Isogeny graphs in cryptography

Luca De Feo

Université Paris Saclay, UVSQ & Inria

March 19–23, 2018, Post-Scryptum Spring School, Les 7 Laux

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

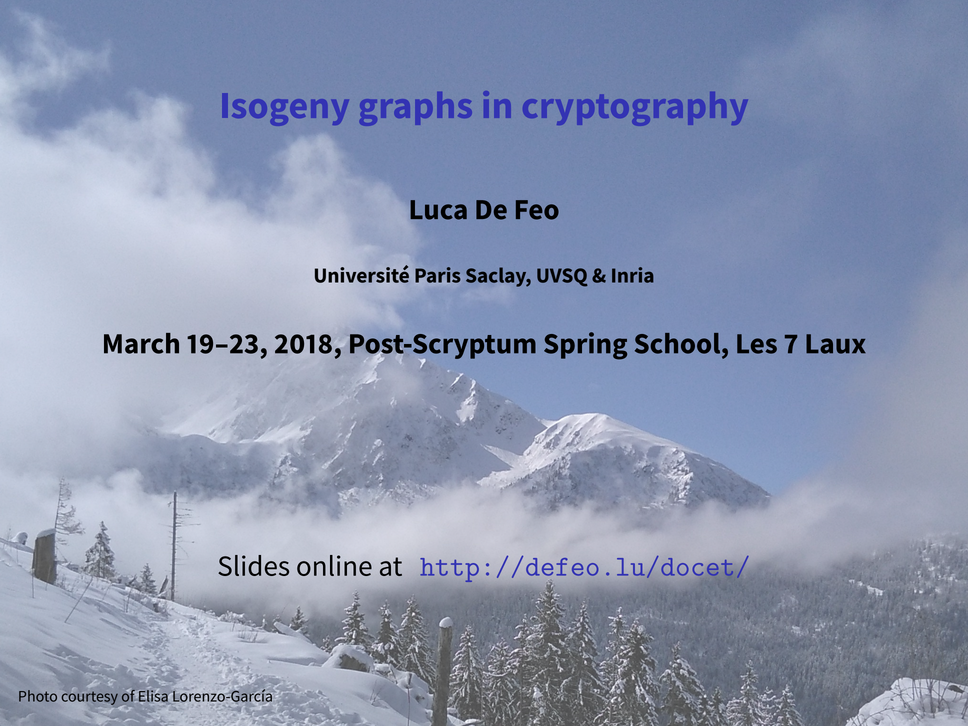


Photo courtesy of Elisa Lorenzo-García

Overview

1. Foundations
   - Elliptic curves
   - Isogenies
   - Complex multiplication

2. Isogeny-based cryptography
   - Isogeny walks
   - Key exchange from ordinary graphs
   - Key exchange from supersingular graphs

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 $(x_0, \dots, x_n) \in \bar{k}^n$ modulo the equivalence relation

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

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

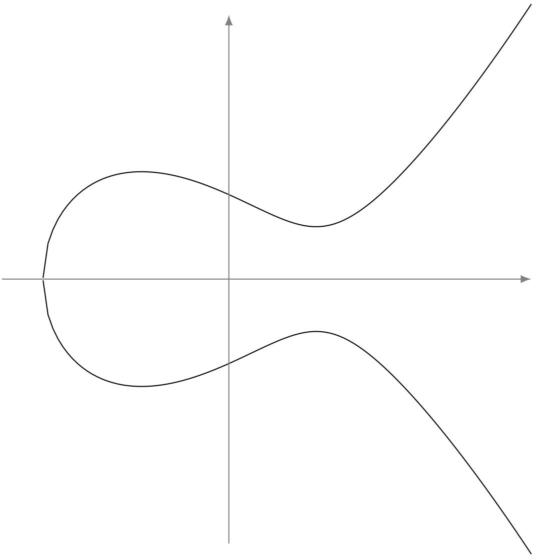
Picture here

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 $4a^3 + 27b^2 \neq 0$.



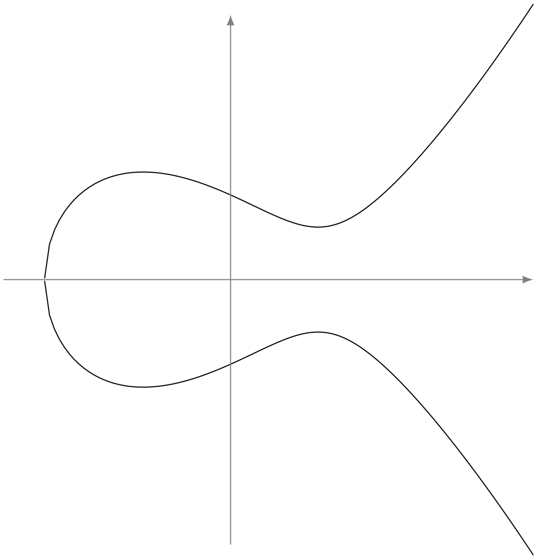
Weierstrass equations

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;



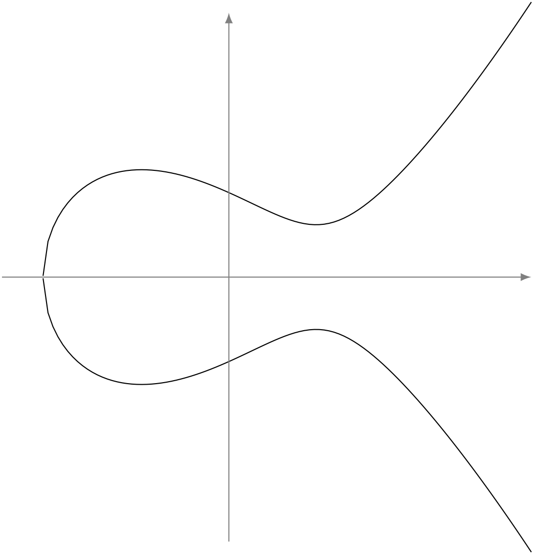
Weierstrass equations

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.

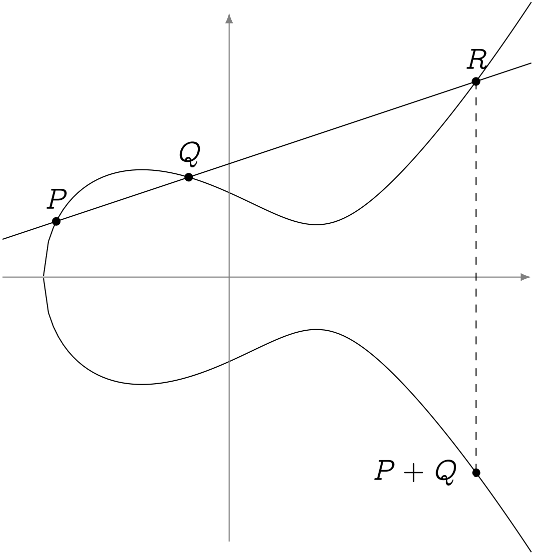


The group law

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.



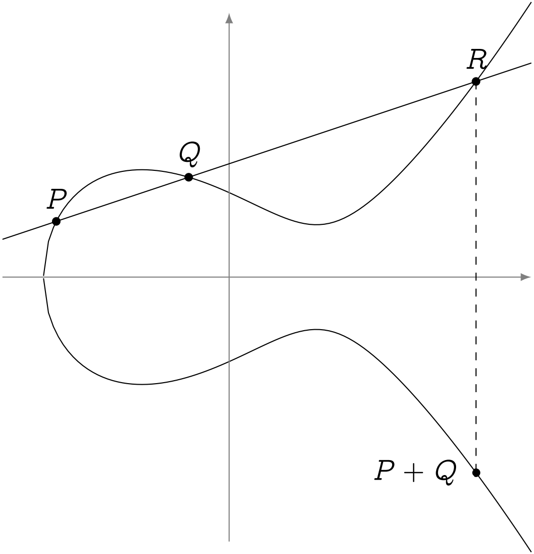
The group law

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*);



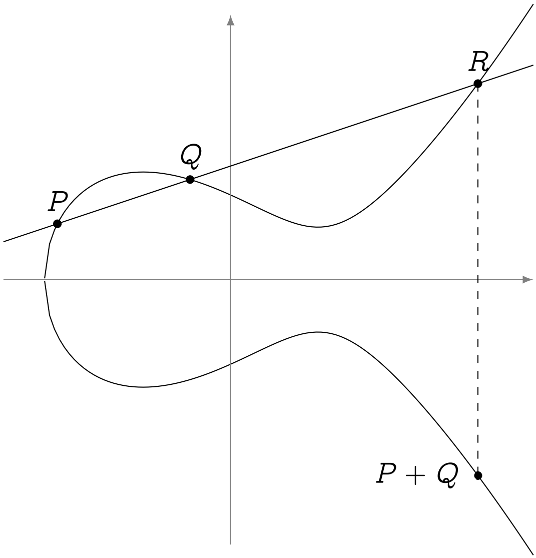
The group law

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.



Group structure

Torsion structure

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

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

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

Free part

Let E be defined over a number field k, the group of k-rational points $E(k)$ is finitely generated.

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 $j(E) = j(E')$.

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.

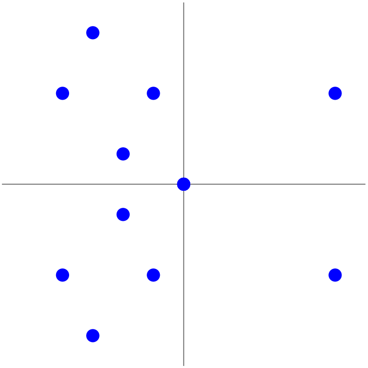
Example: Multiplication-by-m

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

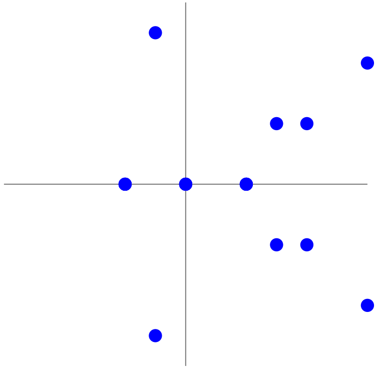
$$\begin{aligned}[m] \ :\ E &\to E,\\ P &\mapsto [m]P.\end{aligned}$$

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

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



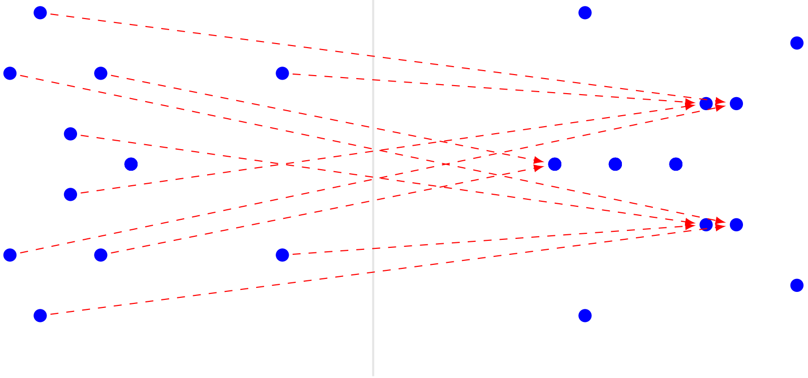
$$E' \;:\; y^2 = x^3 - 4x$$



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

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

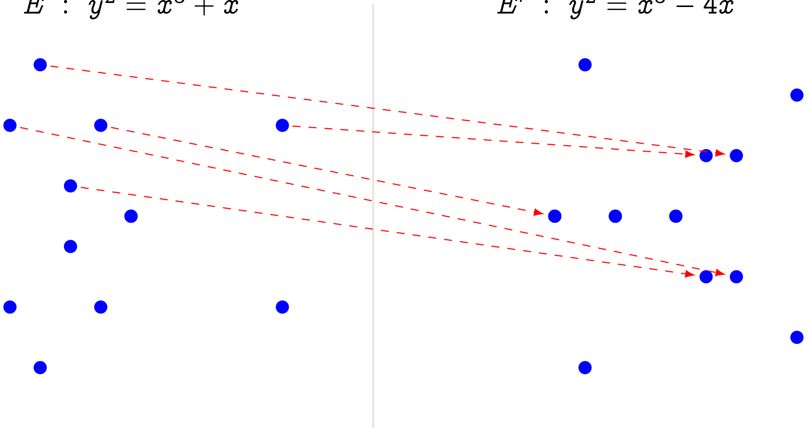
$E \; : \; y^2 = x^3 + x$ $\qquad$ $E' \; : \; y^2 = x^3 - 4x$



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

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

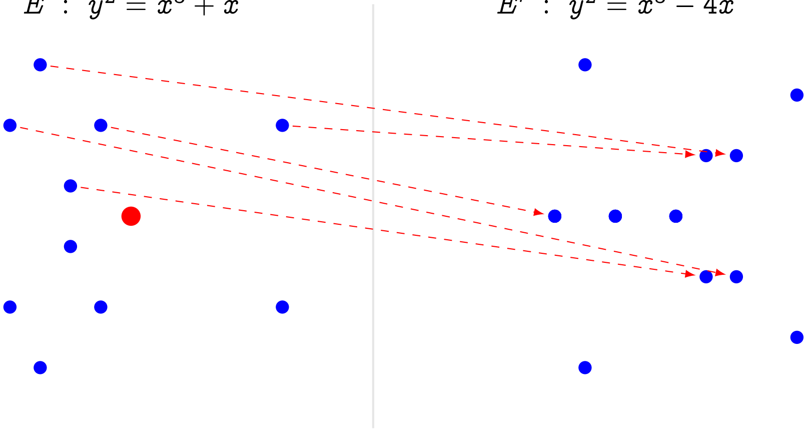
$E \ : \ y^2 = x^3 + x$ $\qquad\qquad$ $E' \ : \ y^2 = x^3 - 4x$



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

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

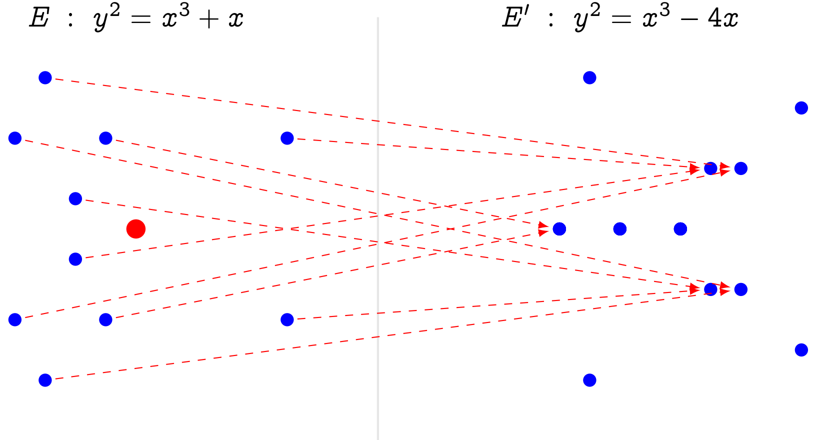
$E : y^2 = x^3 + x$ $\qquad$ $E' : y^2 = x^3 - 4x$



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

- Kernel generator in red.

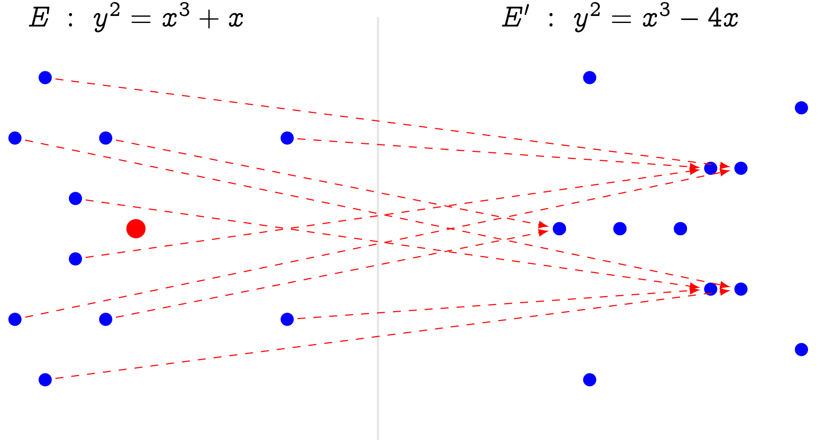
Isogenies: an example over $\mathbb{F}_{11}$



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

- Kernel generator in red.
- This is a degree 2 map.

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



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

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

Curves over finite fields

Frobenius endomorphism

Let E be defined over $\mathbb{F}_q$. The Frobenius endomorphism of E is the map

$$\pi \; : \; (X : Y : Z) \mapsto (X^q : Y^q : Z^q).$$

Hasse's theorem

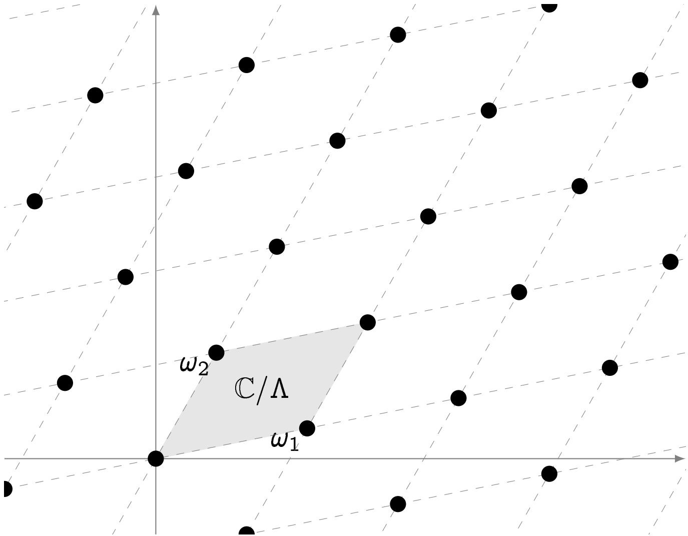
Let E be defined over $\mathbb{F}_q$, then

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

Serre-Tate theorem

Two elliptic curves E, E' defined over a finite field k are isogenous over k if and only if $\#E(k) = \#E'(k)$.

Complex tori

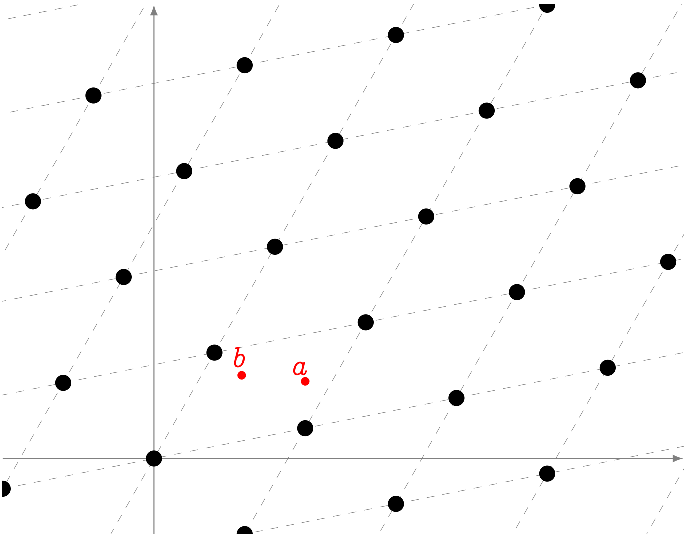


Let $\omega_1, \omega_2 \in \mathbb{C}$ be linearly independent complex numbers. Set

$$\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$$

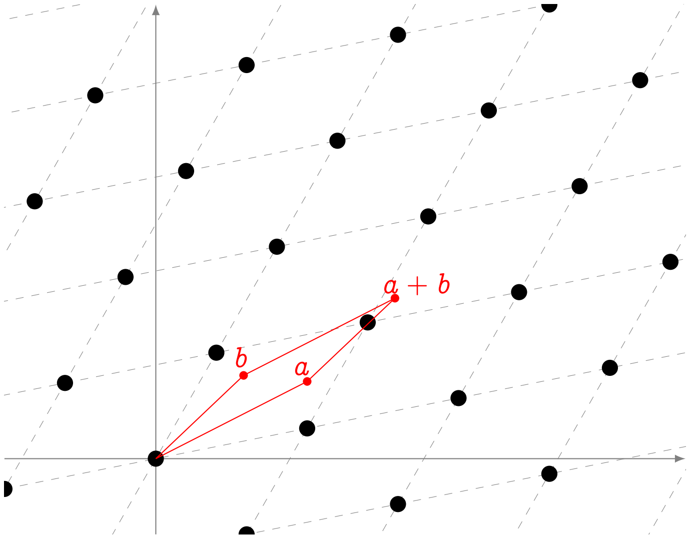
$\mathbb{C}/\Lambda$ is a complex torus.

Complex tori



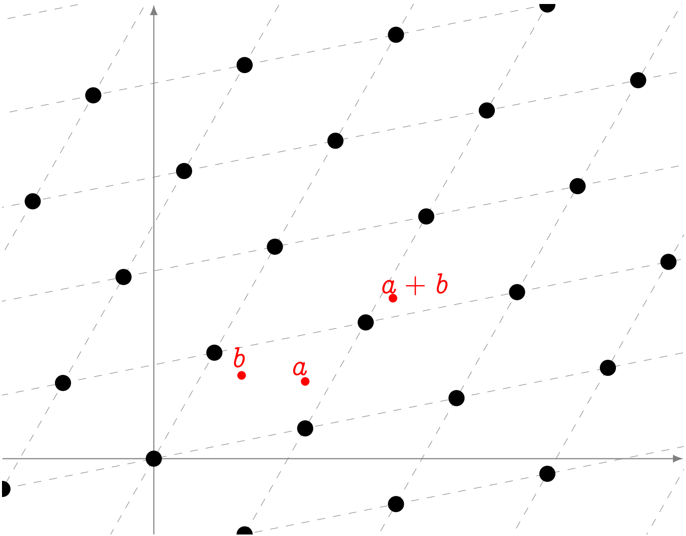
Addition law induced by addition on $\mathbb{C}$.

Complex tori



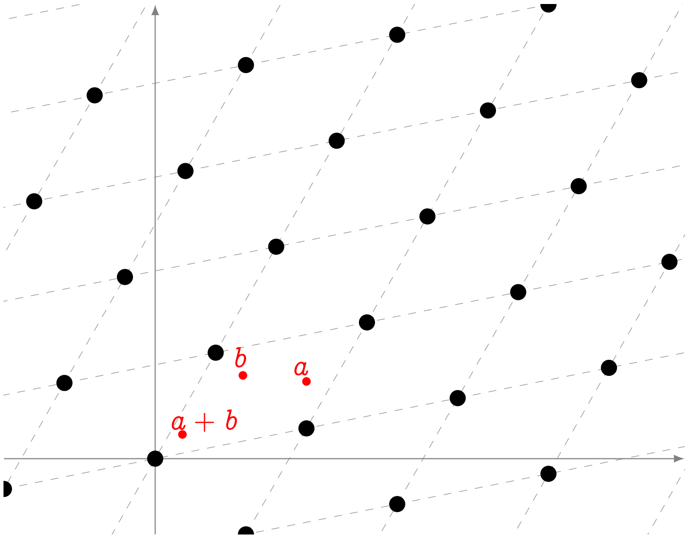
Addition law induced by addition on $\mathbb{C}$.

Complex tori



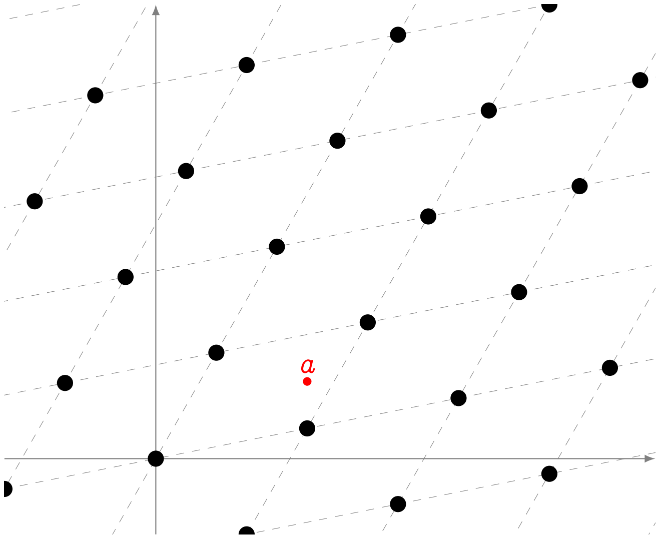
Addition law induced by addition on $\mathbb{C}$.

Complex tori



Addition law induced by addition on $\mathbb{C}$.

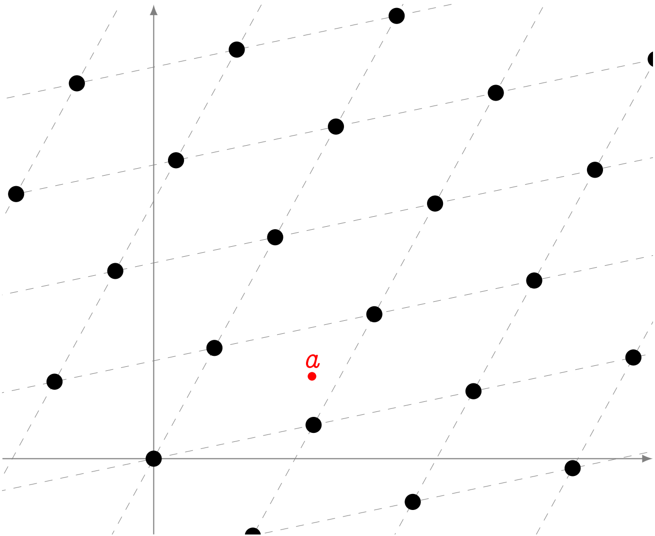
Homotheties



Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

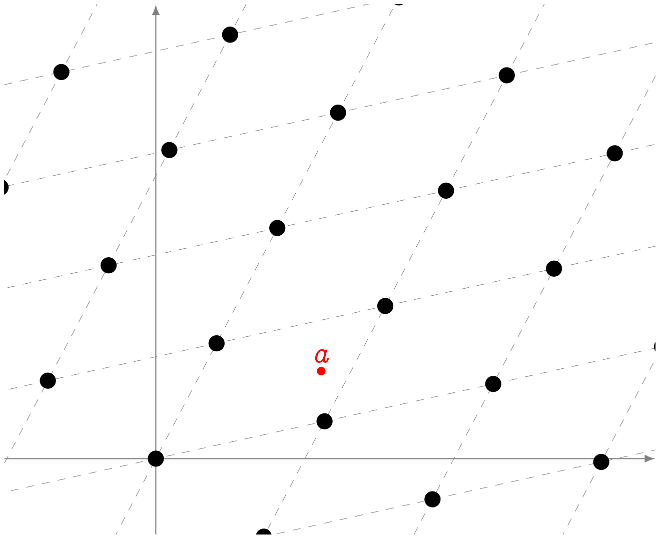
Homotheties



Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

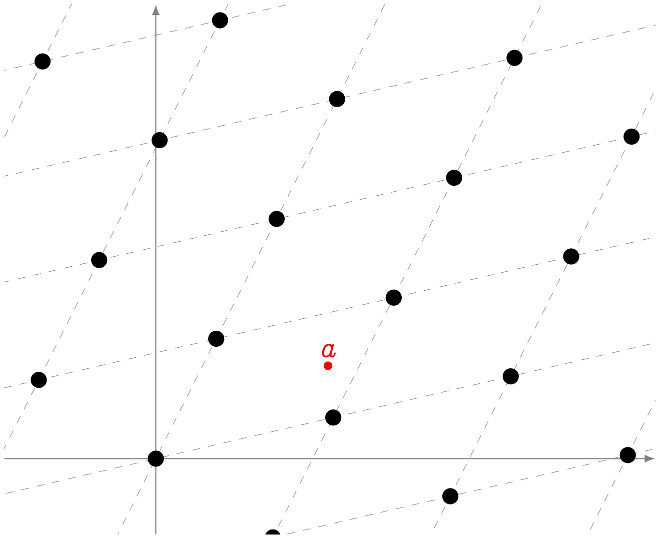
Homotheties



Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

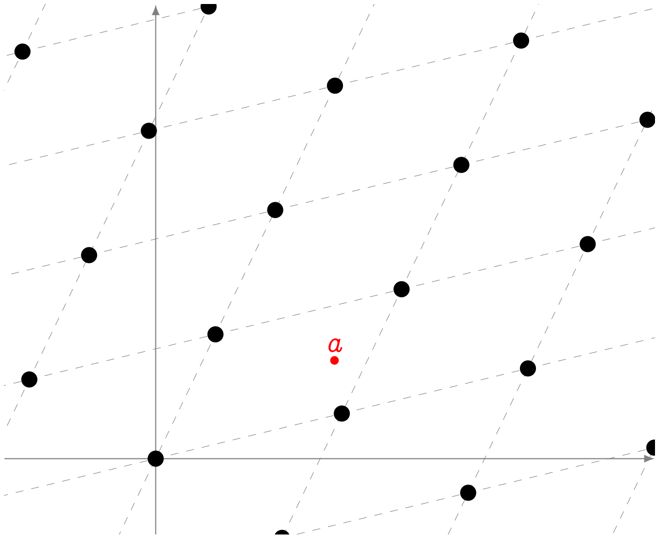
Homotheties



Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

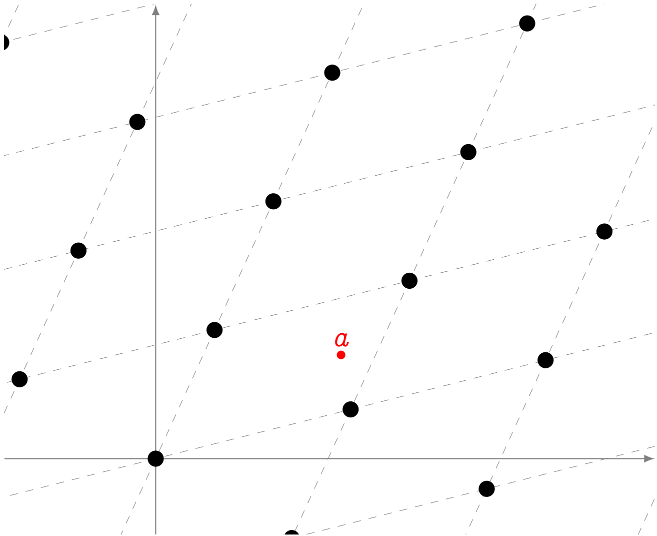
Homotheties



Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

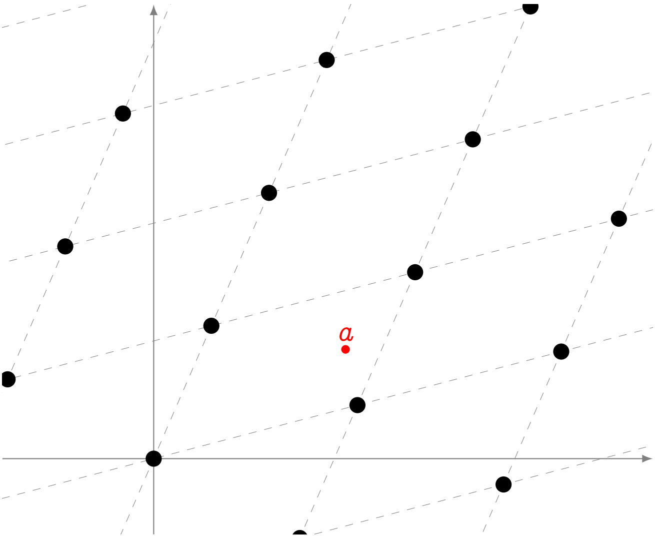
Homotheties



Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

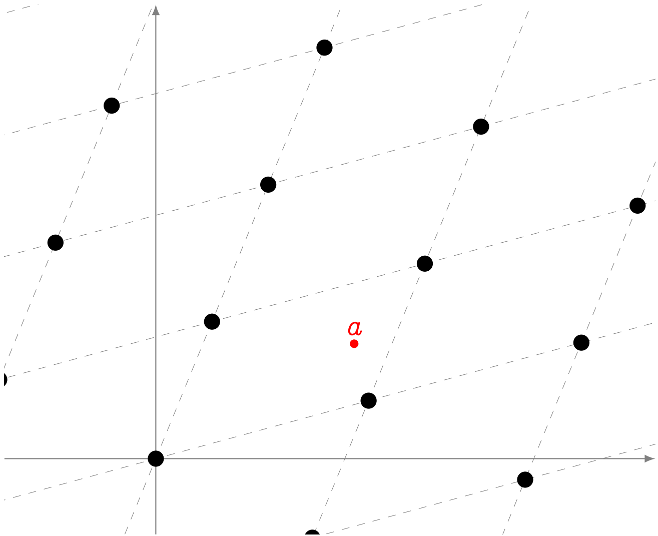
Homotheties



Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

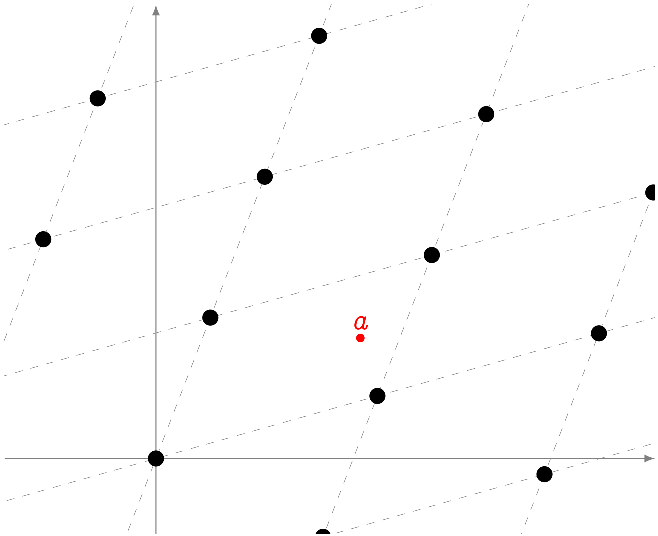
Homotheties



Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

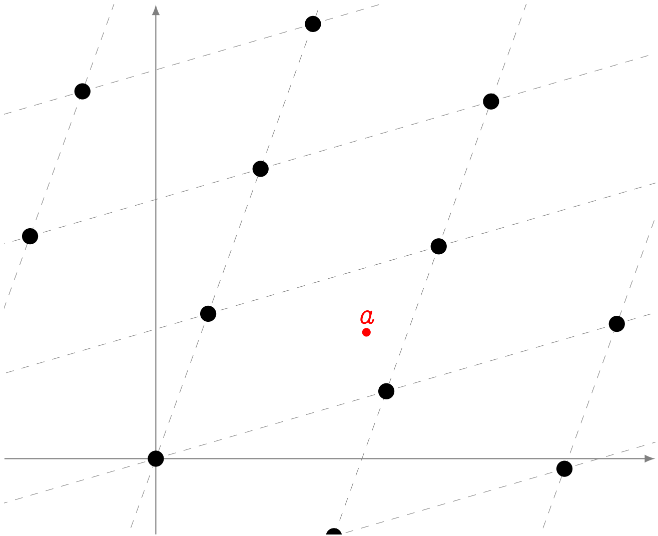
Homotheties



Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

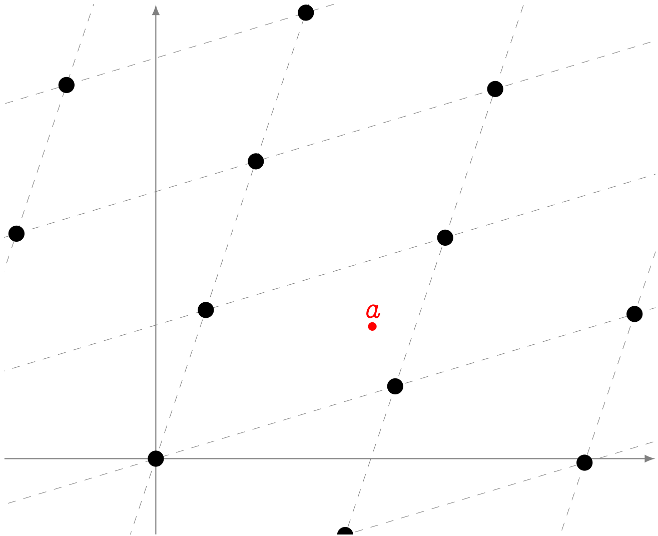
Homotheties



Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

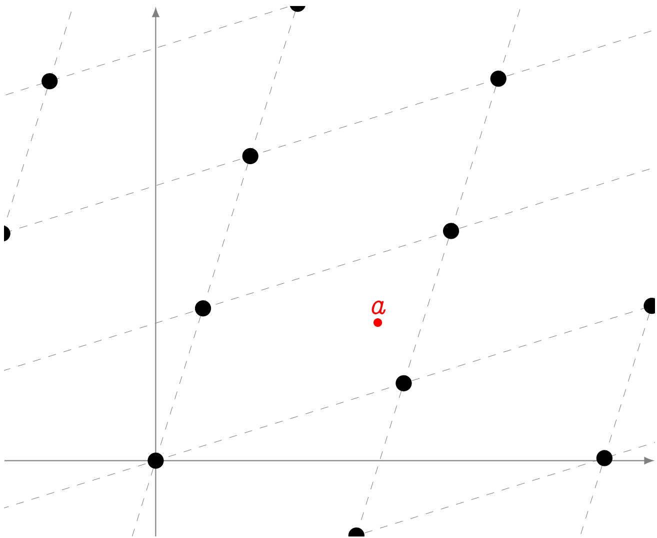
Homotheties



Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

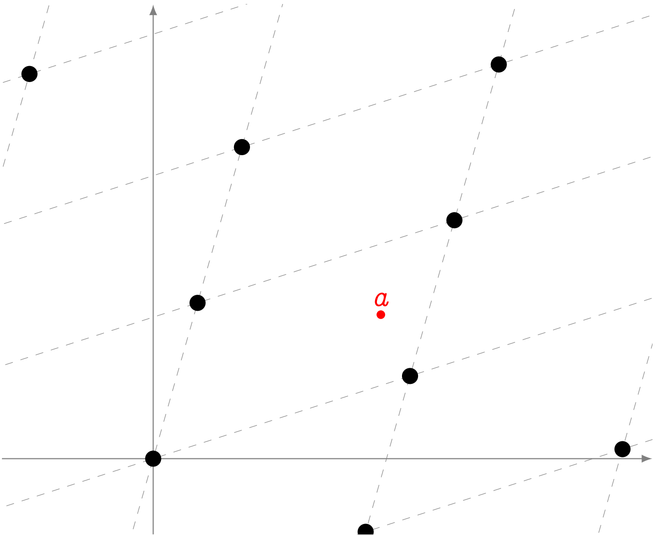
Homotheties



Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

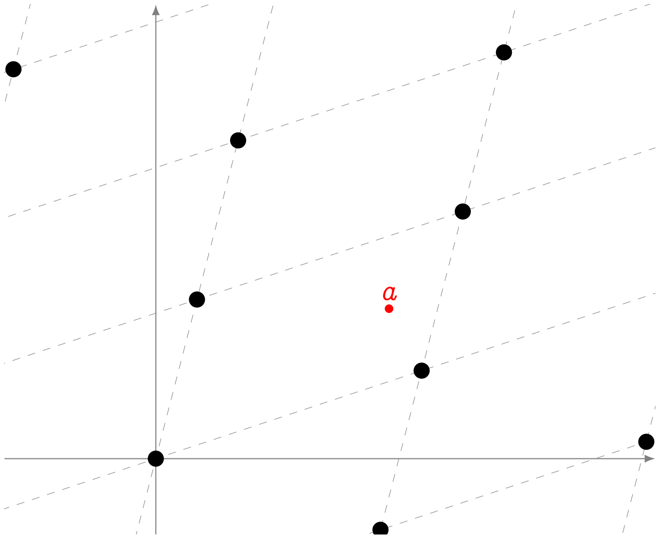
Homotheties



Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

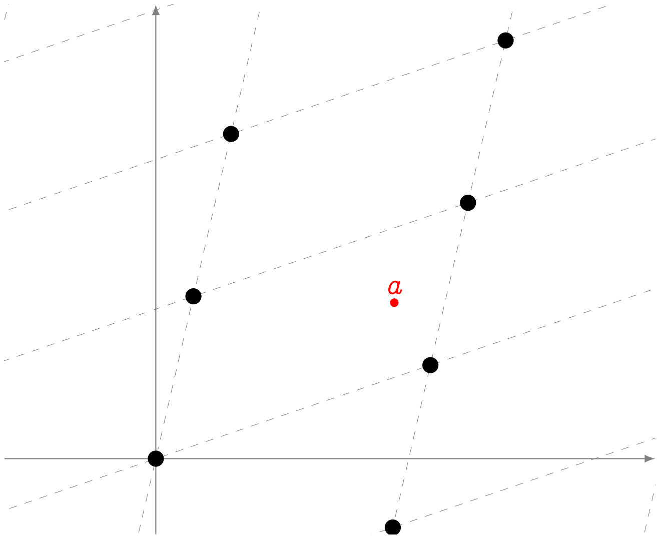
Homotheties



Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

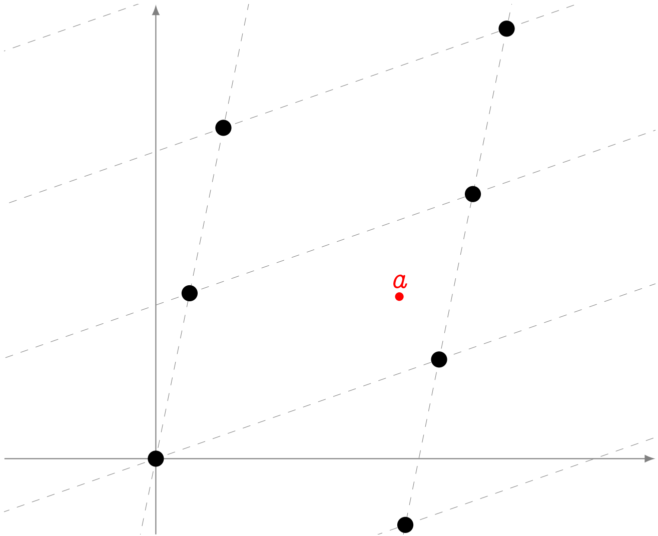
Homotheties



Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

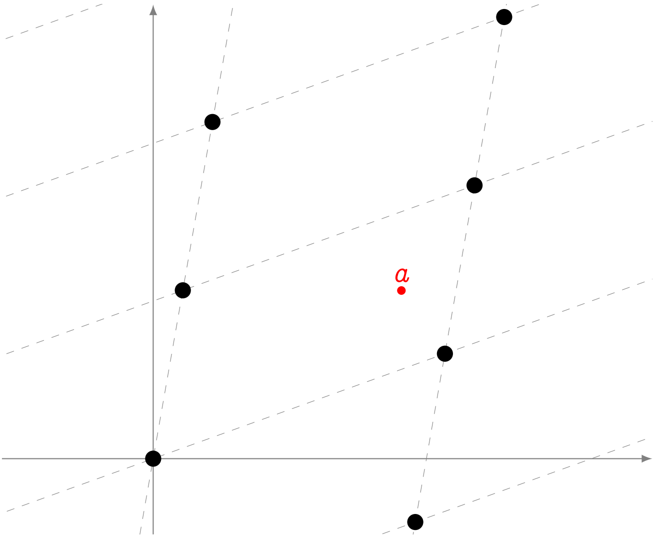
Homotheties



Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

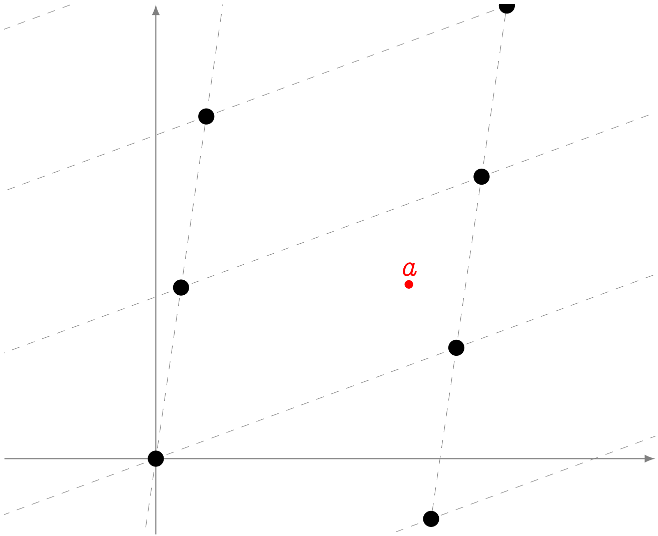
Homotheties



Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

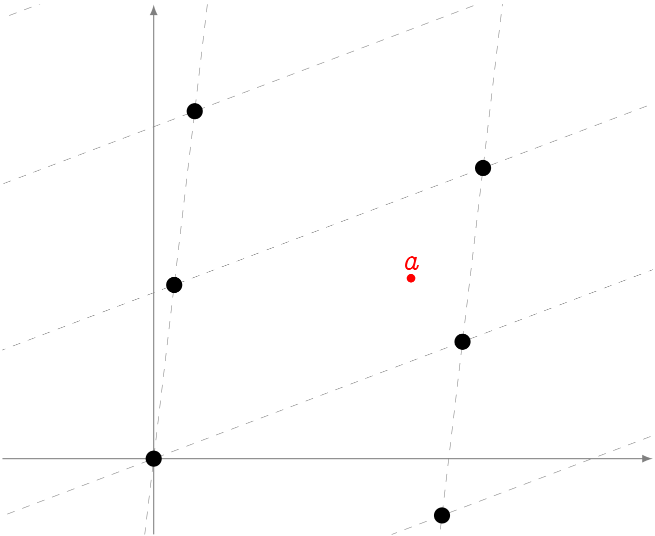
Homotheties



Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

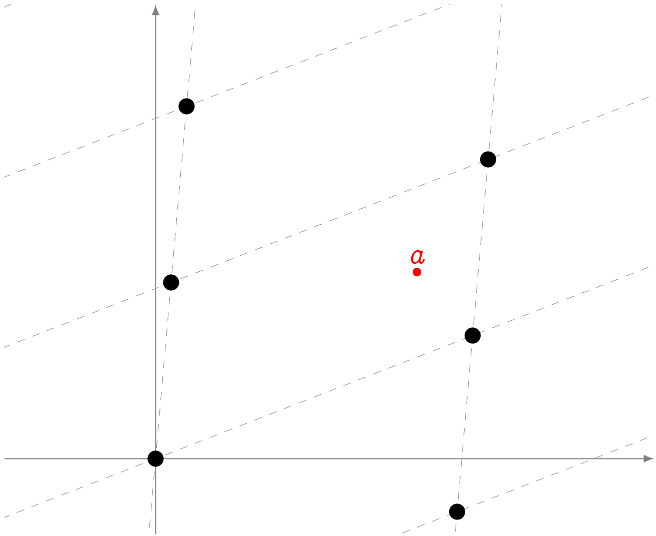
Homotheties



Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

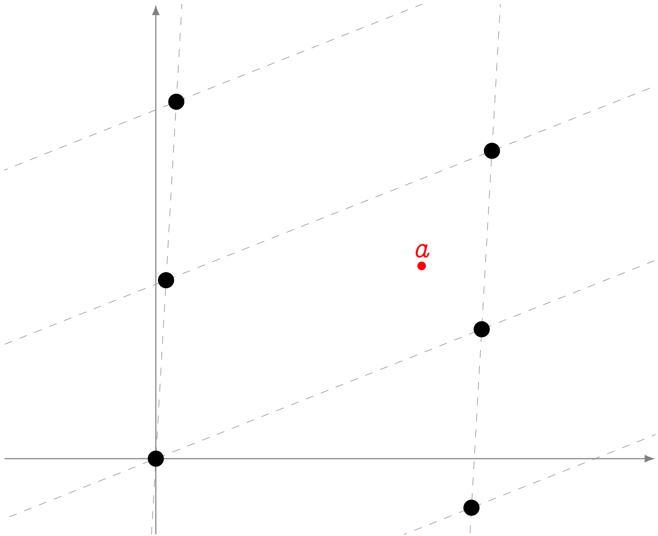
Homotheties



Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

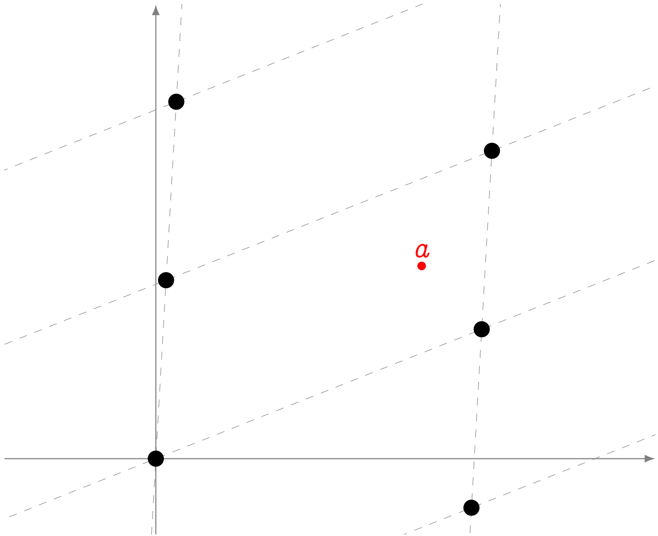
Homotheties



Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

Homotheties



Two lattices are homotetic if there exist $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2$$

The j-invariant

We want to classify complex lattices/tori up to homothety.

Eisenstein series

Let Λ be a complex lattice. For any integer $k > 0$ define

$$G_{2k}(\Lambda) = \sum_{\omega\in\Lambda\setminus\{0\}} \omega^{-2k}.$$

Also set

$$g_2(\Lambda) = 60\,G_4(\Lambda), \qquad g_3(\Lambda) = 140\,G_6(\Lambda).$$

Modular j-invariant

Let Λ be a complex lattice, the modular j-invariant is

$$j(\Lambda) = 1728\frac{g_2(\Lambda)^3}{g_2(\Lambda)^3 - 27g_3(\Lambda)^2}.$$

Two lattices Λ, Λ' are homothetic if and only if $j(\Lambda) = j(\Lambda')$.

Elliptic curves over $\mathbb{C}$

Weierstrass $\wp$ function

Let Λ be a complex lattice, the Weierstrass $\wp$ function associated to Λ is the series

$$\wp(z;\Lambda) = \frac{1}{z^2} + \sum_{\omega\in\Lambda\setminus\{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right).$$

Fix a lattice Λ, then $\wp$ and its derivative $\wp'$ are elliptic functions:

$$\wp(z+\omega) = \wp(z), \qquad \wp'(z+\omega) = \wp'(z)$$

for all $\omega \in \Lambda$.

Uniformization theorem

Let Λ be a complex lattice. The curve

$$E \ : \ y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$$

is an elliptic curve over $\mathbb{C}$. The map

$$\begin{aligned} \mathbb{C}/\Lambda &\to E(\mathbb{C}), \\ 0 &\mapsto (0:1:0), \\ z &\mapsto (\wp(z):\wp'(z):1) \end{aligned}$$

is an isomorphism of Riemann surfaces and a group morphism.

Conversely, for any elliptic curve

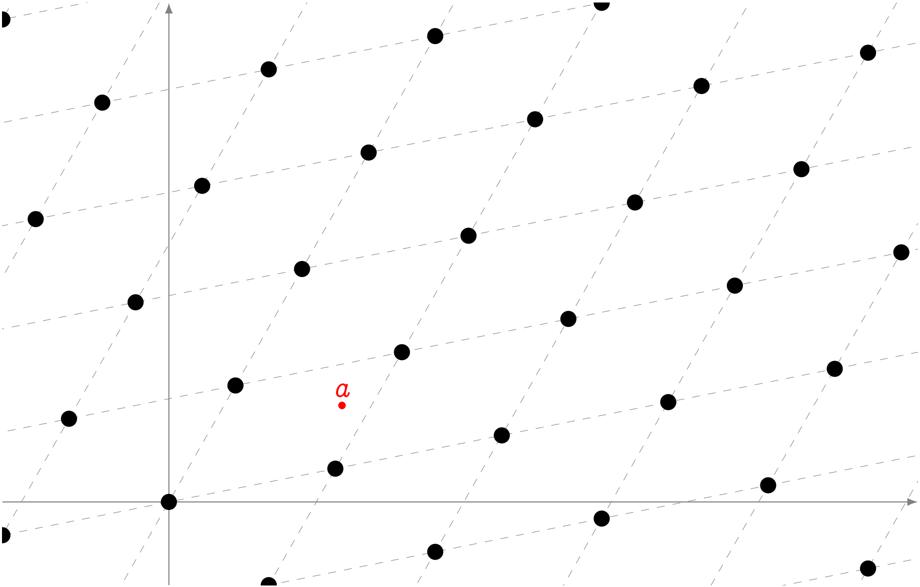
$$E \ : \ y^2 = x^3 + ax + b$$

there is a unique complex lattice Λ such that

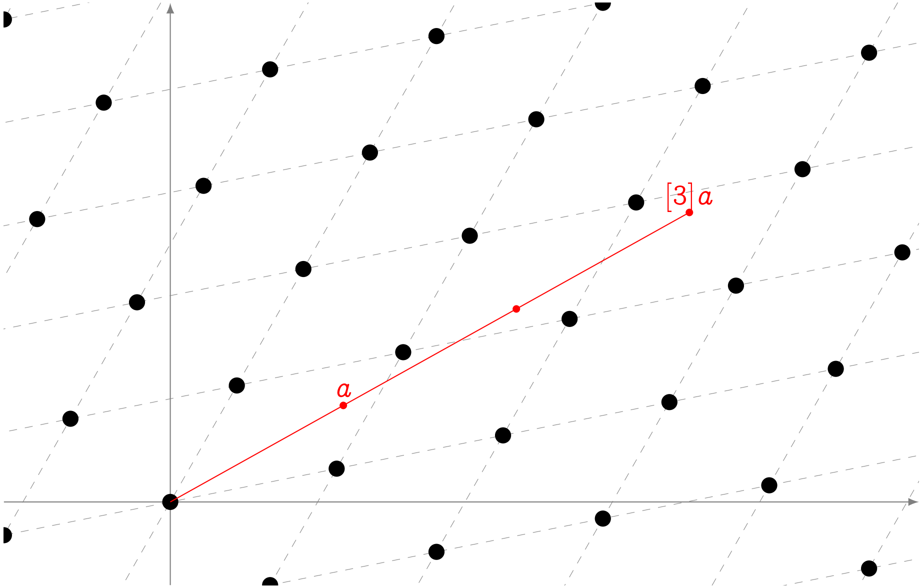
$$g_2(\Lambda) = -4a, \qquad g_3(\Lambda) = -4b.$$

Moreover $j(\Lambda) = j(E)$.

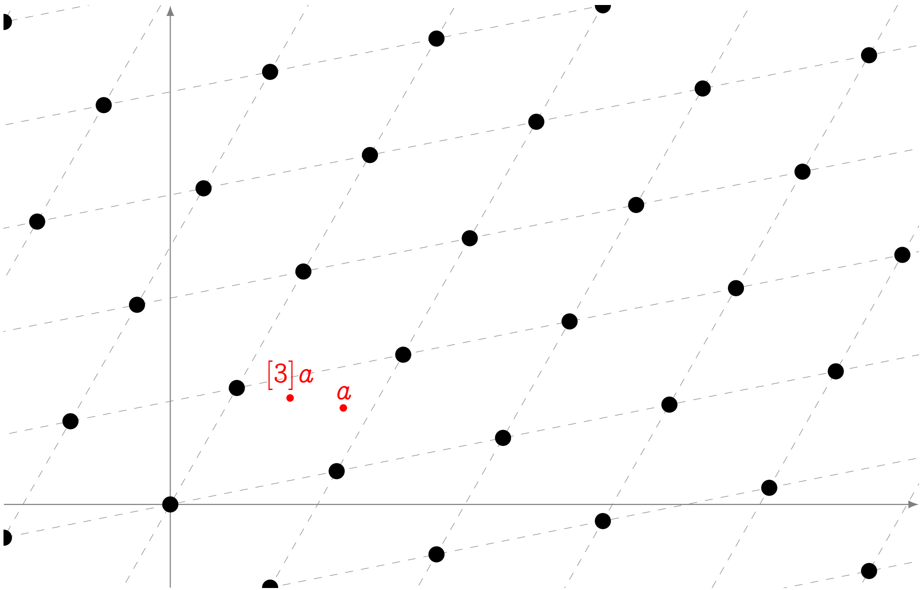
Multiplication



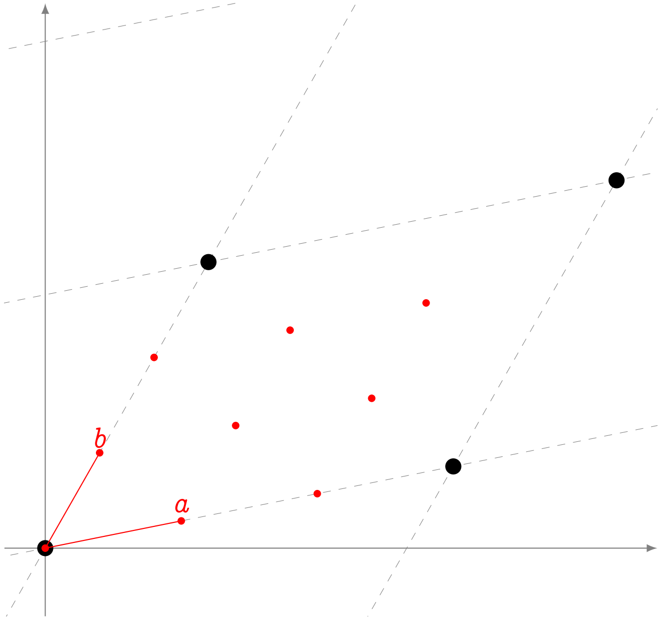
Multiplication



Multiplication



Torsion subgroups



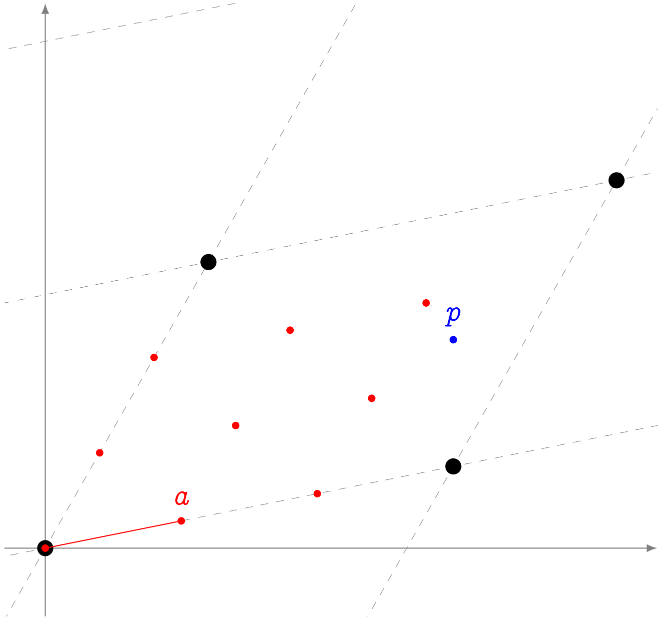
The ℓ-torsion subgroup is made up by the points

$$\left(\frac{i\omega_1}{\ell}, \frac{j\omega_2}{\ell}\right)$$

It is a group of rank two

$$\begin{aligned} E[\ell] &= \langle a, b \rangle \\ &\simeq (\mathbb{Z}/\ell\mathbb{Z})^2 \end{aligned}$$

Isogenies



Let $a \in \mathbb{C}/\Lambda_1$ be an ℓ-torsion point, and let

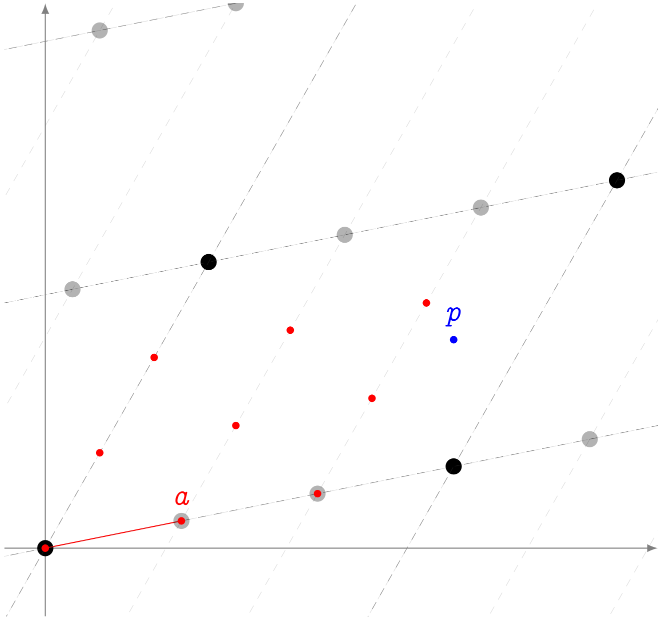
$$\Lambda_2 = a\mathbb{Z} \oplus \Lambda_1$$

Then $\Lambda_1 \subset \Lambda_2$ and we define a degree ℓ cover

$$\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$$

ϕ is a morphism of complex Lie groups and is called an isogeny.

Isogenies



Let $a \in \mathbb{C}/\Lambda_1$ be an ℓ-torsion point, and let

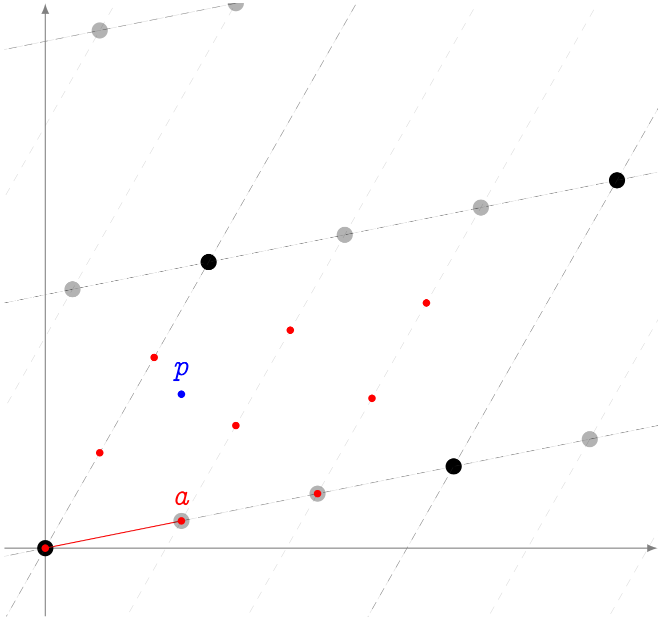
$$\Lambda_2 = a\mathbb{Z} \oplus \Lambda_1$$

Then $\Lambda_1 \subset \Lambda_2$ and we define a degree ℓ cover

$$\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$$

ϕ is a morphism of complex Lie groups and is called an isogeny.

Isogenies



Let $a \in \mathbb{C}/\Lambda_1$ be an ℓ-torsion point, and let

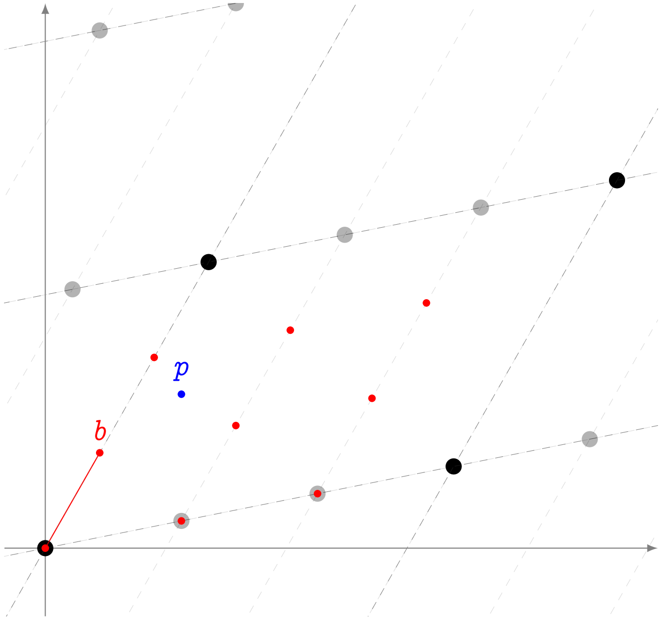
$$\Lambda_2 = a\mathbb{Z} \oplus \Lambda_1$$

Then $\Lambda_1 \subset \Lambda_2$ and we define a degree ℓ cover

$$\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$$

ϕ is a morphism of complex Lie groups and is called an isogeny.

Isogenies



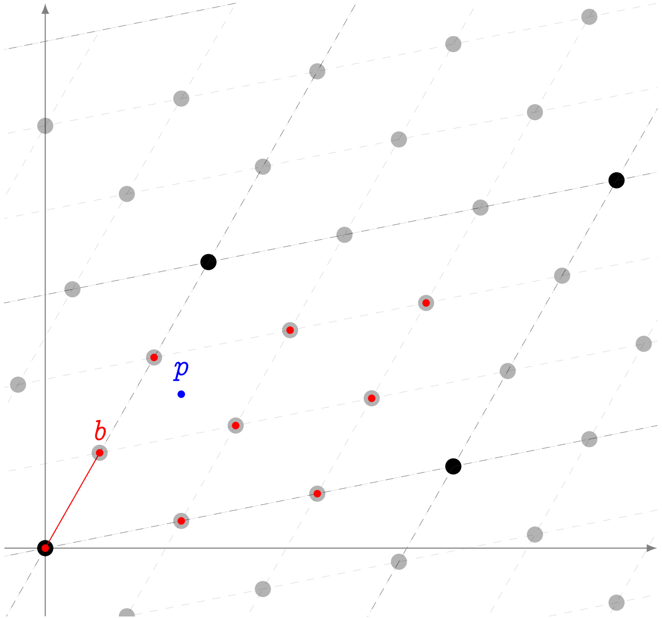
Taking a point b not in the kernel of ϕ, we obtain a new degree ℓ cover

$$\hat{\phi} : \mathbb{C}/\Lambda_2 \to \mathbb{C}/\Lambda_3$$

The composition $\hat{\phi} \circ \phi$ has degree ℓ^2 and is homothetic to the multiplication by ℓ map.

$\hat{\phi}$ is called the dual isogeny of ϕ.

Isogenies



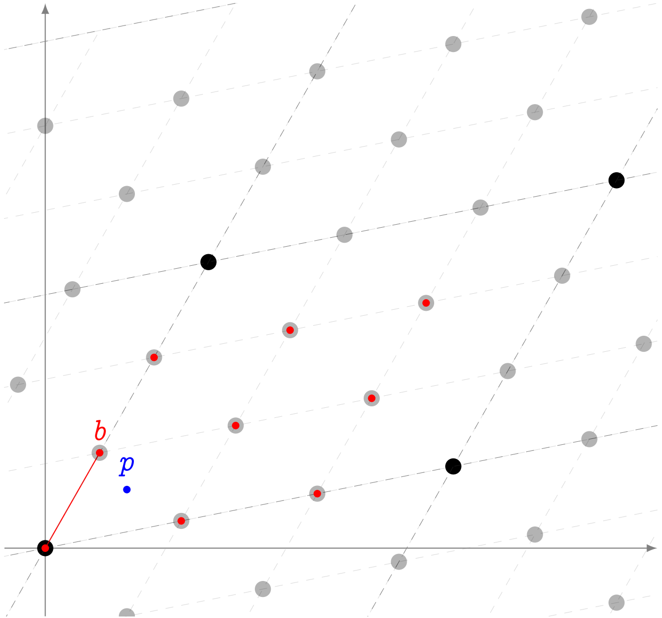
Taking a point b not in the kernel of ϕ, we obtain a new degree ℓ cover

$$\hat{\phi} : \mathbb{C}/\Lambda_2 \to \mathbb{C}/\Lambda_3$$

The composition $\hat{\phi} \circ \phi$ has degree ℓ^2 and is homothetic to the multiplication by ℓ map.

$\hat{\phi}$ is called the dual isogeny of ϕ.

Isogenies



Taking a point b not in the kernel of ϕ, we obtain a new degree ℓ cover

$$\hat{\phi} : \mathbb{C}/\Lambda_2 \to \mathbb{C}/\Lambda_3$$

The composition $\hat{\phi} \circ \phi$ has degree ℓ^2 and is homothetic to the multiplication by ℓ map.
$\hat{\phi}$ is called the dual isogeny of ϕ.

Isogenies: back to algebra

Let $\phi : E \to E'$ be an isogeny defined over a field k of characteristic p.

- $k(E)$ is the field of all rational functions from E to k;
- $\phi^* k(E')$ is the subfield of $k(E)$ defined as

$$\phi^* k(E') = \{f \circ \phi \mid f \in k(E')\}.$$

Degree, separability

1. The degree of ϕ is $\deg \phi = [k(E) : \phi^* k(E')]$. It is always finite.
2. ϕ is said to be separable, inseparable, or purely inseparable if the extension of function fields is.
3. If ϕ is separable, then $\deg \phi = \# \ker \phi$.
4. If ϕ is purely inseparable, then $\ker \phi = \{\mathcal{O}\}$ and $\deg \phi$ is a power of p.
5. Any isogeny can be decomposed as a product of a separable and a purely inseparable isogeny.

Isogenies: back to algebra

Let $\phi : E \to E'$ be an isogeny defined over a field k of characteristic p.

- $k(E)$ is the field of all rational functions from E to k;
- $\phi^* k(E')$ is the subfield of $k(E)$ defined as

$$\phi^* k(E') = \{f \circ \phi \mid f \in k(E')\}.$$

Degree, separability

1. The degree of ϕ is $\deg \phi = [k(E) : \phi^* k(E')]$. It is always finite.
2. ϕ is said to be separable, inseparable, or purely inseparable if the extension of function fields is.
3. If ϕ is separable, then $\deg \phi = \# \ker \phi$.
4. If ϕ is purely inseparable, then $\ker \phi = \{\mathcal{O}\}$ and $\deg \phi$ is a power of p.
5. Any isogeny can be decomposed as a product of a separable and a purely inseparable isogeny.

Isogenies: separable vs inseparable

Purely inseparable isogenies

Examples:

- The Frobenius endomorphism is purely inseparable of degree q.
- All purely inseparable maps in characteristic p are of the form $(X:Y:Z) \mapsto (X^{p^e}:Y^{p^e}:Z^{p^e})$.

Separable isogenies

Let E be an elliptic curve, and let G be a finite subgroup of E. There are a unique elliptic curve E' and a unique separable isogeny ϕ, such that $\ker\phi = G$ and $\phi : E \to E'$.
The curve E' is called the quotient of E by G and is denoted by E/G.

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. $\hat{\hat{\phi}} = \phi$.

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 $\mathrm{End}(E)$ 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. $\mathrm{End}(E)$ 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.

Isogeny volcanoes

Serre-Tate theorem reloaded

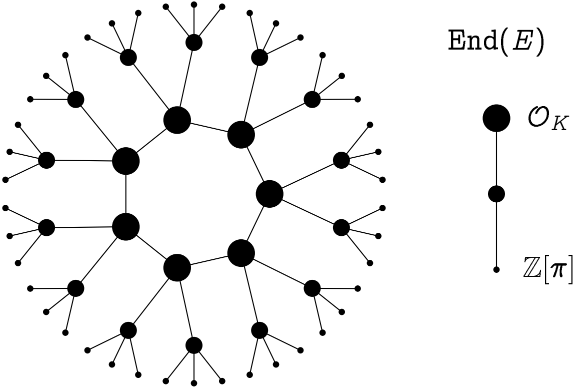
Two elliptic curves E, E' defined over a finite field are isogenous iff their endomorphism algebras $\mathrm{End}(E) \otimes \mathbb{Q}$ and $\mathrm{End}(E') \otimes \mathbb{Q}$ are isomorphic.

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.



Isogeny volcano of degree $\ell = 3$.

Isogeny volcanoes

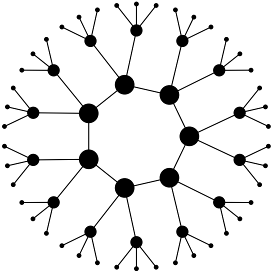
Classifying quadratic orders

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

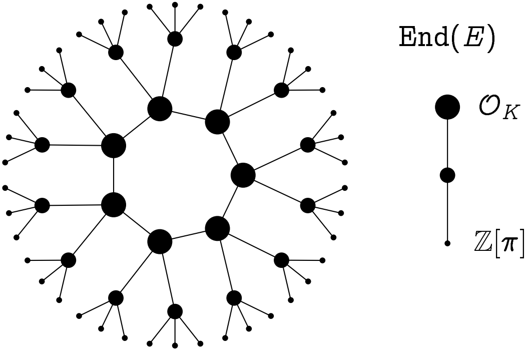
- Any order $\mathcal{O} \subset K$ can be written as $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$ for an integer f, called the conductor of $\mathcal{O}$, denoted by $[\mathcal{O}_k : \mathcal{O}]$.
- If d_K is the discriminant of K, the discriminant of $\mathcal{O}$ is $f^2 d_K$.
- If $\mathcal{O},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

Let E, E' be curves with respective endomorphism rings $\mathcal{O}, \mathcal{O}'$.
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.



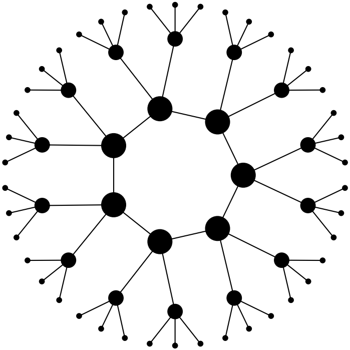
Volcanology

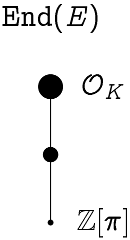


		Horizontal	Ascending	Descending
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$	$1 + \left(\frac{D_K}{\ell}\right)$		
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$	$1 + \left(\frac{D_K}{\ell}\right)$		$\ell - \left(\frac{D_K}{\ell}\right)$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

Volcanology

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



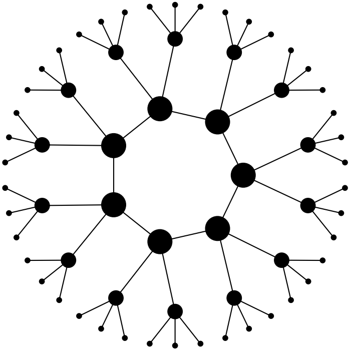


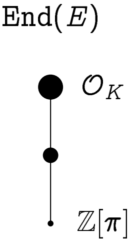
		Horizontal	Ascending	Descending
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \nmid [\mathcal{O} : \mathbb{Z}[\pi]]$	$1 + \left(\frac{D_K}{\ell}\right)$		
$\ell \nmid [\mathcal{O}_K : \mathcal{O}]$	$\ell \mid [\mathcal{O} : \mathbb{Z}[\pi]]$	$1 + \left(\frac{D_K}{\ell}\right)$		$\ell - \left(\frac{D_K}{\ell}\right)$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

Volcanology

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

How large is the crater?





		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	

The class group

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

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

- 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

If E is on the crater of an ℓ volcano, the crater contains $h(\mathrm{End}(E))$ curves.

Supersingular graphs

- Every supersingular curve is defined over $\mathbb{F}_{p^2}$.
- For every maximal order type of the quaternion algebra $\mathbb{Q}_{p,\infty}$ 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 $\sim p/12$.
- Left ideals act on the set of maximal orders like isogenies.
- The graph of ℓ-isogenies is $(\ell + 1)$-regular.

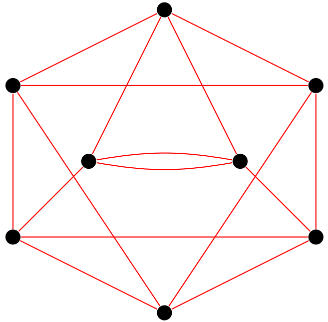


Figure: 3-isogeny graph on $\mathbb{F}_{97^2}$.

Thank you

http://defeo.lu/

@luca_defeo