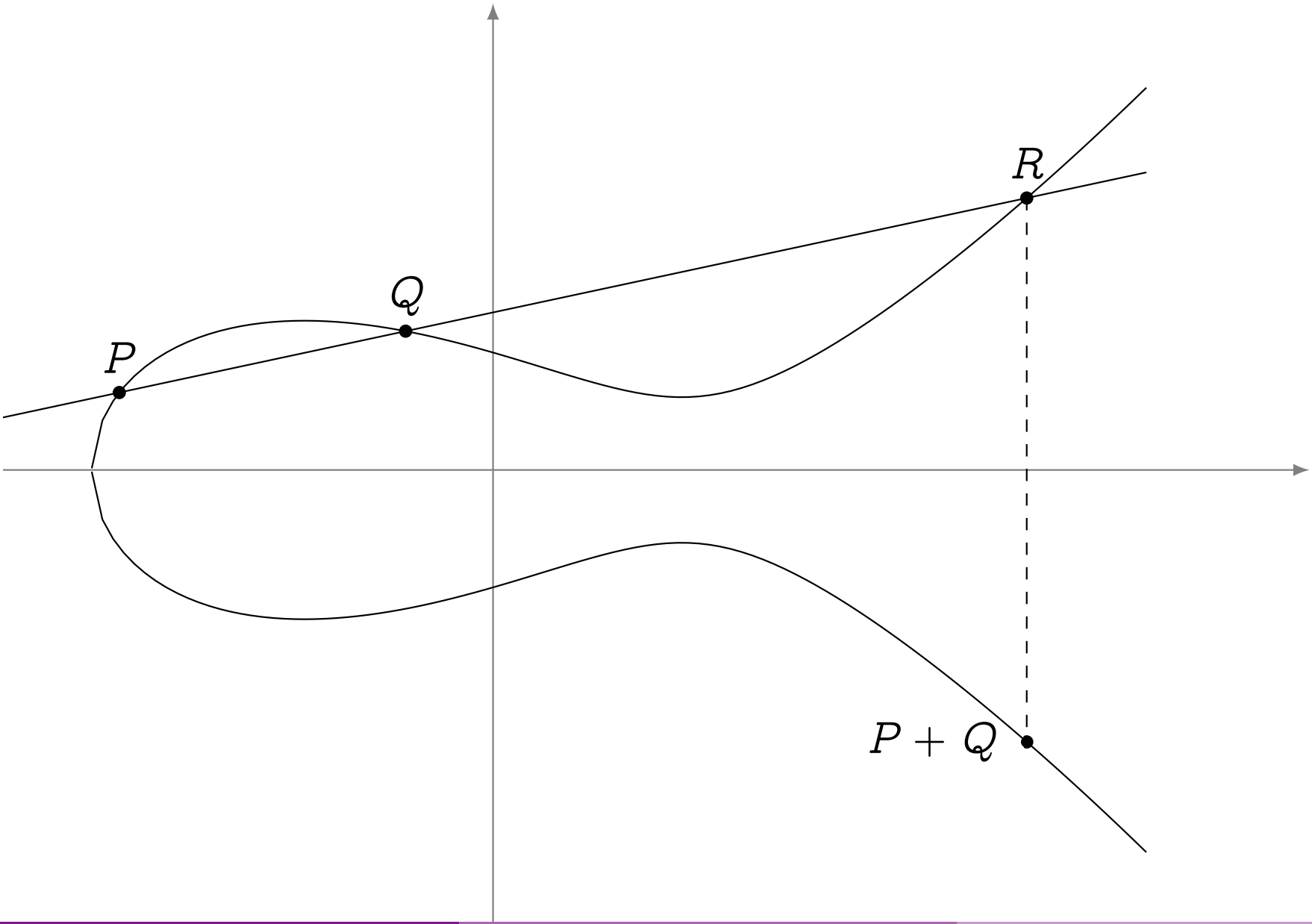
Up to isomorphism



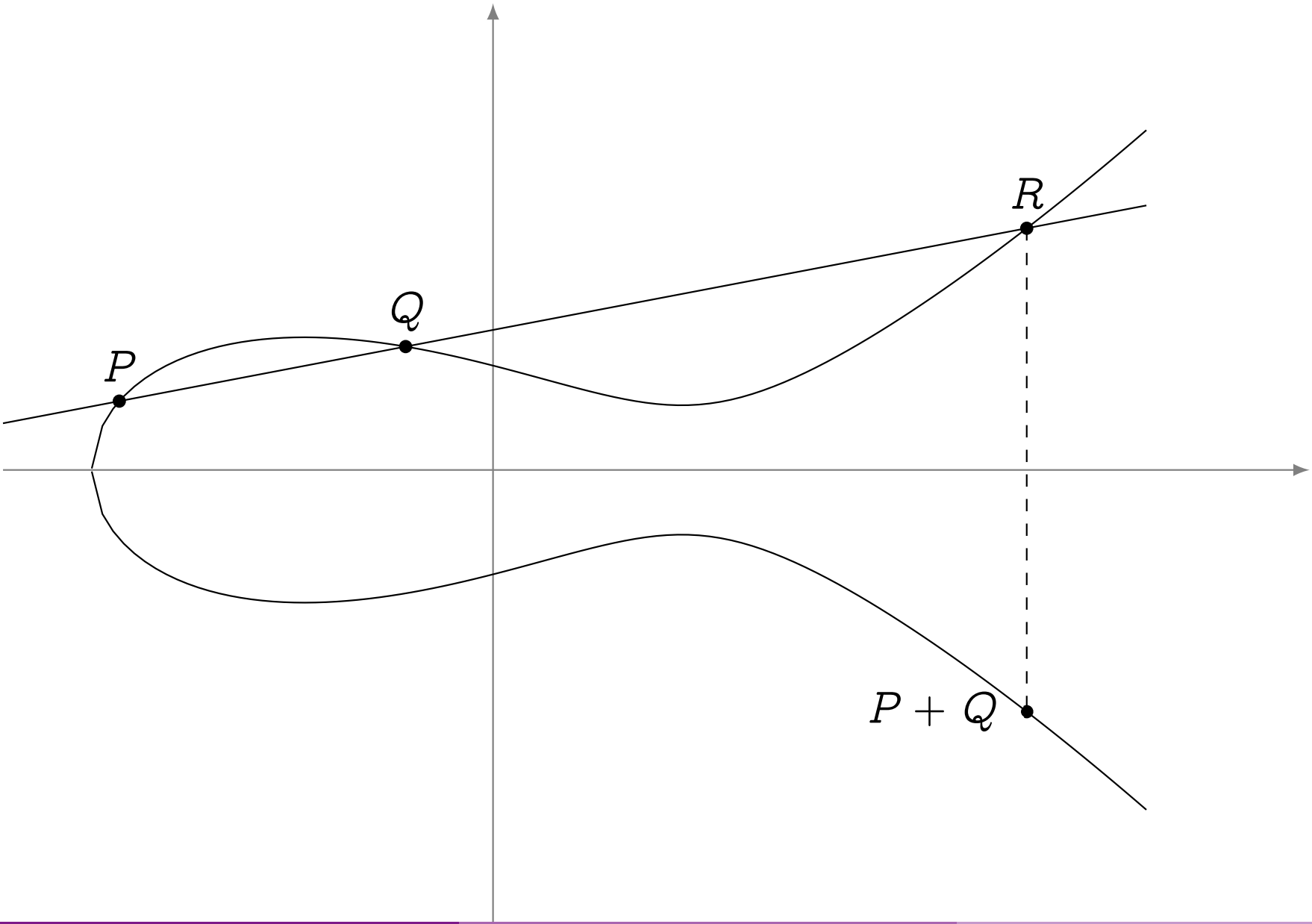
Up to isomorphism



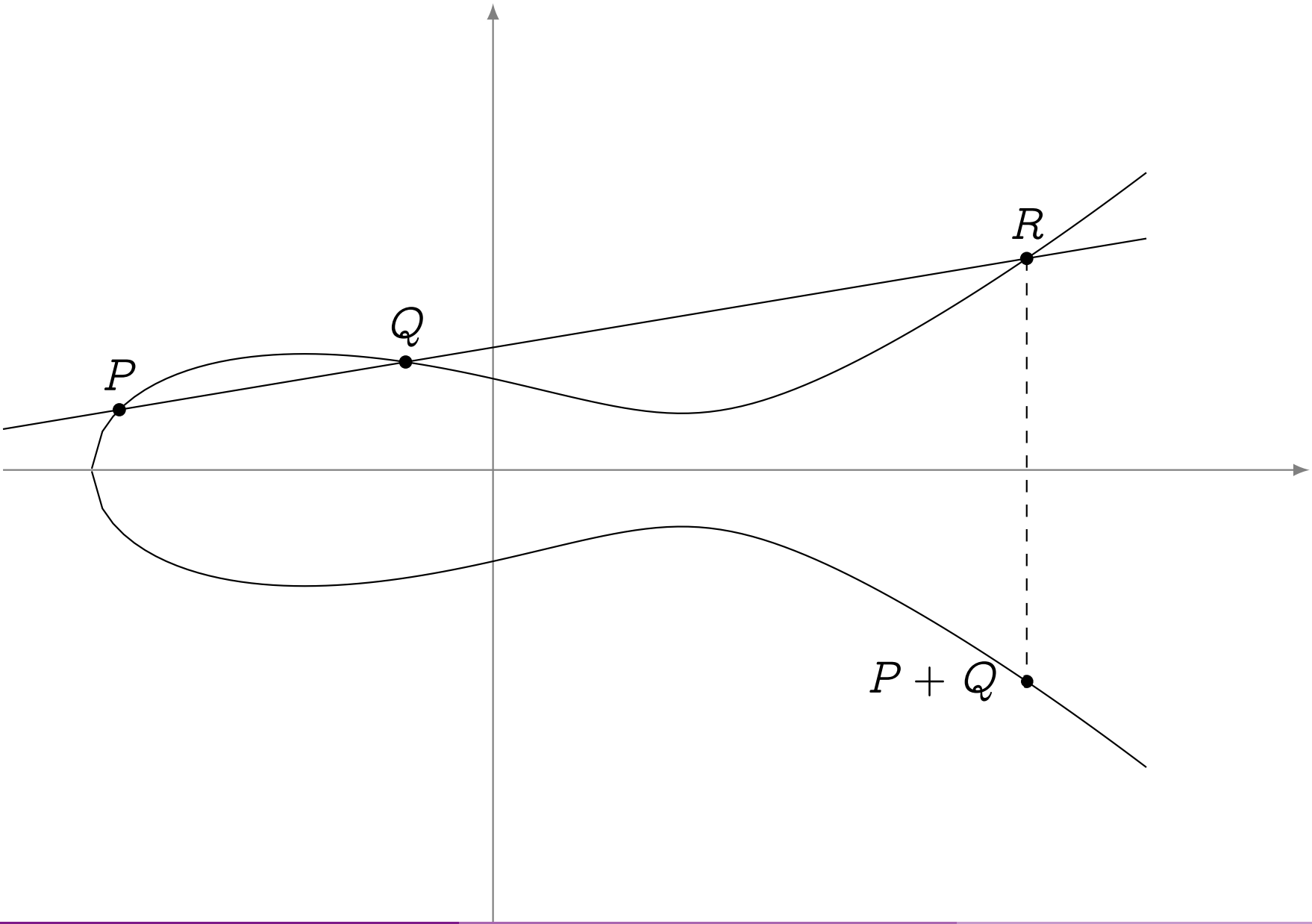
Up to isomorphism



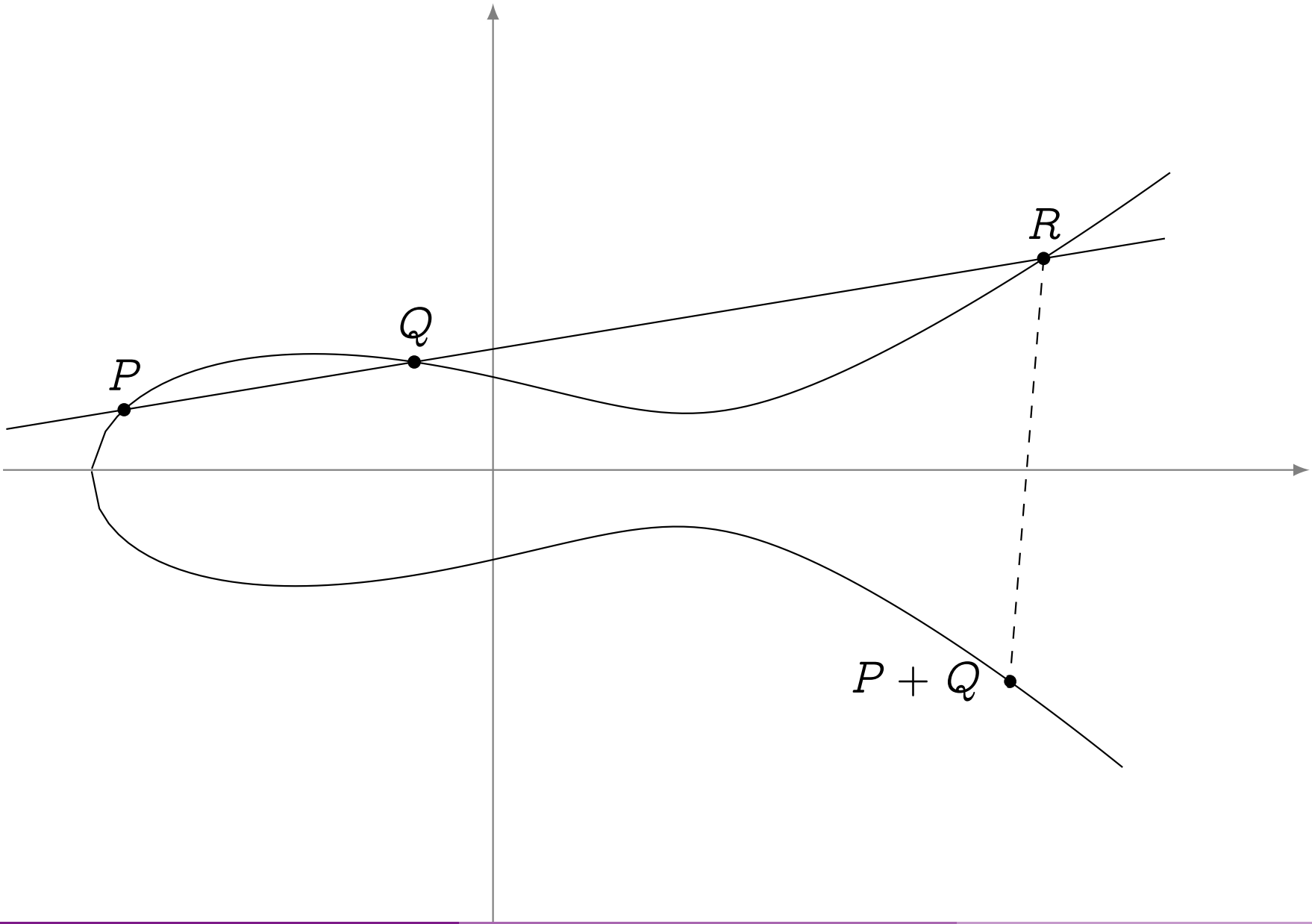
Up to isomorphism



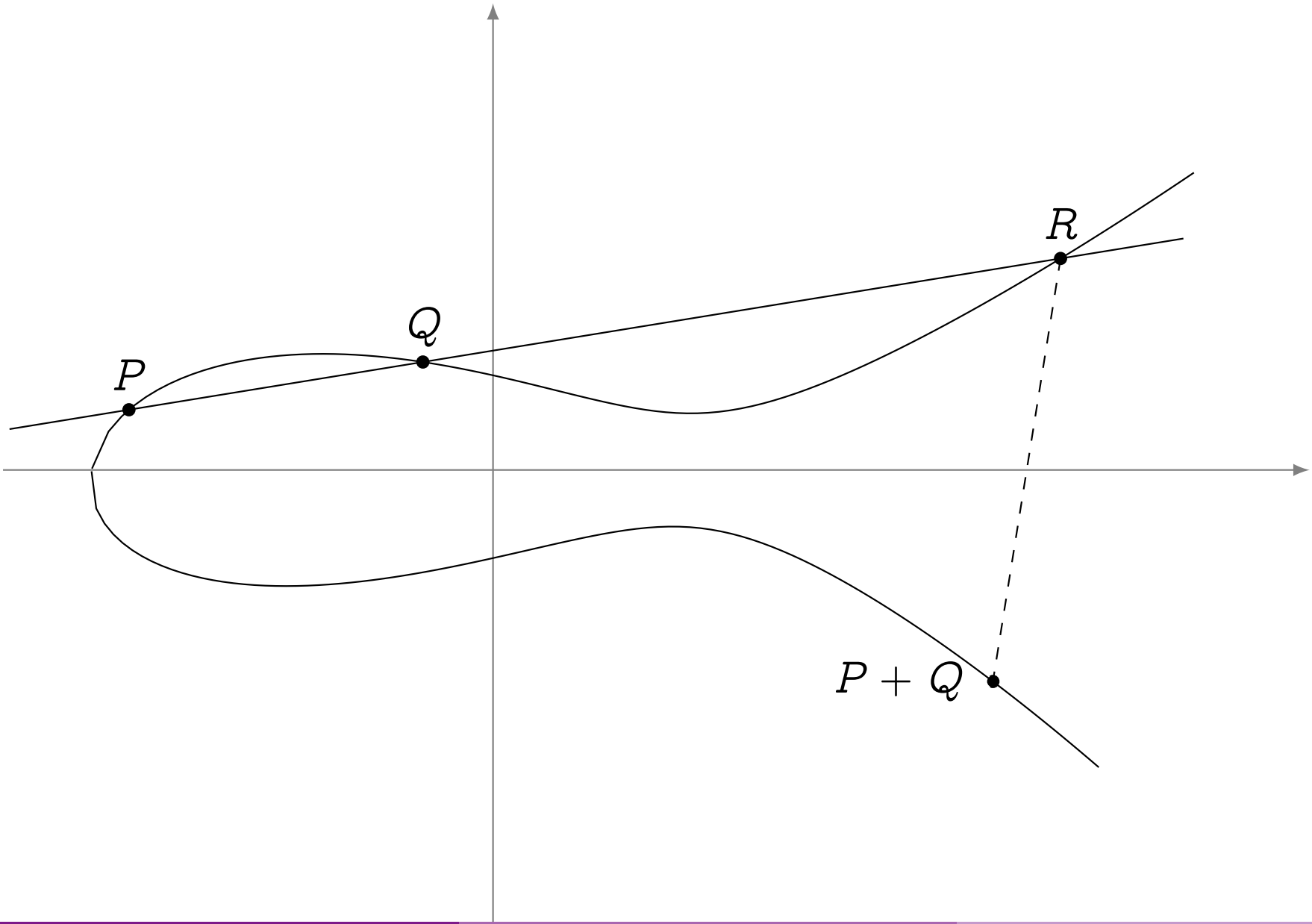
Up to isomorphism



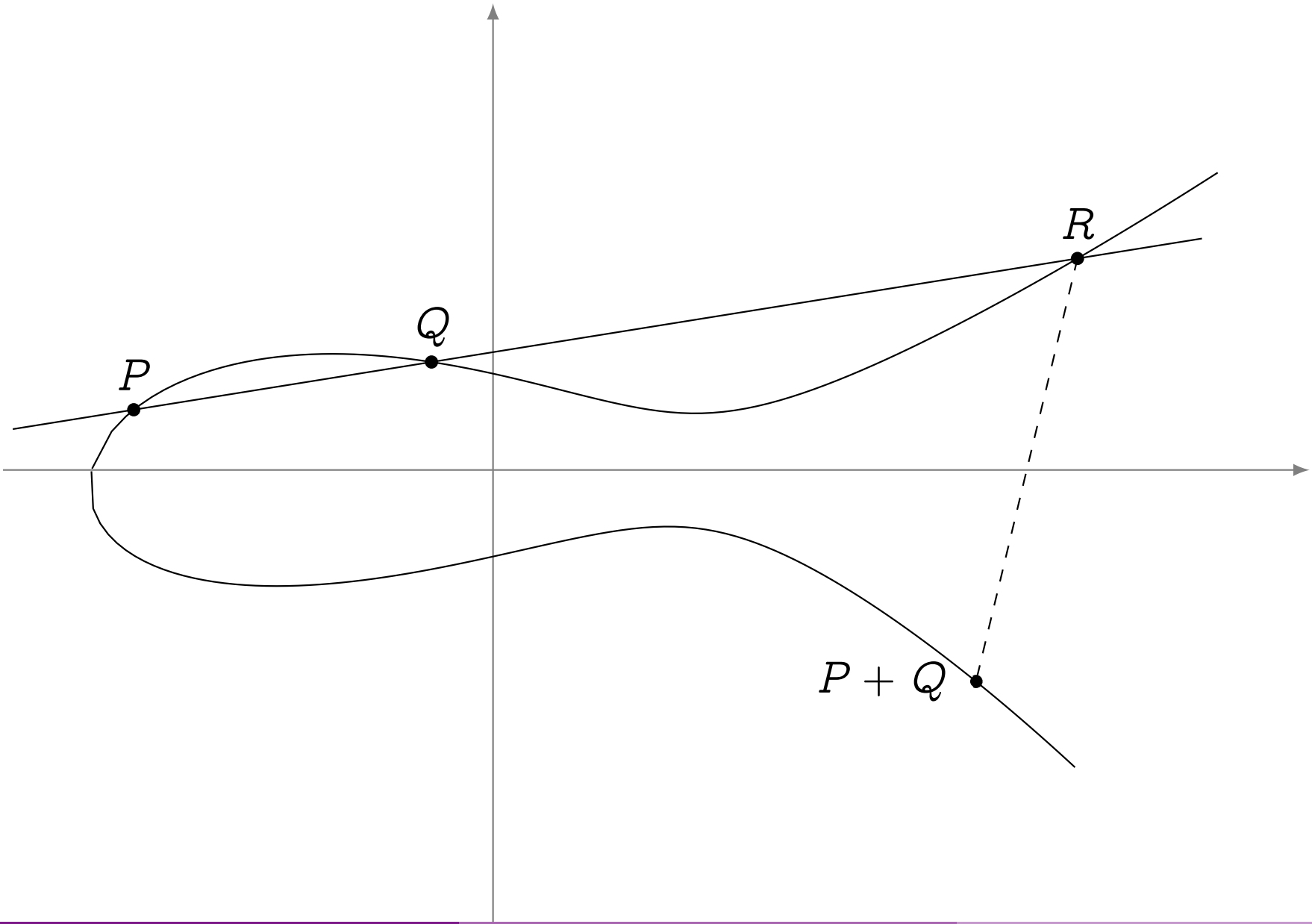
Up to isomorphism



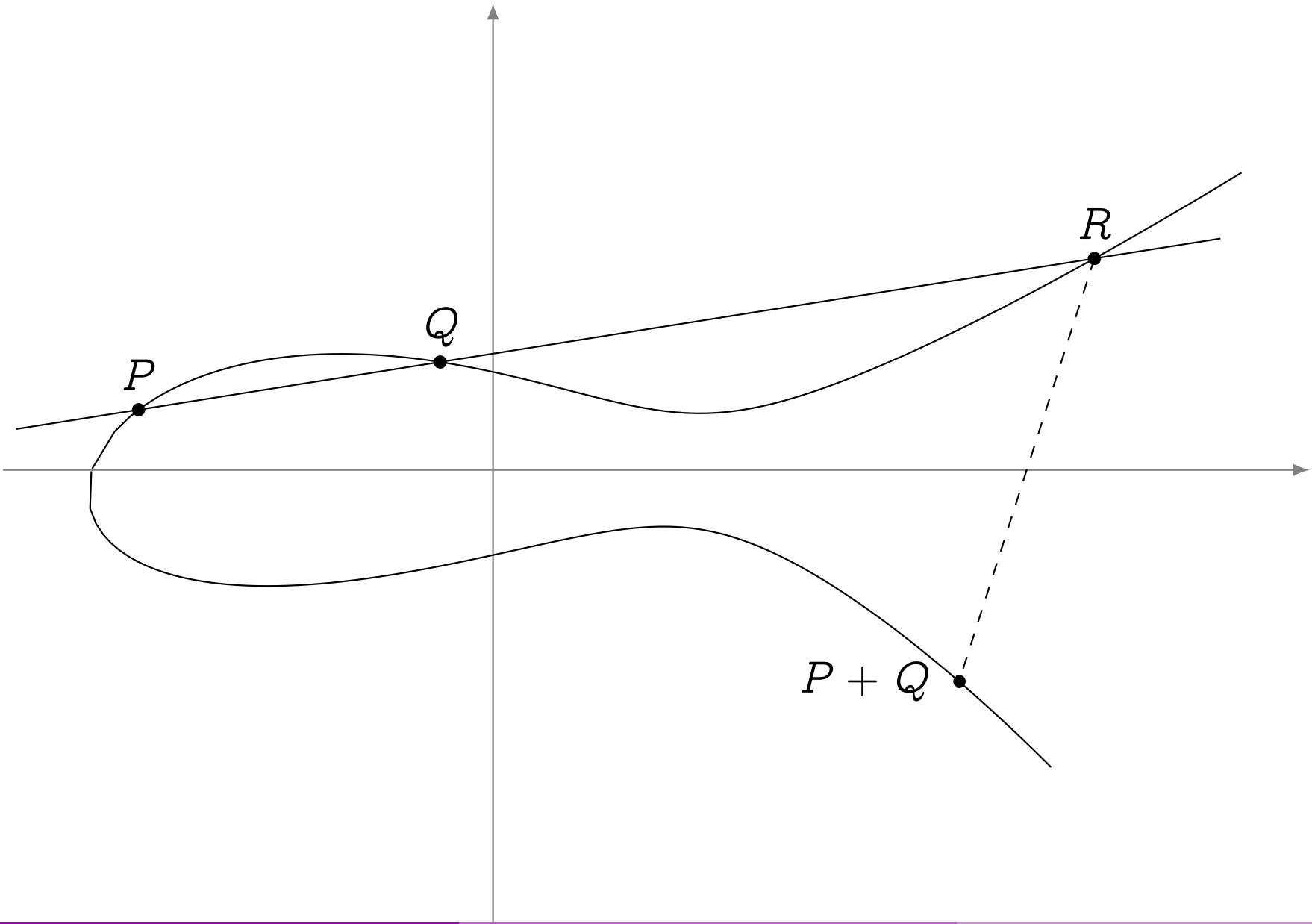
Up to isomorphism



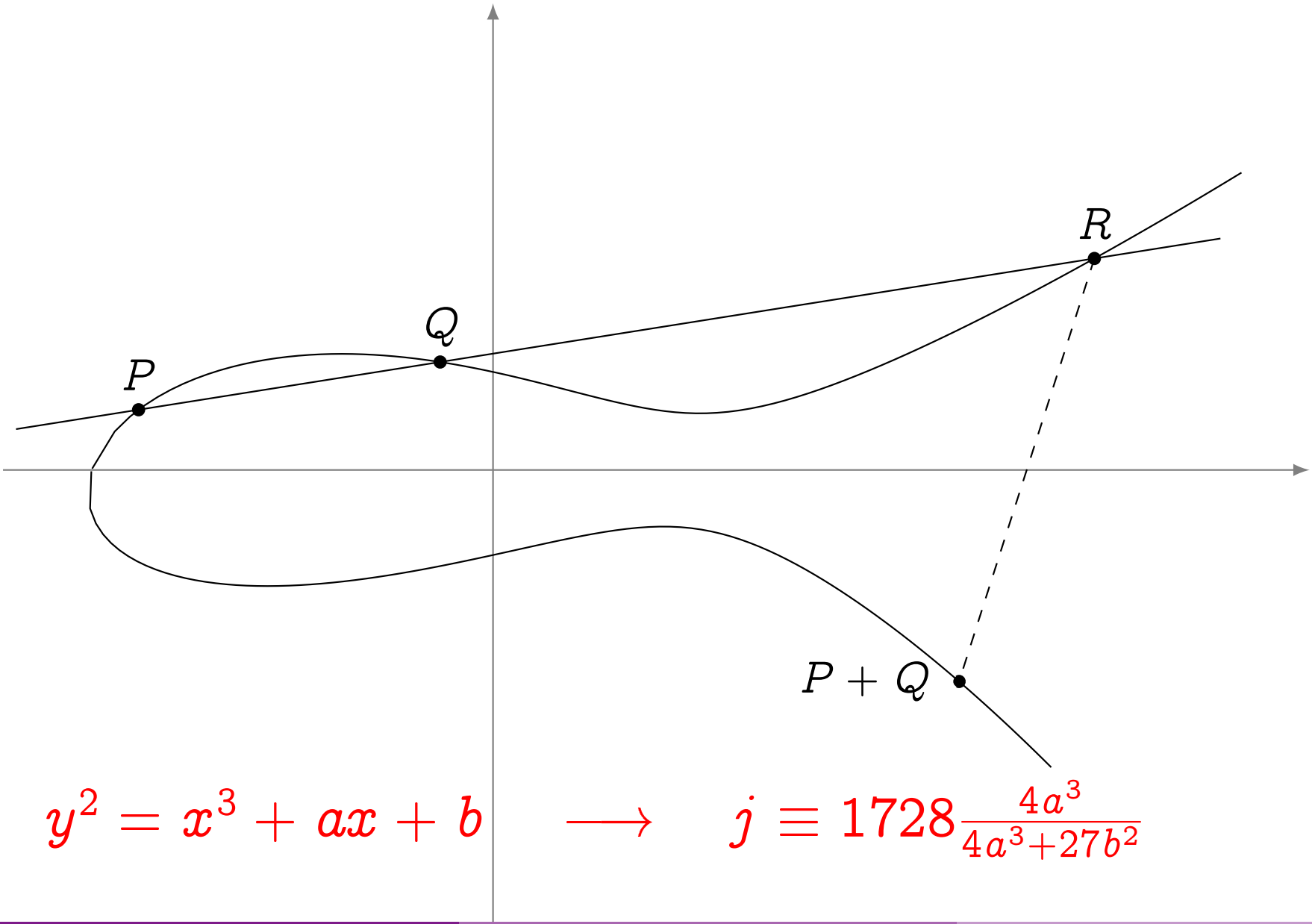
Up to isomorphism



Up to isomorphism

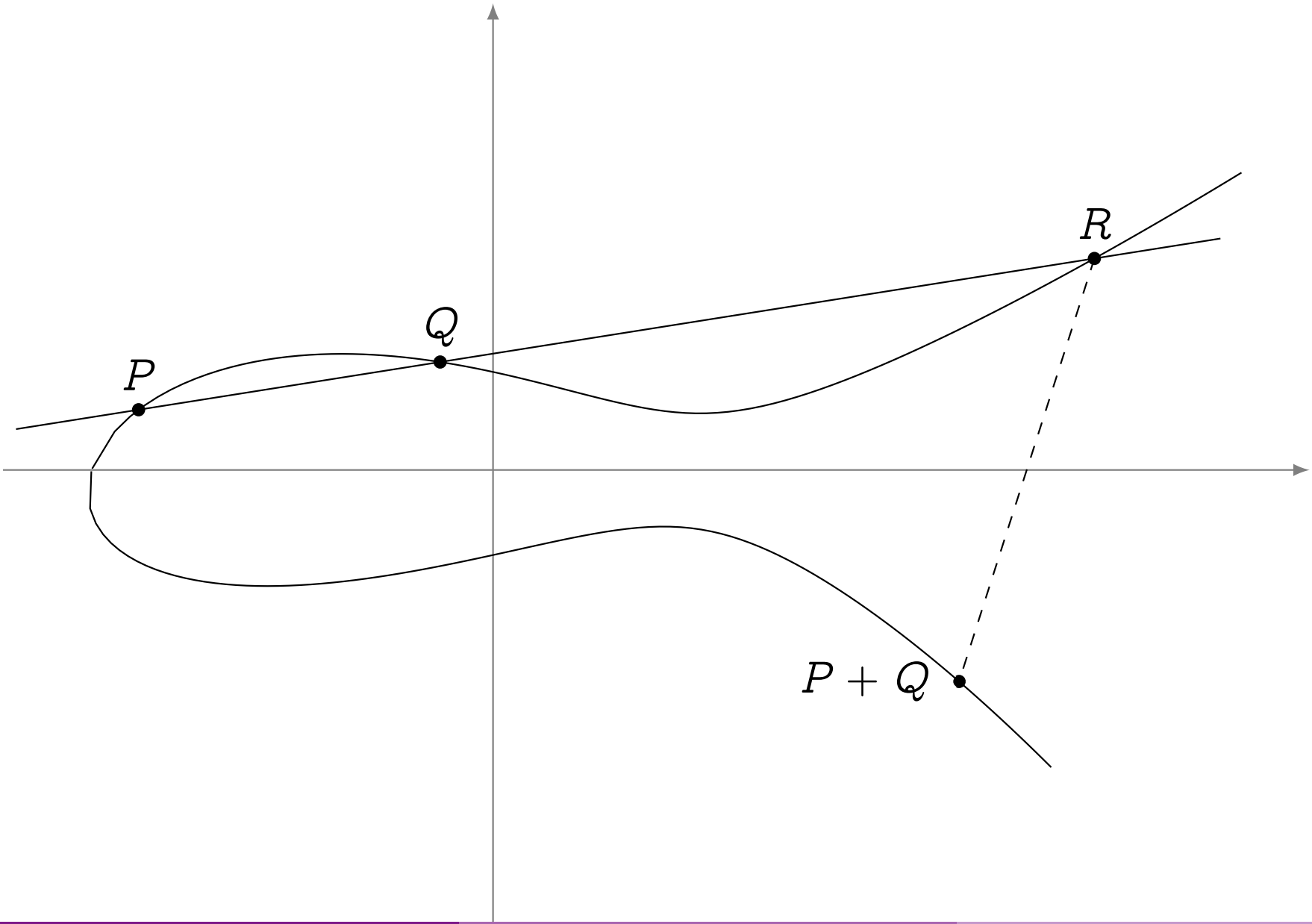


Up to isomorphism

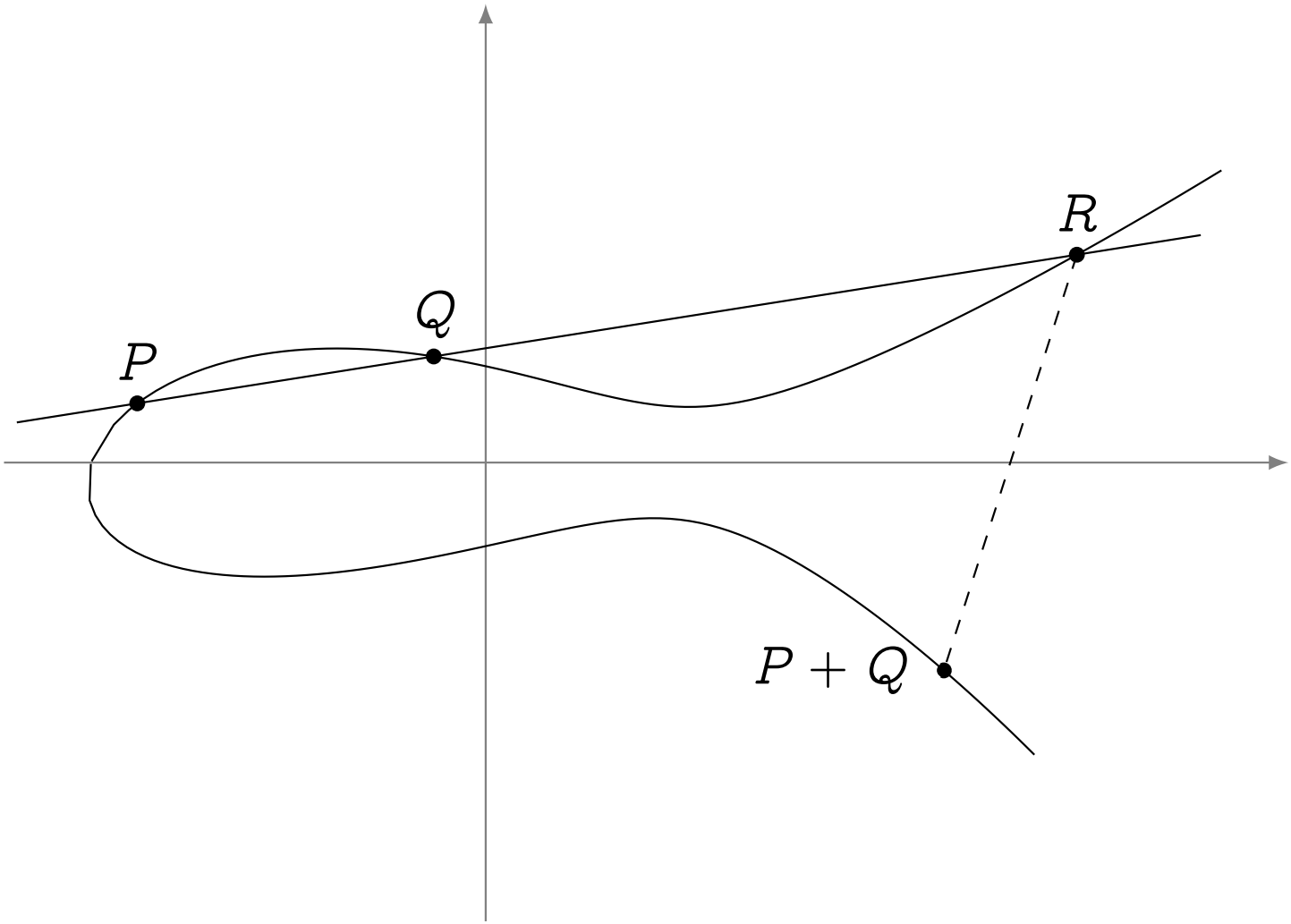


$$y^2 = x^3 + ax + b \quad \longrightarrow \quad j \equiv 1728 \frac{4a^3}{4a^3+27b^2}$$

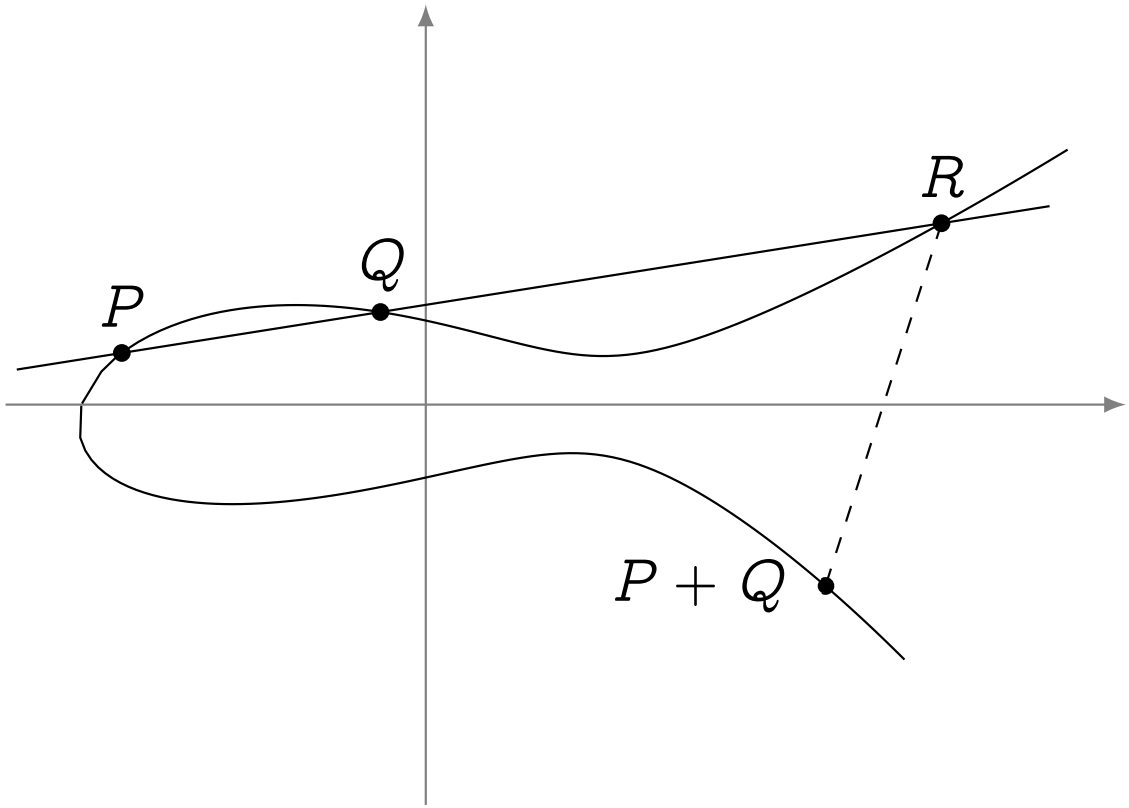
Up to isomorphism



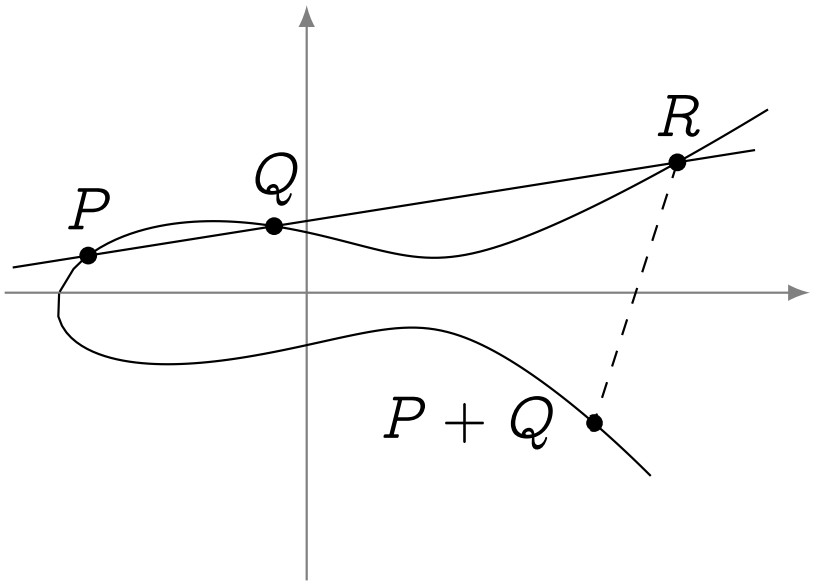
Up to isomorphism



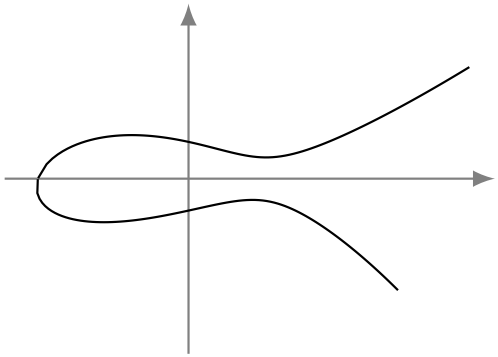
Up to isomorphism



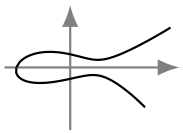
Up to isomorphism



Up to isomorphism



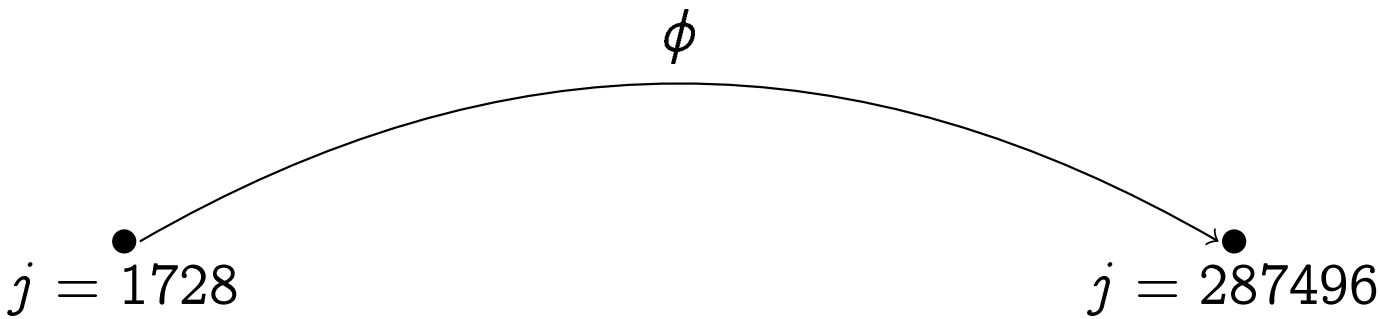
Up to isomorphism



Up to isomorphism

$$j = \overset{\bullet}{1728}$$

Up to isomorphism



Up to isomorphism

Isogeny graphs

Serre-Tate theorem

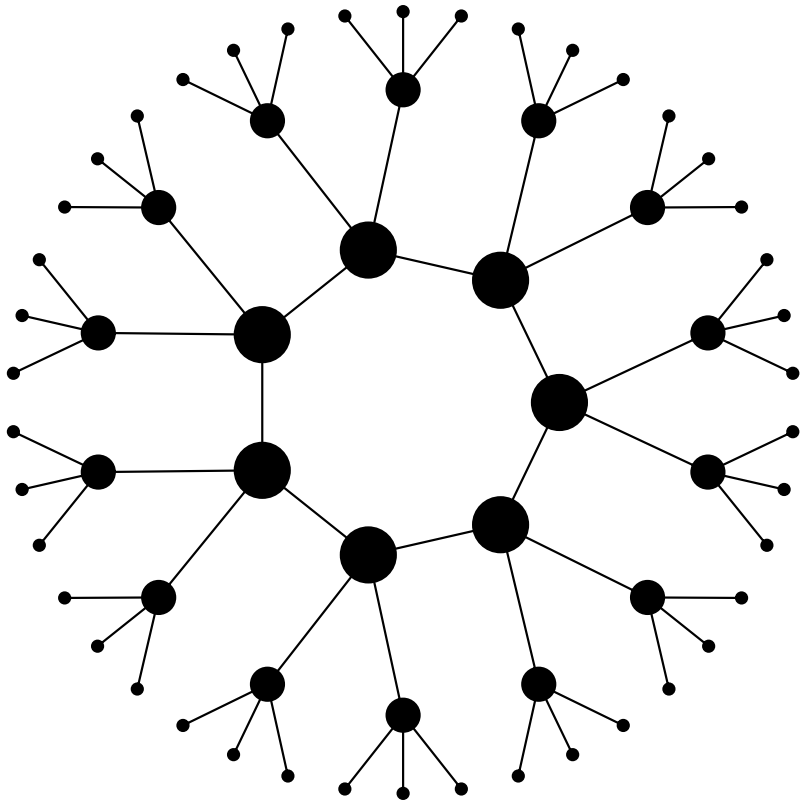
Two elliptic curves E, E' defined over a finite field $\mathbb{F}_q$ are isogenous (over $\mathbb{F}_q$) iff $\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$.

Isogeny graphs

- Vertices are curves up to isomorphism,
- Edges are isogenies up to isomorphism.

Isogeny volcanoes

- Curves are ordinary,
- Isogenies all have degree a prime ℓ.



What do isogeny graphs look like?

Torsion subgroups (ℓ prime)

In an algebraically closed field:

$$E[\ell] = \langle P, Q \rangle \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$$

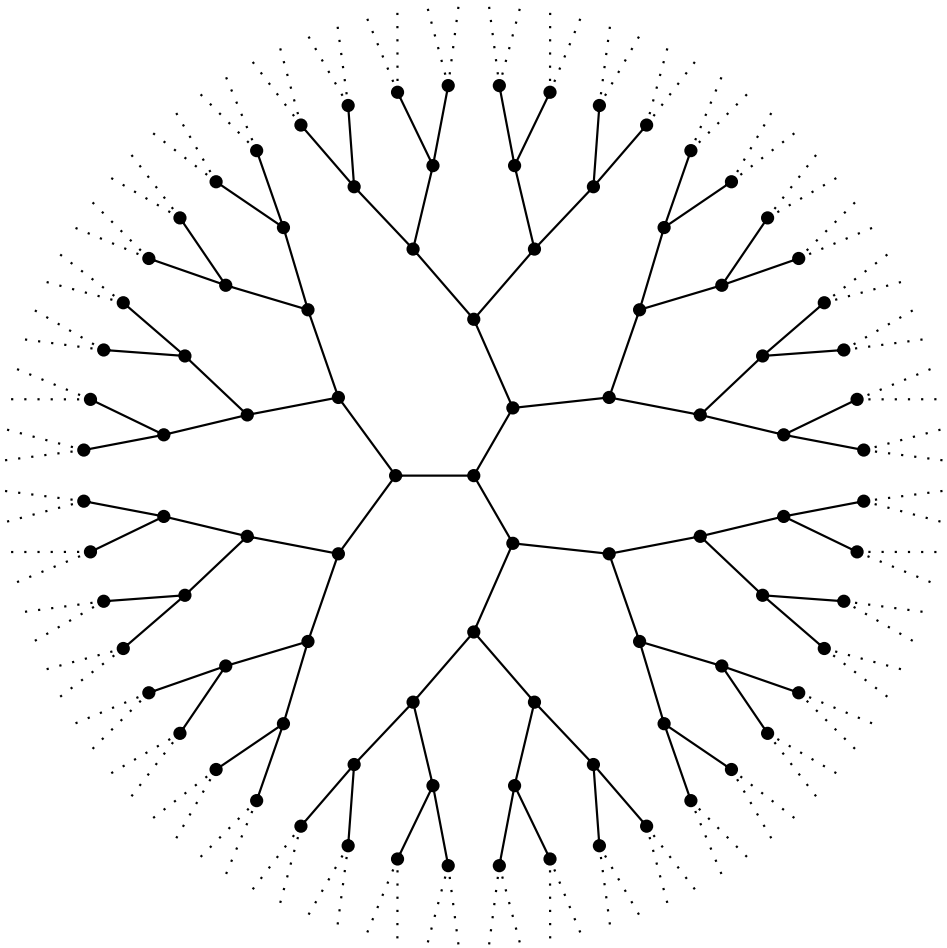
$$\Downarrow$$

There are exactly $\ell + 1$ cyclic subgroups $H \subset E$ of order ℓ:

$$\langle P + Q \rangle, \langle P + 2Q \rangle, \ldots, \langle P \rangle, \langle Q \rangle$$

$$\Downarrow$$

There are exactly $\ell + 1$ distinct isogenies of degree ℓ.



(non-CM) 2-isogeny graph over $\mathbb{C}$

What happens over a finite field $\mathbb{F}_p$?

Rational isogenies ($\ell \neq p$)

In the algebraic closure $\bar{\mathbb{F}}_p$

$$E[\ell] = \langle P, Q \rangle \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$$

However, an isogeny is defined over $\mathbb{F}_p$ only if its kernel is Galois invariant.

Enter the Frobenius map

$$\begin{aligned} \pi : E &\longrightarrow E \\ (x, y) &\longmapsto (x^p, y^p) \end{aligned}$$

E is seen here as a curve over $\bar{\mathbb{F}}_p$.

The Frobenius action on $E[\ell]$

$$\begin{aligned} \pi(P) &= aP + bQ \\ \pi(Q) &= cP + dQ \end{aligned}$$

What happens over a finite field $\mathbb{F}_p$?

Rational isogenies ($\ell \neq p$)

In the algebraic closure $\bar{\mathbb{F}}_p$

$$E[\ell] = \langle P, Q \rangle \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$$

However, an isogeny is defined over $\mathbb{F}_p$ only if its kernel is Galois invariant.

Enter the Frobenius map

$$\begin{aligned} \pi : E &\longrightarrow E \\ (x, y) &\longmapsto (x^p, y^p) \end{aligned}$$

E is seen here as a curve over $\bar{\mathbb{F}}_p$.

The Frobenius action on $E[\ell]$

$$aP + bQ$$

$$cP + dQ$$

What happens over a finite field $\mathbb{F}_p$?

Rational isogenies ($\ell \neq p$)

In the algebraic closure $\bar{\mathbb{F}}_p$

$$E[\ell] = \langle P, Q \rangle \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$$

However, an isogeny is defined over $\mathbb{F}_p$ only if its kernel is Galois invariant.

Enter the Frobenius map

$$\begin{aligned} \pi : E &\longrightarrow E \\ (x, y) &\longmapsto (x^p, y^p) \end{aligned}$$

E is seen here as a curve over $\bar{\mathbb{F}}_p$.

The Frobenius action on $E[\ell]$

$$\begin{pmatrix} aP + bQ \\ cP + dQ \end{pmatrix}$$

What happens over a finite field $\mathbb{F}_p$?

Rational isogenies ($\ell \neq p$)

In the algebraic closure $\bar{\mathbb{F}}_p$

$$E[\ell] = \langle P, Q \rangle \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$$

However, an isogeny is defined over $\mathbb{F}_p$ only if its kernel is Galois invariant.

Enter the Frobenius map

$$\begin{aligned} \pi : E &\longrightarrow E \\ (x, y) &\longmapsto (x^p, y^p) \end{aligned}$$

E is seen here as a curve over $\bar{\mathbb{F}}_p$.

The Frobenius action on $E[\ell]$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

What happens over a finite field $\mathbb{F}_p$?

Rational isogenies ($\ell \neq p$)

In the algebraic closure $\bar{\mathbb{F}}_p$

$$E[\ell] = \langle P, Q \rangle \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$$

However, an isogeny is defined over $\mathbb{F}_p$ only if its kernel is Galois invariant.

Enter the Frobenius map

$$\begin{aligned} \pi : E &\longrightarrow E \\ (x, y) &\longmapsto (x^p, y^p) \end{aligned}$$

E is seen here as a curve over $\bar{\mathbb{F}}_p$.

The Frobenius action on $E[\ell]$

$$\pi : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \bmod \ell$$

What happens over a finite field $\mathbb{F}_p$?

Rational isogenies ($\ell \neq p$)

In the algebraic closure $\bar{\mathbb{F}}_p$

$$E[\ell] = \langle P, Q \rangle \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$$

However, an isogeny is defined over $\mathbb{F}_p$ only if its kernel is Galois invariant.

Enter the Frobenius map

$$\begin{aligned} \pi : E &\longrightarrow E \\ (x, y) &\longmapsto (x^p, y^p) \end{aligned}$$

E is seen here as a curve over $\bar{\mathbb{F}}_p$.

The Frobenius action on $E[\ell]$

$$\pi : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \bmod \ell$$

We identify $\pi | E[\ell]$ to a conjugacy class in $\mathrm{GL}(\mathbb{Z}/\ell\mathbb{Z})$.

What happens over a finite field $\mathbb{F}_p$?

Galois invariant proper subgroups of $E[\ell]$

=

eigenspaces of $\pi \in \mathrm{GL}(\mathbb{Z}/\ell\mathbb{Z})$

=

rational isogenies of degree ℓ

What happens over a finite field $\mathbb{F}_p$?

Galois invariant proper subgroups of $E[\ell]$

=

eigenspaces of $\pi \in \mathrm{GL}(\mathbb{Z}/\ell\mathbb{Z})$

=

rational isogenies of degree ℓ

How many Galois invariant subgroups?

- $\pi|E[\ell] \sim \left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda \end{smallmatrix}\right)$ $\rightarrow \ell + 1$ isogenies
- $\pi|E[\ell] \sim \left(\begin{smallmatrix} \lambda & 0 \\ 0 & \mu \end{smallmatrix}\right)$ with $\lambda \neq \mu$ $\rightarrow$ two isogenies
- $\pi|E[\ell] \sim \left(\begin{smallmatrix} \lambda & * \\ 0 & \lambda \end{smallmatrix}\right)$ $\rightarrow$ one isogeny
- $\pi|E[\ell]$ has no eigenvalues in $\mathbb{Z}/\ell\mathbb{Z}$ $\rightarrow$ no isogeny

Algebras, orders

- A quadratic imaginary number field is an extension of $\mathbb{Q}$ of the form $Q[\sqrt{-D}]$ for some non-square $D > 0$.
- A quaternion algebra is an algebra of the form $\mathbb{Q} + \alpha\mathbb{Q} + \beta\mathbb{Q} + \alpha\beta\mathbb{Q}$, where the generators satisfy the relations

$$\alpha^2, \beta^2 \in \mathbb{Q}, \quad \alpha^2 < 0, \quad \beta^2 < 0, \quad \beta\alpha = -\alpha\beta.$$

Orders

Let K be a finitely generated $\mathbb{Q}$-algebra. An order $\mathcal{O} \subset K$ is a subring of K that is a finitely generated $\mathbb{Z}$-module of maximal dimension. An order that is not contained in any other order of K is called a maximal order.

Examples:

- $\mathbb{Z}$ is the only order contained in $\mathbb{Q}$,
- $\mathbb{Z}[i]$ is the only maximal order of $\mathbb{Q}(i)$,
- $\mathbb{Z}[\sqrt{5}]$ is a non-maximal order of $\mathbb{Q}(\sqrt{5})$,
- The ring of integers of a number field is its only maximal order,
- In general, maximal orders in quaternion algebras are not unique.

The endomorphism ring

The endomorphism ring $\mathtt{End}(E)$ of an elliptic curve E is the ring of all isogenies $E \to E$ (plus the null map) with addition and composition.

Theorem (Deuring)

Let E be an elliptic curve defined over a field k of characteristic p.
$\mathtt{End}(E)$ is isomorphic to one of the following:

- $\mathbb{Z}$, only if $p = 0$

  E is ordinary.

- An order $\mathcal{O}$ in a quadratic imaginary field:

  E is ordinary with complex multiplication by $\mathcal{O}$.

- Only if $p > 0$, a maximal order in a quaternion algebra[a]:

  E is supersingular.

[a] (ramified at p and ∞)

The finite field case

Theorem (Hasse)

Let E be defined over a finite field. Its Frobenius endomorphism π satisfies a quadratic equation

$$\pi^2 - t\pi + q = 0$$

in $\mathrm{End}(E)$ for some $|t| \leq 2\sqrt{q}$, called the trace of π. The trace t is coprime to q if and only if E is ordinary.

Suppose E is ordinary, then $D_\pi = t^2 - 4q < 0$ is the discriminant of $\mathbb{Z}[\pi]$.

- $K = \mathbb{Q}(\pi) = \mathbb{Q}(\sqrt{D_\pi})$ is the endomorphism algebra of E.
- Denote by $\mathcal{O}_K$ its ring of integers, then

$$\mathbb{Z} \neq \mathbb{Z}[\pi] \subset \mathrm{End}(E) \subset \mathcal{O}_K.$$

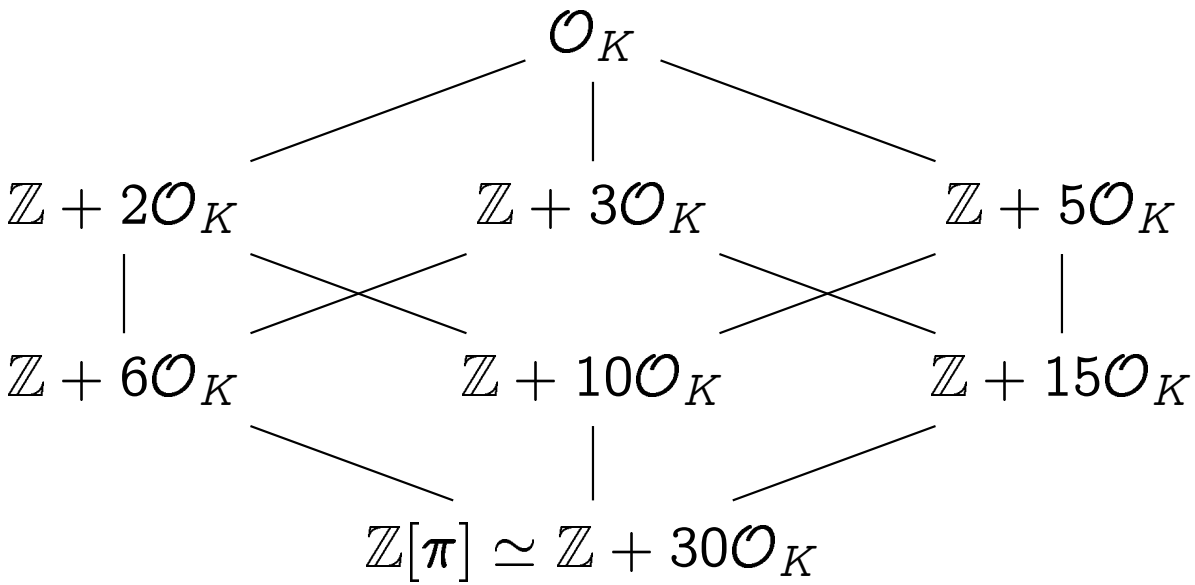
In the supersingular case, π may or may not be in $\mathbb{Z}$, depending on q.

Endomorphism rings of ordinary curves

Classifying quadratic orders

Let K be a quadratic number field, and let $\mathcal{O}_K$ be its ring of integers.

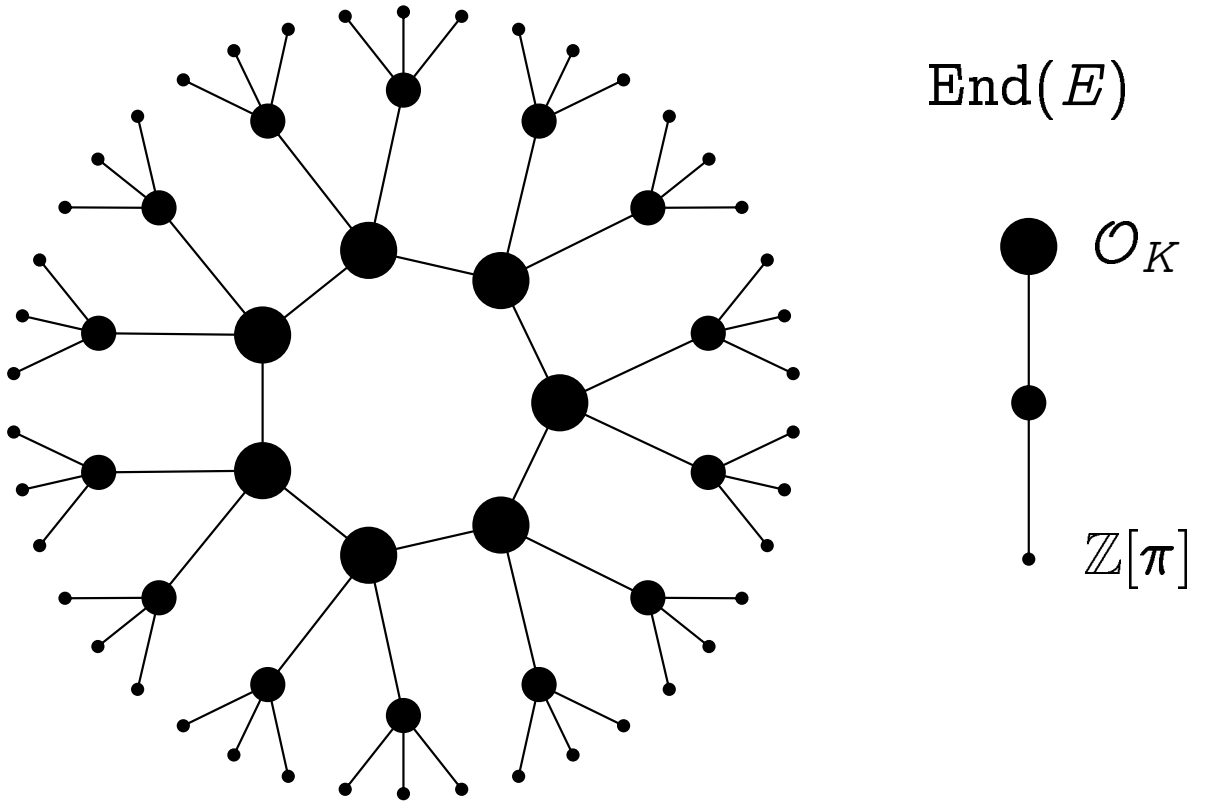
- Any order $\mathcal{O} \subset K$ can be written as $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$ for an integer f, called the conductor of $\mathcal{O}$, denoted by $[\mathcal{O}_k : \mathcal{O}]$.
- If d_K is the discriminant of K, the discriminant of $\mathcal{O}$ is $f^2 d_K$.
- If $\mathcal{O}, \mathcal{O}'$ are two orders with discriminants d, d', then $\mathcal{O} \subset \mathcal{O}'$ iff $d' \mid d$.



Volcanology (Kohel 1996)

Let E, E' be curves with respective endomorphism rings $\mathcal{O}, \mathcal{O}' \subset K$.
Let $\phi : E \to E'$ be an isogeny of prime degree ℓ, then:

if $\mathcal{O} = \mathcal{O}'$, ϕ is horizontal;
if $[\mathcal{O}' : \mathcal{O}] = \ell$, ϕ is ascending;
if $[\mathcal{O} : \mathcal{O}'] = \ell$, ϕ is descending.

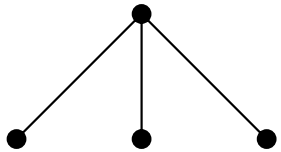


Ordinary isogeny volcano of degree $\ell = 3$.

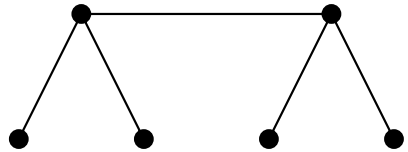
Volcanology (Kohel 1996)

Let E be ordinary,
$\mathrm{End}(E) \subset K$.

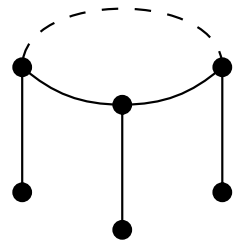
$\mathcal{O}_K$: maximal order of K,
D_K: discriminant of K.



$\left(\frac{D_K}{\ell}\right) = -1$



$\left(\frac{D_K}{\ell}\right) = 0$



$\left(\frac{D_K}{\ell}\right) = +1$

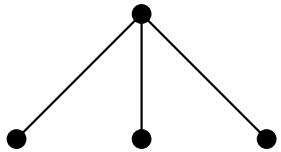
		Horizontal	**Ascending**	**Descending**
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$	$1 + \left(\frac{D_K}{\ell}\right)$		
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$	$1 + \left(\frac{D_K}{\ell}\right)$		$\ell - \left(\frac{D_K}{\ell}\right)$
$\ell \mid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$		1	ℓ
$\ell \mid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$		1	

Volcanology (Kohel 1996)

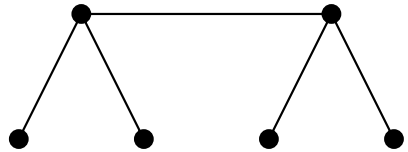
Let E be ordinary,
$\mathrm{End}(E) \subset K$.

$\mathcal{O}_K$: maximal order of K,
D_K: discriminant of K.

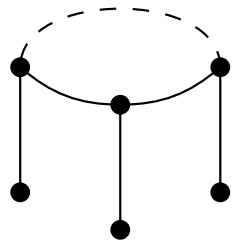
Height $= v_\ell([\mathcal{O}_K : \mathbb{Z}[\pi]])$.



$\left(\frac{D_K}{\ell}\right) = -1$



$\left(\frac{D_K}{\ell}\right) = 0$



$\left(\frac{D_K}{\ell}\right) = +1$

		Horizontal	Ascending	Descending
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$	$1 + \left(\frac{D_K}{\ell}\right)$		
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$	$1 + \left(\frac{D_K}{\ell}\right)$		$\ell - \left(\frac{D_K}{\ell}\right)$
$\ell \mid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$		1	ℓ
$\ell \mid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$		1	

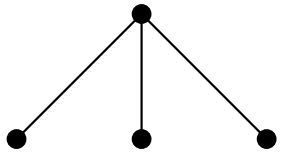
Volcanology (Kohel 1996)

Let E be ordinary,
$\mathrm{End}(E) \subset K$.

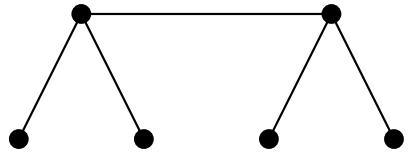
$\mathcal{O}_K$: maximal order of K,
D_K: discriminant of K.

Height $= v_\ell([\mathcal{O}_K : \mathbb{Z}[\pi]])$.

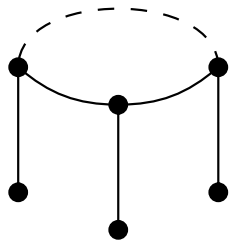
How large is the crater?



$\left(\frac{D_K}{\ell}\right) = -1$



$\left(\frac{D_K}{\ell}\right) = 0$



$\left(\frac{D_K}{\ell}\right) = +1$

		Horizontal	Ascending	Descending
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$	$1 + \left(\frac{D_K}{\ell}\right)$		
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$	$1 + \left(\frac{D_K}{\ell}\right)$		$\ell - \left(\frac{D_K}{\ell}\right)$
$\ell \mid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$		1	ℓ
$\ell \mid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$		1	

How large is the crater of a volcano?

Let $\mathrm{End}(E) = \mathcal{O} \subset \mathbb{Q}(\sqrt{-D})$. Define

- $\mathcal{I}(\mathcal{O})$, the group of invertible fractional ideals,
- $\mathcal{P}(\mathcal{O})$, the group of principal ideals,

The class group

The class group of $\mathcal{O}$ is

$$\mathrm{Cl}(\mathcal{O}) = \mathcal{I}(\mathcal{O})/\mathcal{P}(O).$$

- It is a finite abelian group.
- Its order $h(\mathcal{O})$ is called the class number of $\mathcal{O}$.
- It arises as the Galois group of an abelian extension of $\mathbb{Q}(\sqrt{-D})$.

Complex multiplication

The $\mathfrak{a}$-torsion

- Let $\mathfrak{a} \subset \mathcal{O}$ be an (integral invertible) ideal of $\mathcal{O}$;
- Let $E[\mathfrak{a}]$ be the subgroup of E annihilated by $\mathfrak{a}$:

$$E[\mathfrak{a}] = \{P \in E \mid \alpha(P) = 0 \text{ for all } \alpha \in \mathfrak{a}\};$$

- Let $\phi : E \to E_{\mathfrak{a}}$, where $E_{\mathfrak{a}} = E/E[\mathfrak{a}]$.

Then $\mathrm{End}(E_{\mathfrak{a}}) = \mathcal{O}$ (i.e., ϕ is horizontal).

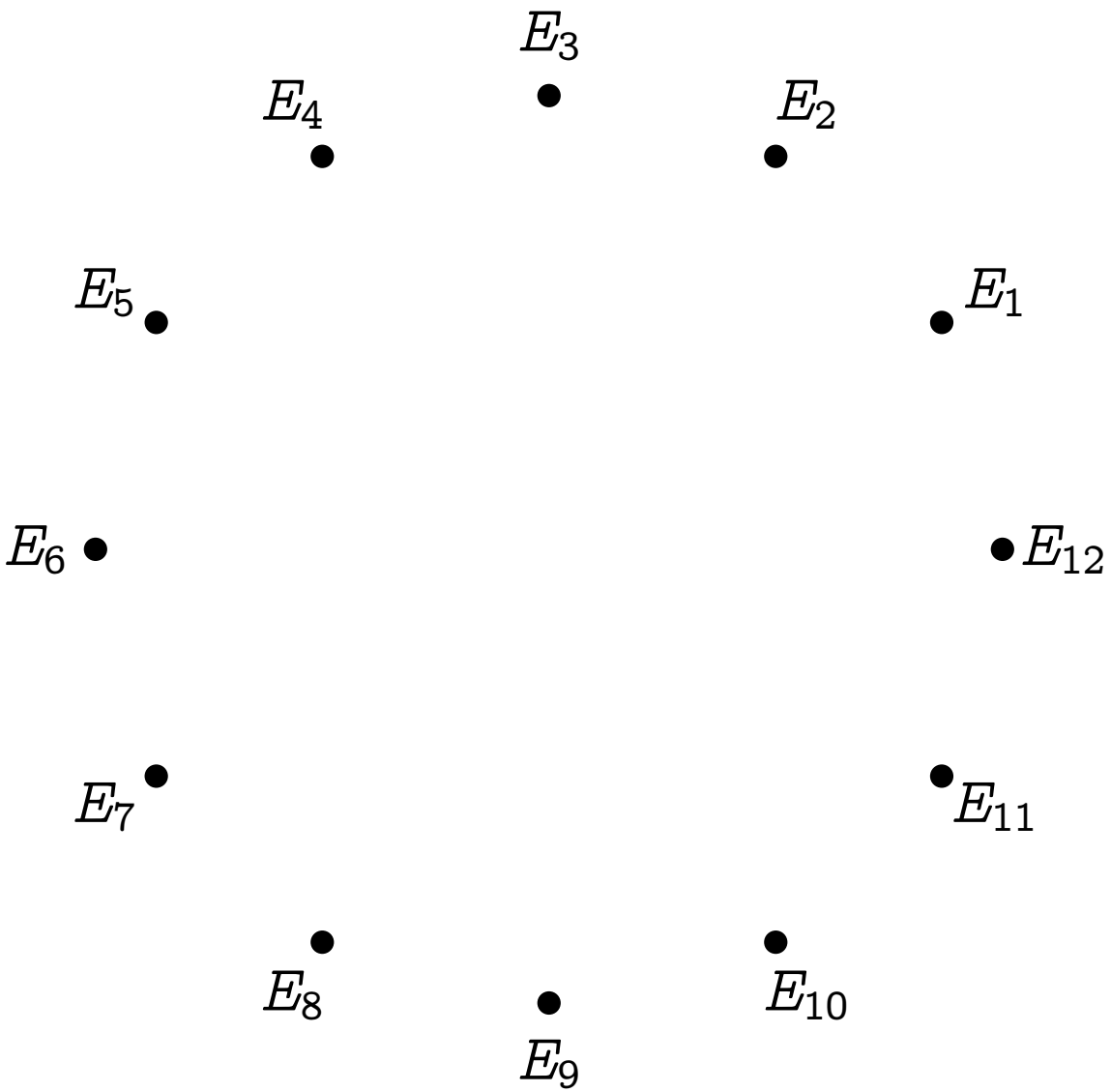
Theorem (Complex multiplication)

The action on the set of elliptic curves with complex multiplication by $\mathcal{O}$ defined by $\mathfrak{a} * j(E) = j(E_{\mathfrak{a}})$ factors through $\mathrm{Cl}(\mathcal{O})$, is faithful and transitive.

Corollary

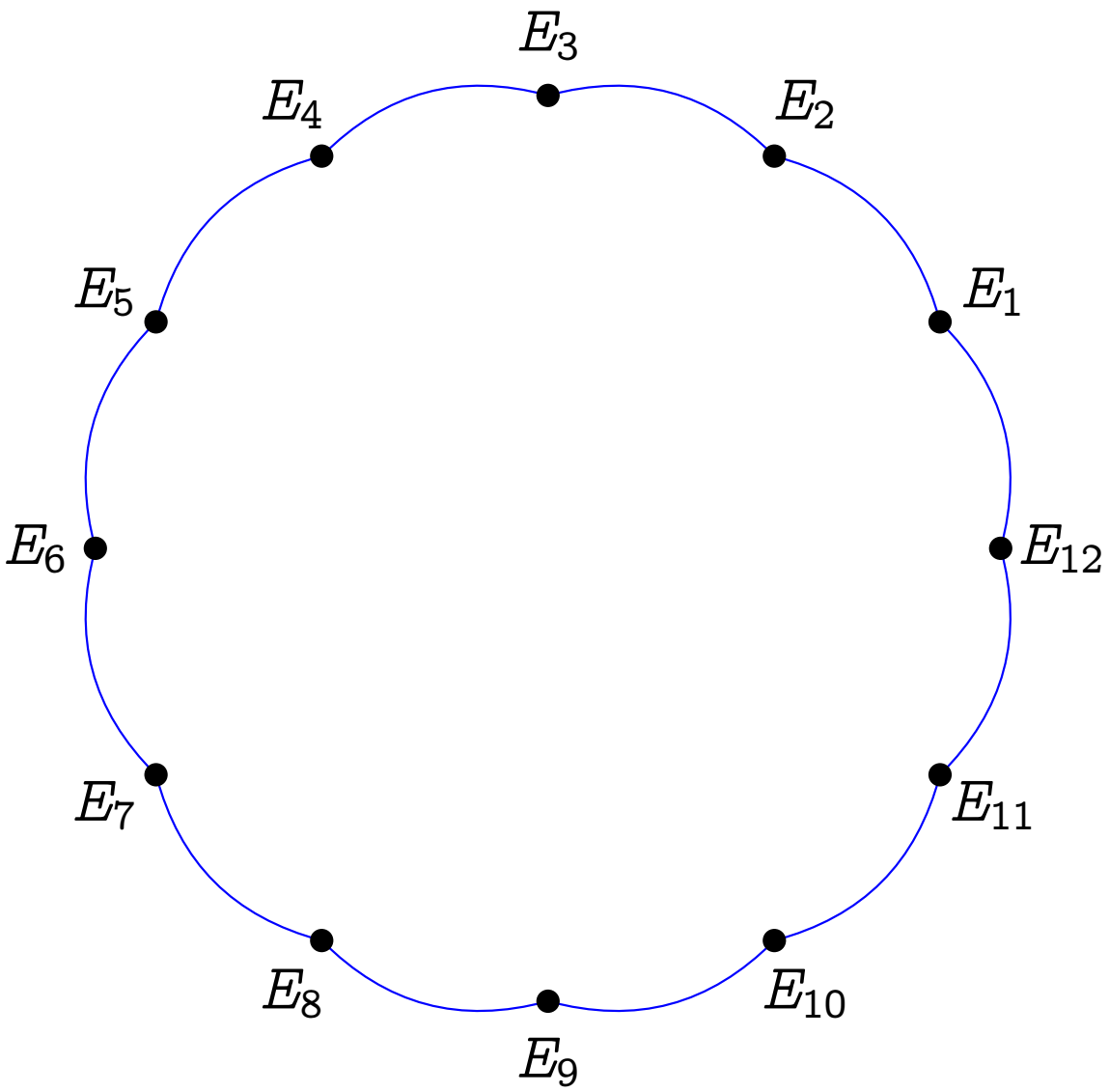
Let $\mathrm{End}(E)$ have discriminant D. Assume that $\left(\frac{D}{\ell}\right) = 1$, then E is on a crater of size N of an ℓ-volcano, and $N | h(\mathrm{End}(E))$

Complex multiplication graphs



Vertices are elliptic curves with complex multiplication by $\mathcal{O}_K$ (i.e., $\mathrm{End}(E) \simeq \mathcal{O}_K \subset \mathbb{Q}(\sqrt{-D})$).

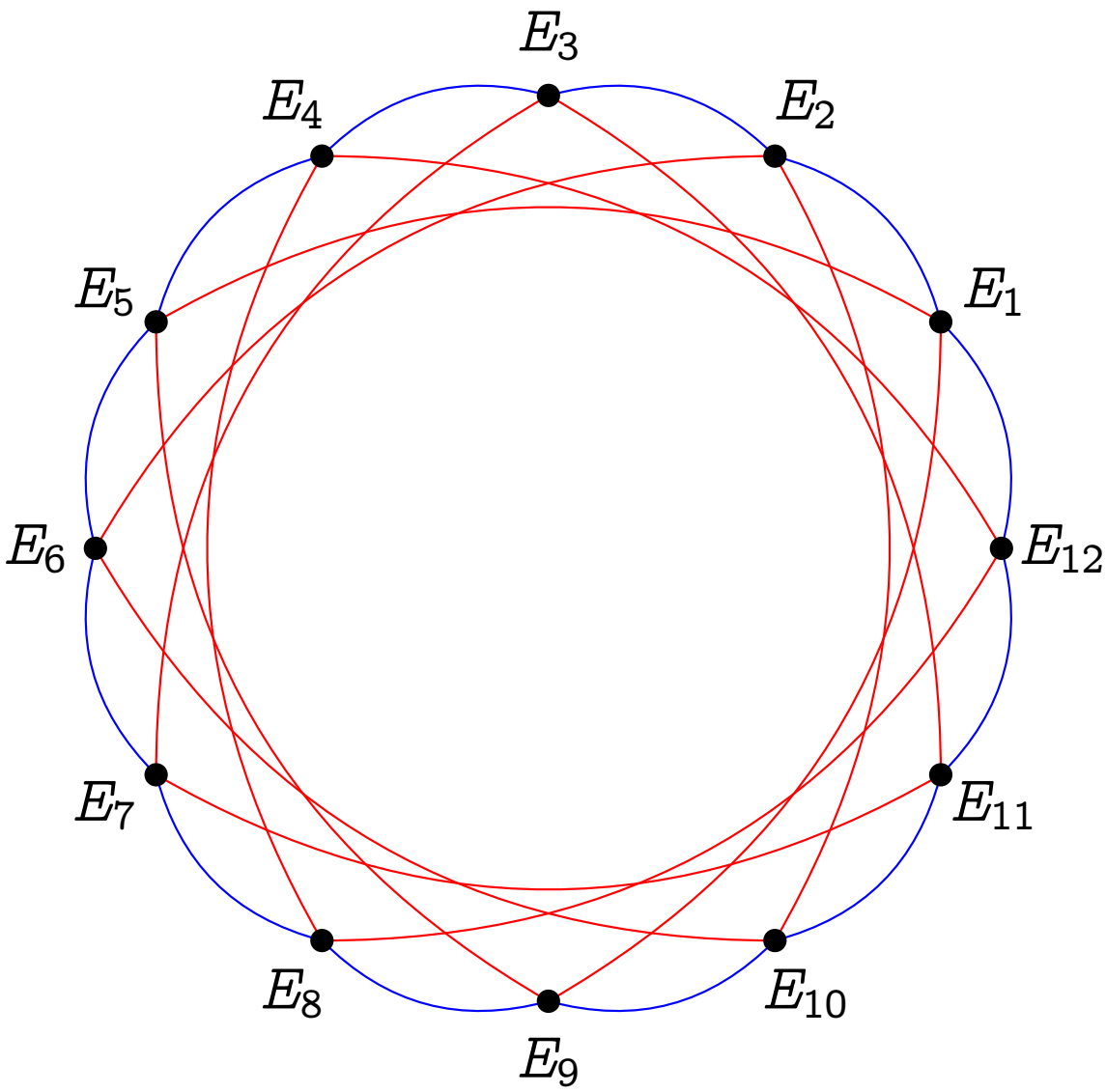
Complex multiplication graphs



Vertices are elliptic curves with complex multiplication by $\mathcal{O}_K$ (i.e., $\mathrm{End}(E) \simeq \mathcal{O}_K \subset \mathbb{Q}(\sqrt{-D})$).
Edges are horizontal isogenies of bounded prime degree.

— degree 2

Complex multiplication graphs

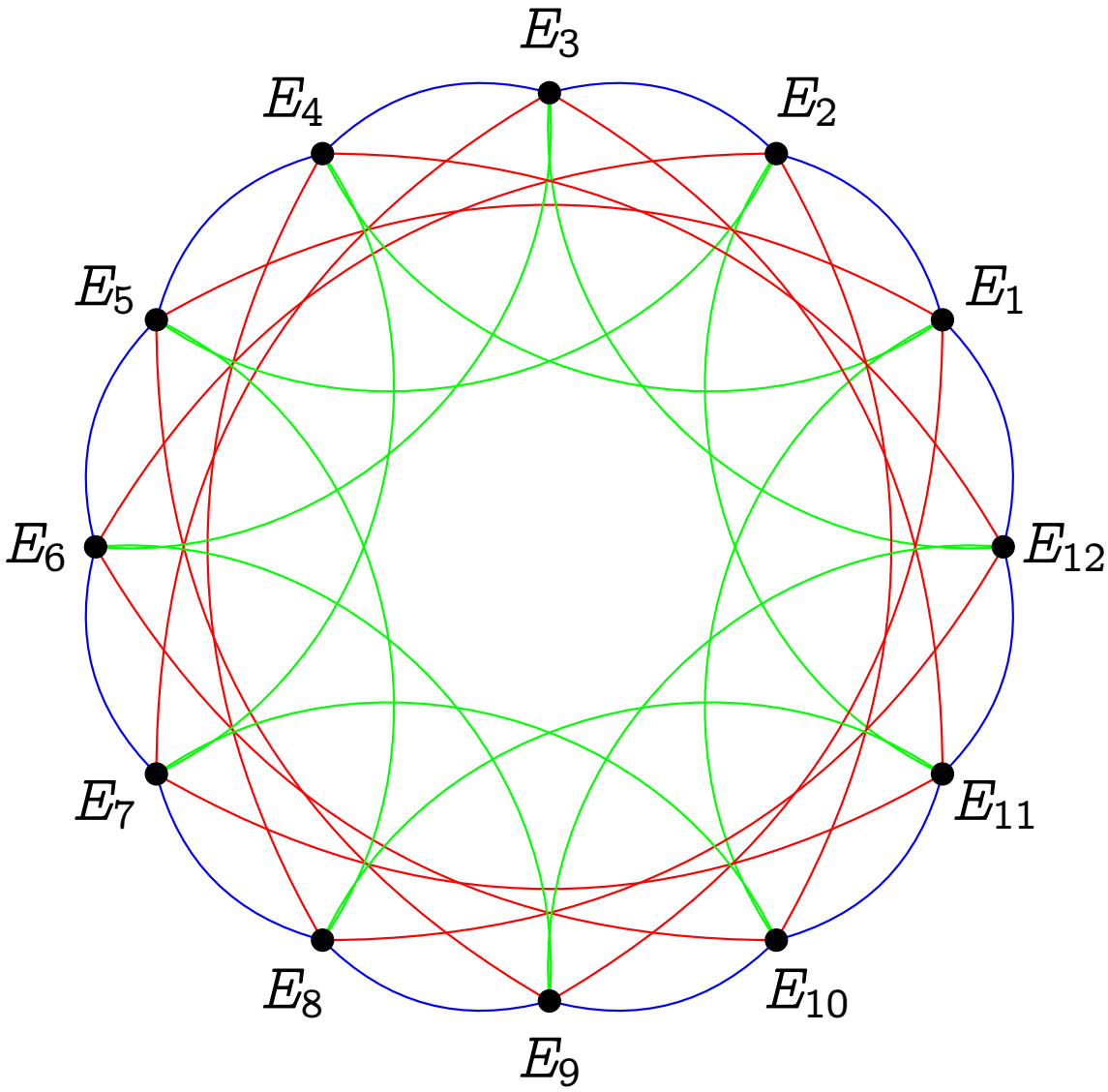


Vertices are elliptic curves with complex multiplication by $\mathcal{O}_K$ (i.e., $\mathrm{End}(E) \simeq \mathcal{O}_K \subset \mathbb{Q}(\sqrt{-D})$).
Edges are horizontal isogenies of bounded prime degree.

— degree 2

— degree 3

Complex multiplication graphs



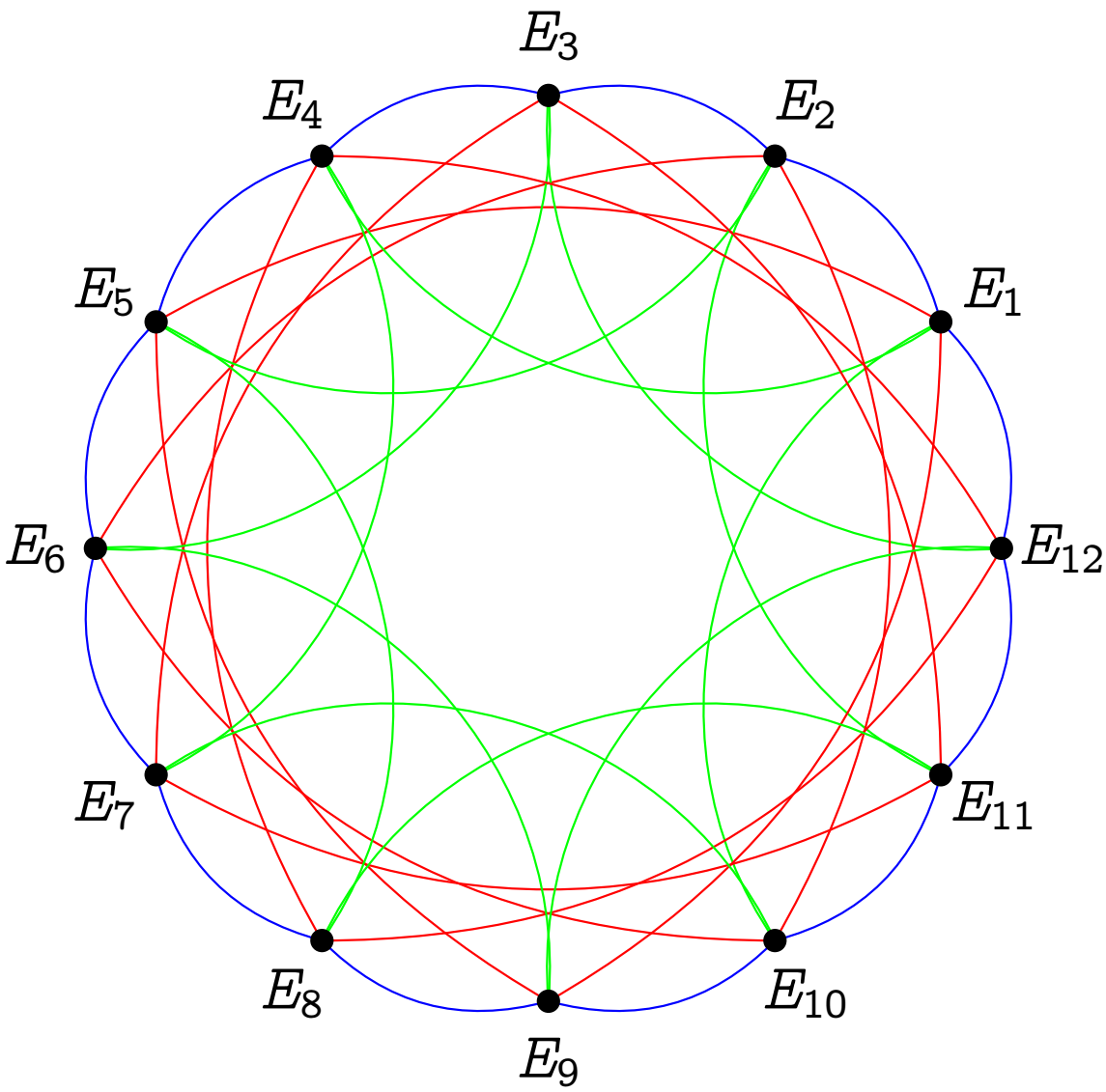
Vertices are elliptic curves with complex multiplication by $\mathcal{O}_K$ (i.e., $\mathrm{End}(E) \simeq \mathcal{O}_K \subset \mathbb{Q}(\sqrt{-D})$).
Edges are horizontal isogenies of bounded prime degree.

— degree 2

— degree 3

— degree 5

Complex multiplication graphs



Vertices are elliptic curves with complex multiplication by $\mathcal{O}_K$ (i.e., $\mathrm{End}(E) \simeq \mathcal{O}_K \subset \mathbb{Q}(\sqrt{-D})$).
Edges are horizontal isogenies of bounded prime degree.

— degree 2

— degree 3

— degree 5

Isomorphic to a Cayley graph of $\mathrm{Cl}(\mathcal{O}_K)$.

Supersingular endomorphisms

Recall, a curve E over a field $\mathbb{F}_q$ of characteristic p is supersingular iff

$$\pi^2 - t\pi + q = 0$$

with $t = 0 \mod p$.

Case: $t = 0 \Rightarrow D_\pi = -4q$

- Only possibility for $E/\mathbb{F}_p$,
- $E/\mathbb{F}_p$ has CM by an order of $\mathbb{Q}(\sqrt{-p})$, similar to the ordinary case.

Case: $t = \pm 2\sqrt{q} \Rightarrow D_\pi = 0$

- General case for $E/\mathbb{F}_q$, when q is an even power.
- $\pi = \pm\sqrt{q}$, hence no complex multiplication.

We will ignore marginal cases: $t = \pm\sqrt{q}, \pm\sqrt{2q}, \pm\sqrt{3q}$.

Supersingular complex multiplication

Let $E/\mathbb{F}_p$ be a supersingular curve, then $\pi^2 = -p$, and

$$\pi = \begin{pmatrix} \sqrt{-p} & 0 \\ 0 & -\sqrt{-p} \end{pmatrix} \mod \ell$$

for any ℓ s.t. $\left(\frac{-p}{\ell}\right) = 1$.

Theorem (Delfs, Galbraith 2016)

Let $\mathrm{End}_{\mathbb{F}_p}(E)$ denote the ring of $\mathbb{F}_p$-rational endomorphisms of E. Then

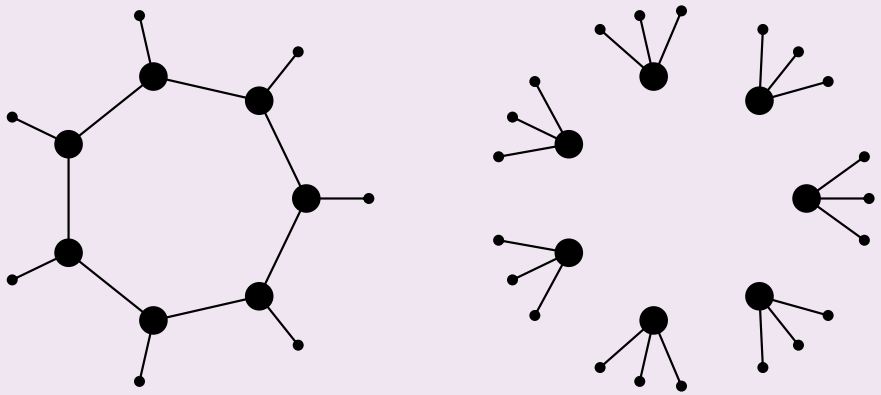
$$\mathbb{Z}[\pi] \subset \mathrm{End}_{\mathbb{F}_p}(E) \subset \mathbb{Q}(\sqrt{-p}).$$

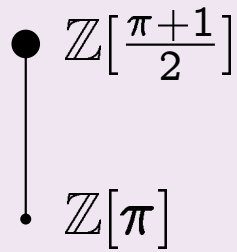
Orders of $\mathbb{Q}(\sqrt{-p})$

- If $p = 1 \mod 4$, then $\mathbb{Z}[\pi]$ is the maximal order.
- If $p = -1 \mod 4$, then $\mathbb{Z}[\frac{\pi+1}{2}]$ is the maximal order, and $[\mathbb{Z}[\frac{\pi+1}{2}] : \mathbb{Z}[\pi]] = 2$.

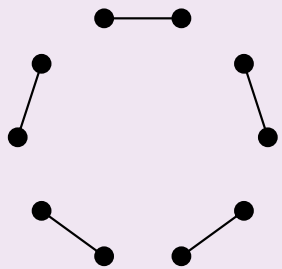
Supersingular CM graphs

2-volcanoes, $p = -1 \bmod 4$





2-graphs, $p = 1 \bmod 4$



- $\mathbb{Z}[\pi]$

All other ℓ-graphs are cycles of horizontal isogenies iff $\left(\frac{-p}{\ell}\right) = 1$.

The full endomorphism ring

Theorem (Deuring)

Let E be a supersingular elliptic curve, then

- E is isomorphic to a curve defined over $\mathbb{F}_{p^2}$;
- Every isogeny of E is defined over $\mathbb{F}_{p^2}$;
- Every endomorphism of E is defined over $\mathbb{F}_{p^2}$;
- $\mathrm{End}(E)$ is isomorphic to a maximal order in a quaternion algebra ramified at p and ∞.

In particular:

- If E is defined over $\mathbb{F}_p$, then $\mathrm{End}_{\mathbb{F}_p}(E)$ is strictly contained in $\mathrm{End}(E)$.
- Some endomorphisms do not commute!

An example

The curve of j-invariant 1728

$$E : y^2 = x^3 + x$$

is supersingular over $\mathbb{F}_p$ iff $p = -1 \mod 4$.

Endomorphisms

$\mathrm{End}(E) = \mathbb{Z}\langle \iota, \pi \rangle$, with:

- π the Frobenius endomorphism, s.t. $\pi^2 = -p$;
- ι the map

$$\iota(x, y) = (-x, iy),$$

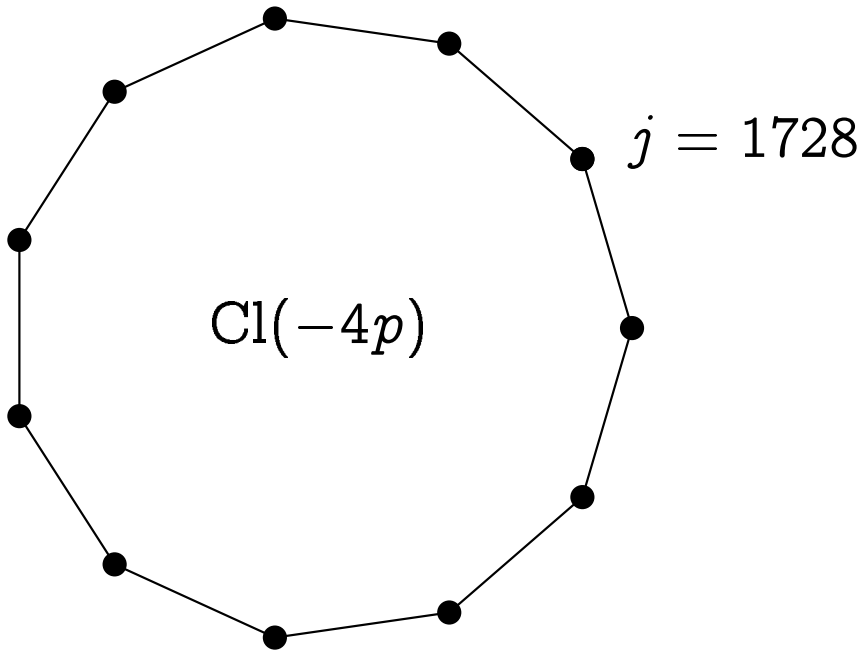
where $i \in \mathbb{F}_{p^2}$ is a 4-th root of unity. Clearly, $\iota^2 = -1$.

And $\iota\pi = -\pi\iota$.

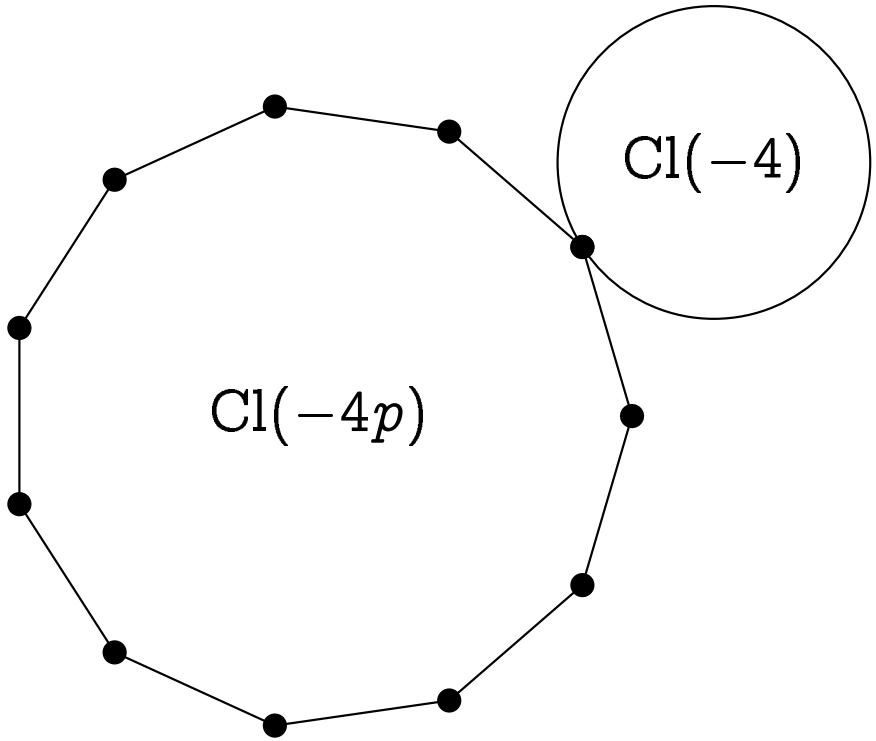
Class group action party

- $j = 1728$

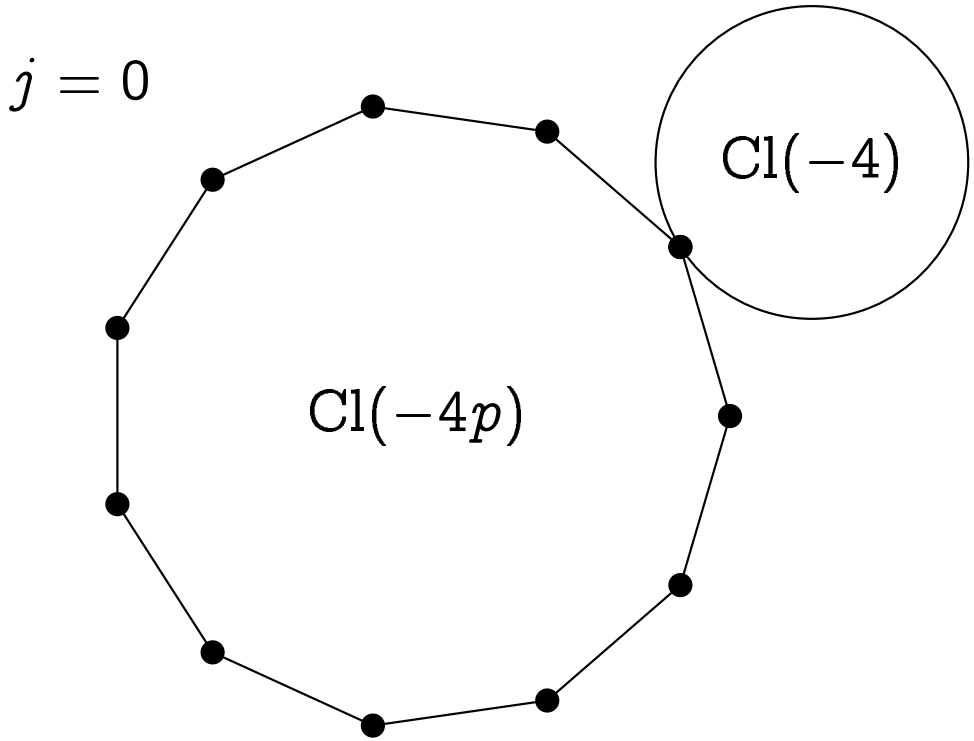
Class group action party



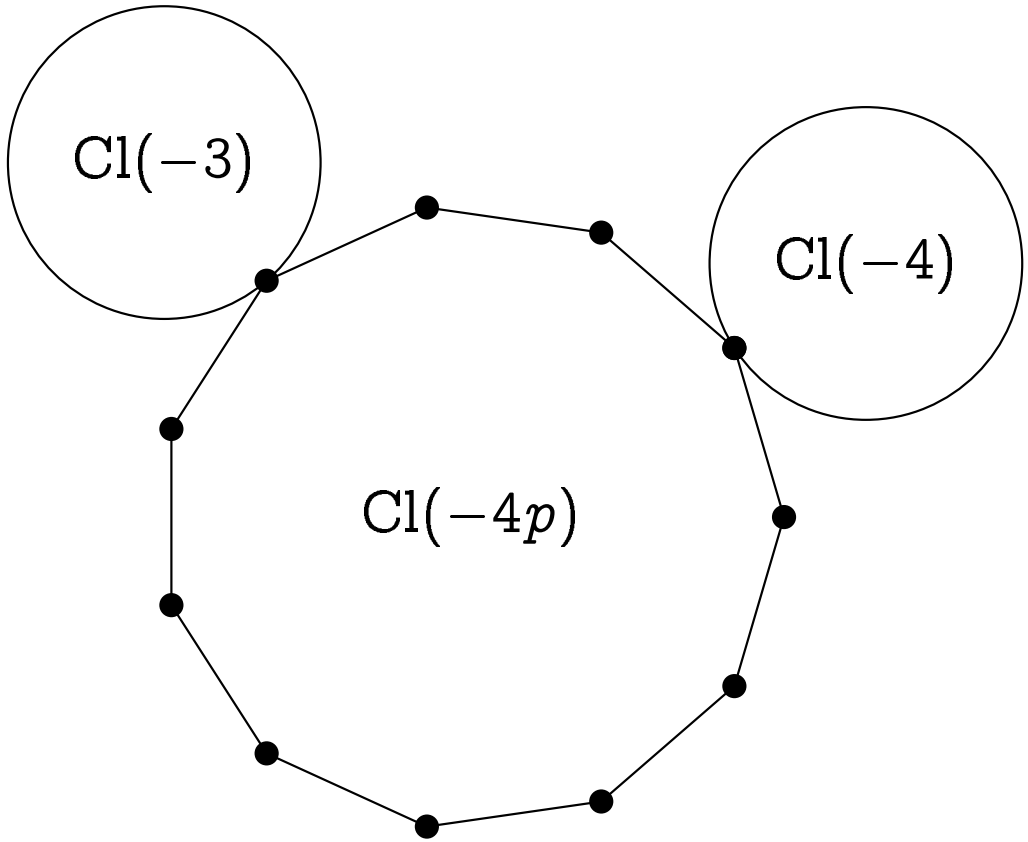
Class group action party



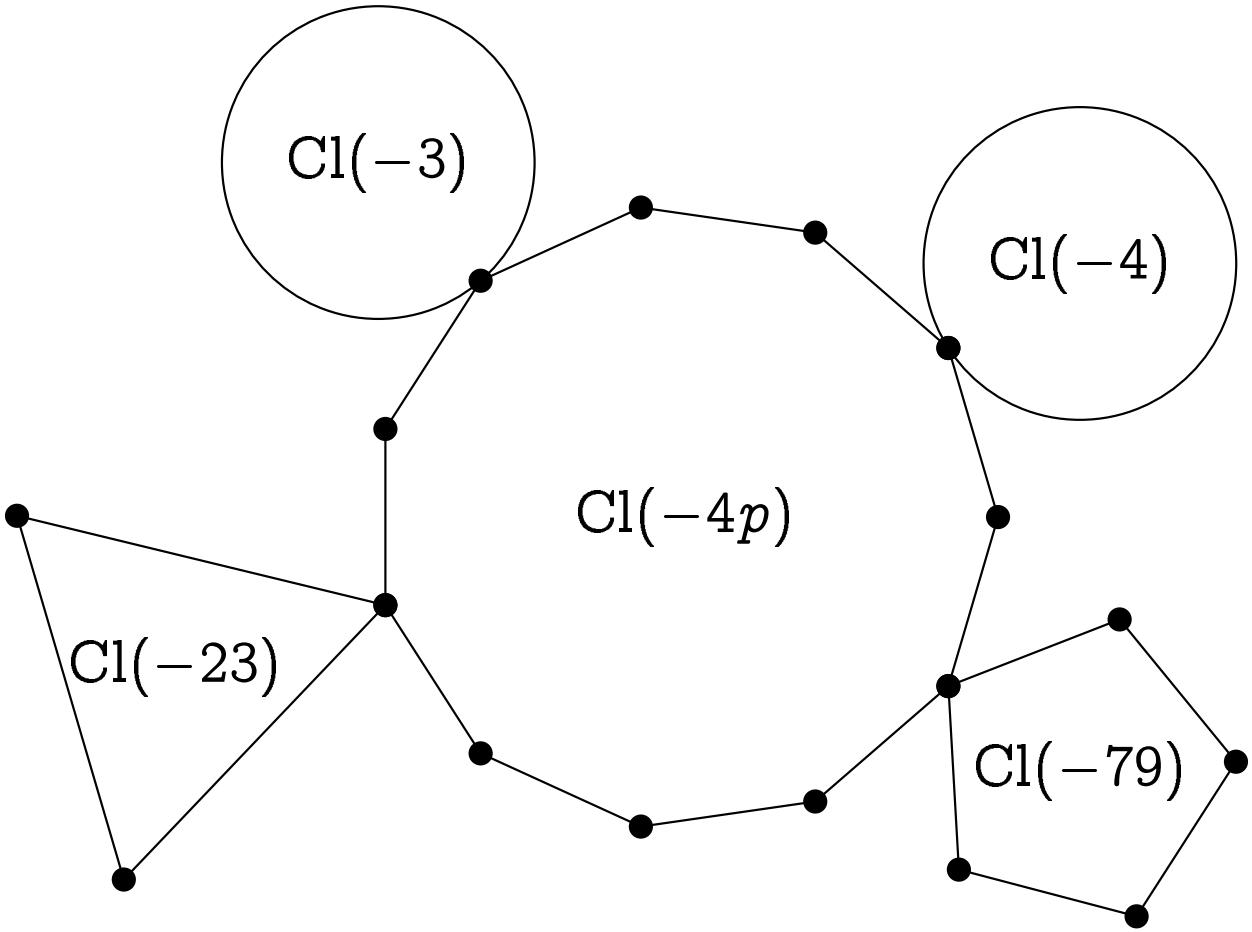
Class group action party



Class group action party



Class group action party



Quaternion algebra?! WTF?[2]

The quaternion algebra $B_{p,\infty}$ is:

- A 4-dimensional $\mathbb{Q}$-vector space with basis $(1, i, j, k)$.
- A non-commutative division algebra[1] $B_{p,\infty} = \mathbb{Q}\langle i, j \rangle$ with the relations:

$$i^2 = a, \quad j^2 = -p, \quad ij = -ji = k,$$

  for some $a < 0$ (depending on p).
- All elements of $B_{p,\infty}$ are quadratic algebraic numbers.
- $B_{p,\infty} \otimes \mathbb{Q}_\ell \simeq \mathcal{M}_{2\times 2}(\mathbb{Q}_\ell)$ for all $\ell \neq p$.
  I.e., endomorphisms restricted to $E[\ell^e]$ are just 2×2 matrices $\bmod \ell^e$.
- $B_{p,\infty} \otimes \mathbb{R}$ is isomorphic to Hamilton's quaternions.
- $B_{p,\infty} \otimes \mathbb{Q}_p$ is a division algebra.

[1] All elements have inverses.

[2] What The Field?

Supersingular graphs

- Quaternion algebras have many maximal orders.
- For every maximal order type of $B_{p,\infty}$ there are 1 or 2 curves over $\mathbb{F}_{p^2}$ having endomorphism ring isomorphic to it.
- There is a unique isogeny class of supersingular curves over $\bar{\mathbb{F}}_p$ of size $\approx p/12$.
- Left ideals act on the set of maximal orders like isogenies.
- The graph of ℓ-isogenies is $(\ell+1)$-regular.

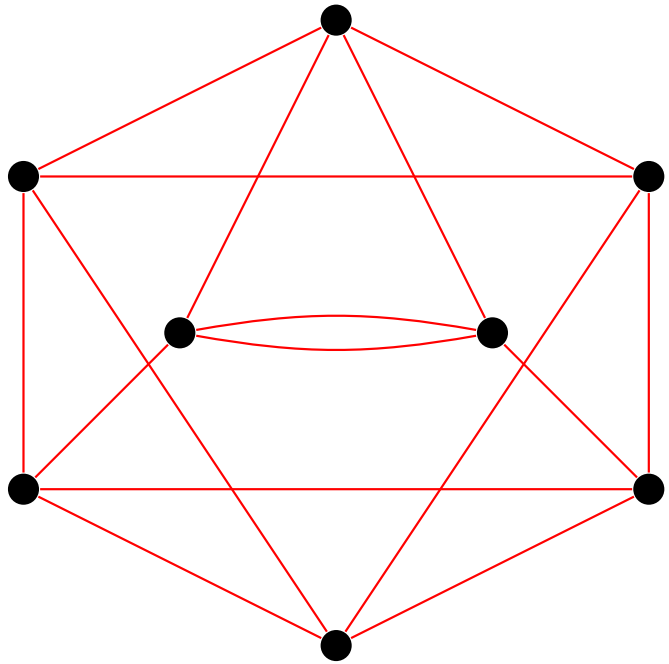


Figure: 3-isogeny graph on $\mathbb{F}_{97^2}$.

Graphs lexicon

Degree:	Number of (outgoing/ingoing) edges.
k-regular:	All vertices have degree k.
Connected:	There is a path between any two vertices.
Distance:	The length of the shortest path between two vertices.
Diameter:	The longest distance between two vertices.
$\lambda_1 \geq \cdots \geq \lambda_n$:	The (ordered) eigenvalues of the adjacency matrix.

Expander graphs

Proposition

If G is a k-regular graph, its largest and smallest eigenvalues satisfy

$$k = \lambda_1 \geq \lambda_n \geq -k.$$

Expander families

An infinite family of connected k-regular graphs on n vertices is an expander family if there exists an $\epsilon > 0$ such that all non-trivial eigenvalues satisfy $|\lambda| \leq (1 - \epsilon)k$ for n large enough.

- Expander graphs have short diameter ($O(\log n)$);
- Random walks mix rapidly (after $O(\log n)$ steps, the induced distribution on the vertices is close to uniform).

Expander graphs from isogenies

Theorem (Pizer)

Let ℓ be fixed. The family of graphs of supersingular curves over $\mathbb{F}_{p^2}$ with ℓ-isogenies, as $p \to \infty$, is an expander family[a].

[a] Even better, it has the Ramanujan property.

Theorem (Jao, Miller, Venkatesan)

Let $\mathcal{O} \subset \mathbb{Q}(\sqrt{-D})$ be an order in a quadratic imaginary field. The graphs of all curves over $\mathbb{F}_q$ with complex multiplication by $\mathcal{O}$, with isogenies of prime degree bounded[a] by $(\log q)^{2+\delta}$, are expanders.

[a] May contain traces of GRH.

Executive summary

- Separable ℓ-isogeny = finite kernel = subgroup of $E[\ell]$,
  - eigenspace of π iff $\mathbb{F}_q$-rational,
  - distinct eigenvalues $\lambda \neq \mu$ define distinct directions on the crater.
- Isogeny graphs have j-invariants for vertices and "some" isogenies for edges.
- By varying the choices for the vertex and the isogeny set, we obtain graphs with different properties.
- ℓ-isogeny graphs of ordinary curves are volcanoes, (full) ℓ-isogeny graphs of supersingular curves are finite $(\ell + 1)$-regular.
- CM theory naturally leads to define graphs of horizontal isogenies (both in the ordinary and the supersingular case) that are isomorphic to Cayley graphs of class groups.
- CM graphs are expanders. Supersingular full ℓ-isogeny graphs are Ramanujan.

Thank you

https://defeo.lu/

@luca_defeo

Weil pairing

Let $(N, p) = 1$, fix any basis $E[N] = \langle R, S \rangle$. For any points $P, Q \in E[N]$

$$P = aR + bS$$
$$Q = cR + dS$$

the form $\det_N(P, Q) = \det \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = ad - bc \in \mathbb{Z}/N\mathbb{Z}$
is bilinear, non-degenerate, and independent from the choice of basis.

Theorem

Let $E/\mathbb{F}_q$ be a curve, there exists a Galois invariant bilinear map

$$e_N : E[N] \times E[N] \longrightarrow \mu_N \subset \bar{\mathbb{F}}_q,$$

called the Weil pairing of order N, and a primitive N-th root of unity $\zeta \in \bar{\mathbb{F}}_q$ such that

$$e_N(P, Q) = \zeta^{\det_N(P,Q)}.$$

The degree k of the smallest extension such that $\zeta \in \mathbb{F}_{q^k}$ is called the embedding degree of the pairing.

Weil pairing and isogenies

Note

The Weil pairing is Galois invariant $\Leftrightarrow$ $\det(\pi|E[N]) = q$.

Theorem

Let $\phi : E \to E'$ be an isogeny and $\hat{\phi} : E' \to E$ its dual.
Let e_N be the Weil pairing of E and e'_N that of E'. Then, for

$$e_N(P, \hat{\phi}(Q)) = e'_N(\phi(P), Q),$$

for any $P \in E[N]$ and $Q \in E'[N]$.

Corollary

$$e'_N(\phi(P), \phi(Q)) = e_N(P, Q)^{\deg \phi}.$$