Expander properties of superspecial digraphs

Krijn Reijnders
CRYPTO 2026

KU LEUVEN

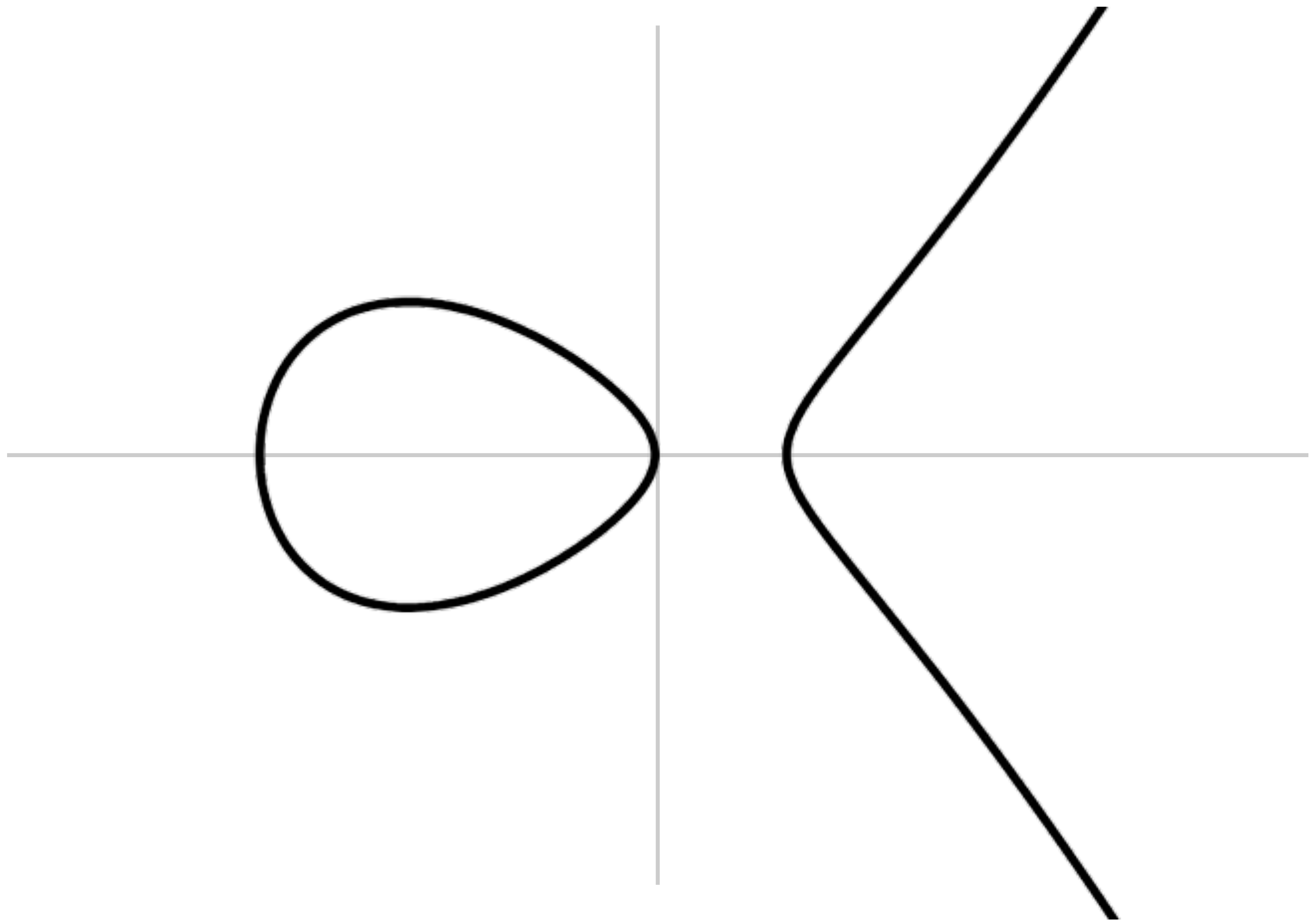
https://eprint.iacr.org/2026/500

Joint work with **Thomas Decru**

Dimension

1

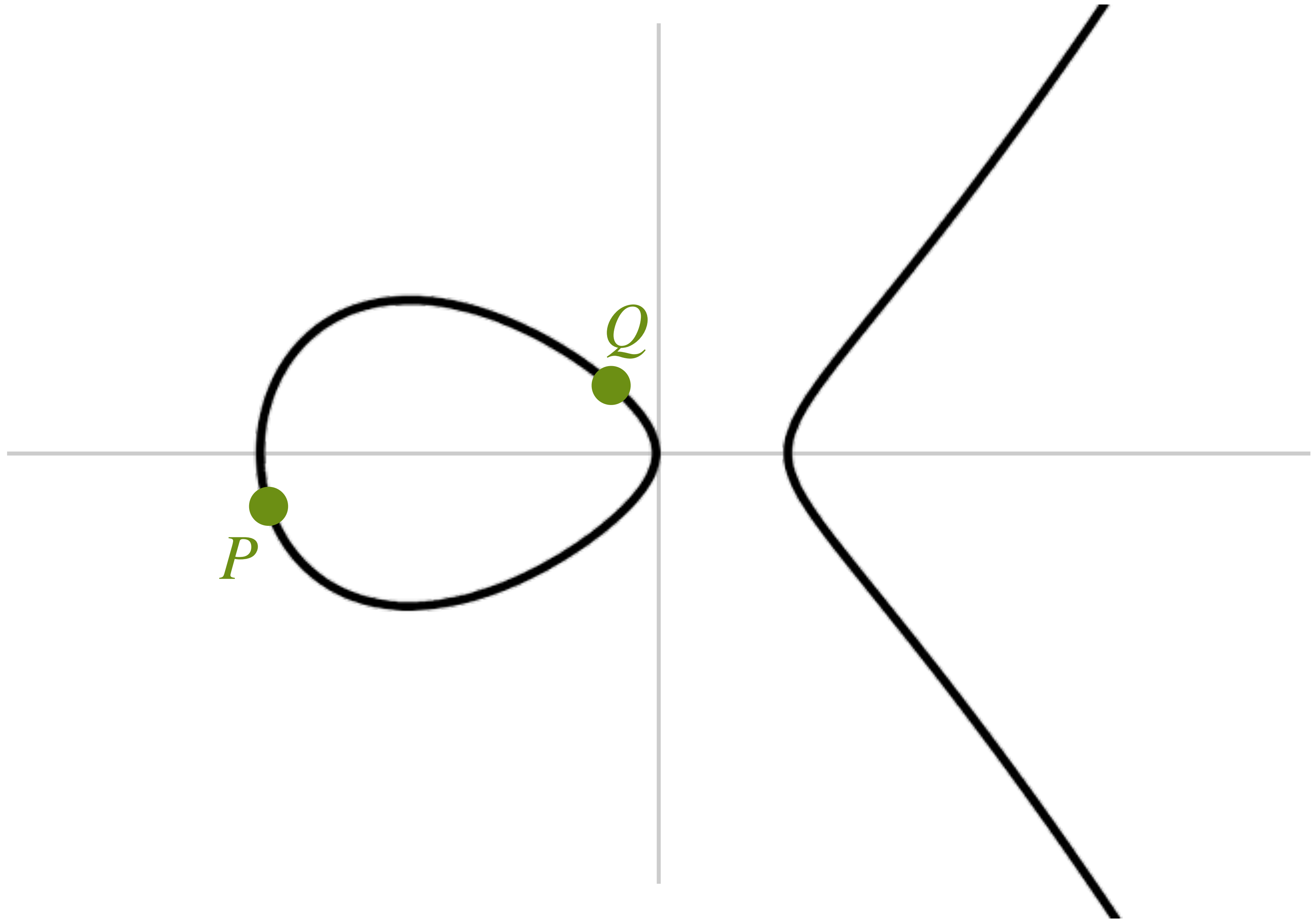
$$E : y^2 = x^3 + ax + b$$



Dimension

1

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

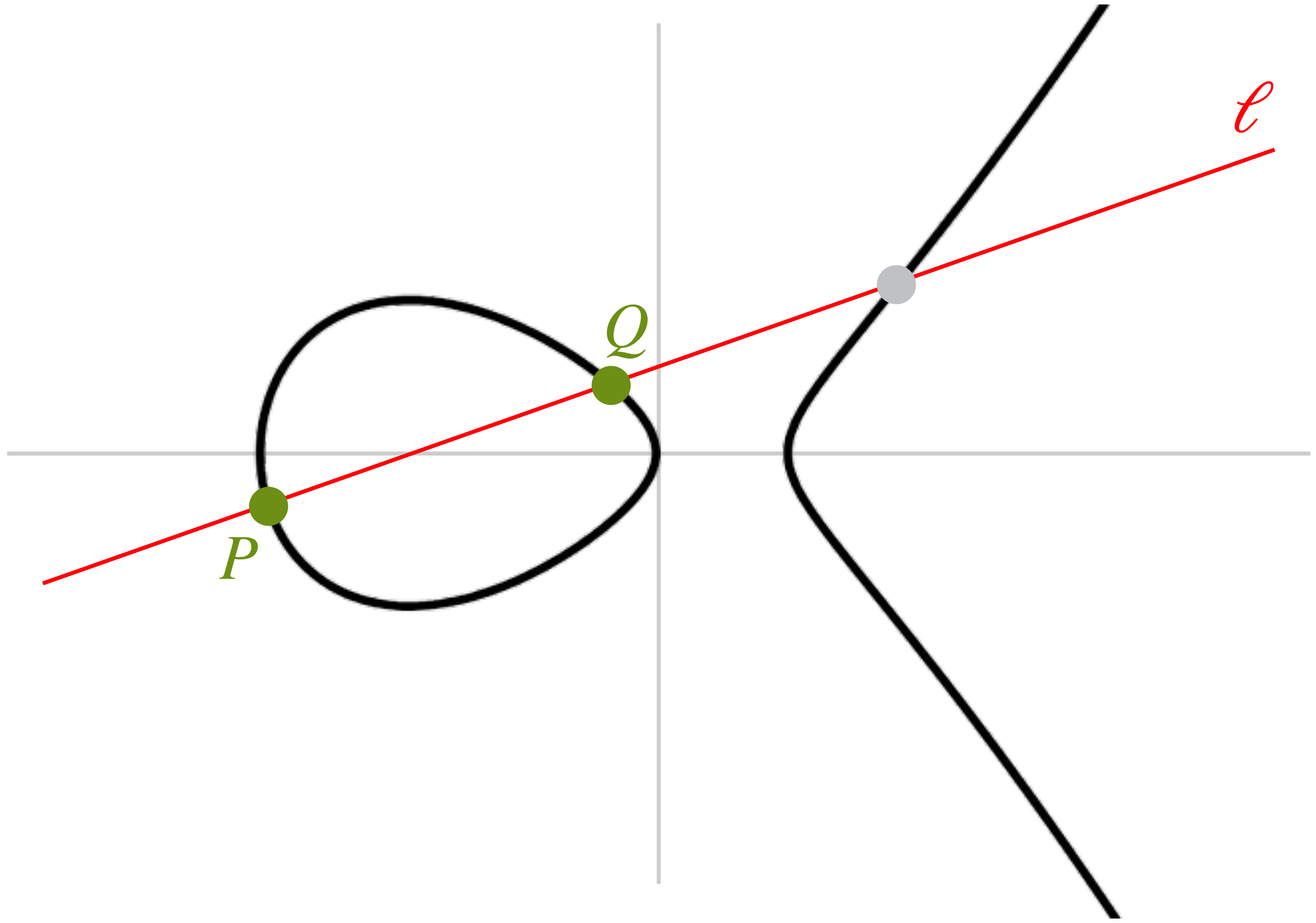


KU LEUVEN

Dimension

1

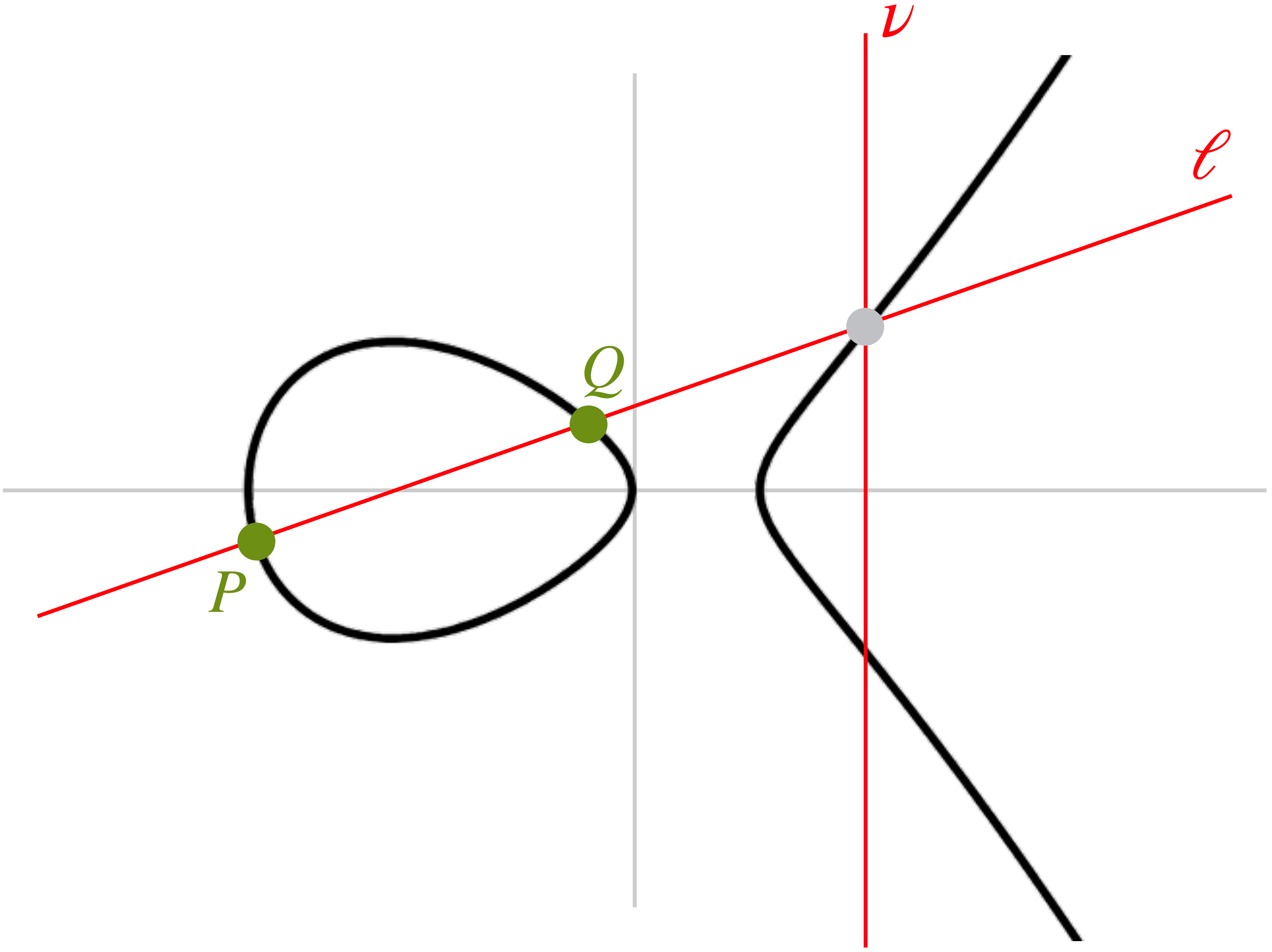
$$E : y^2 = x^3 + ax + b$$



Dimension

1

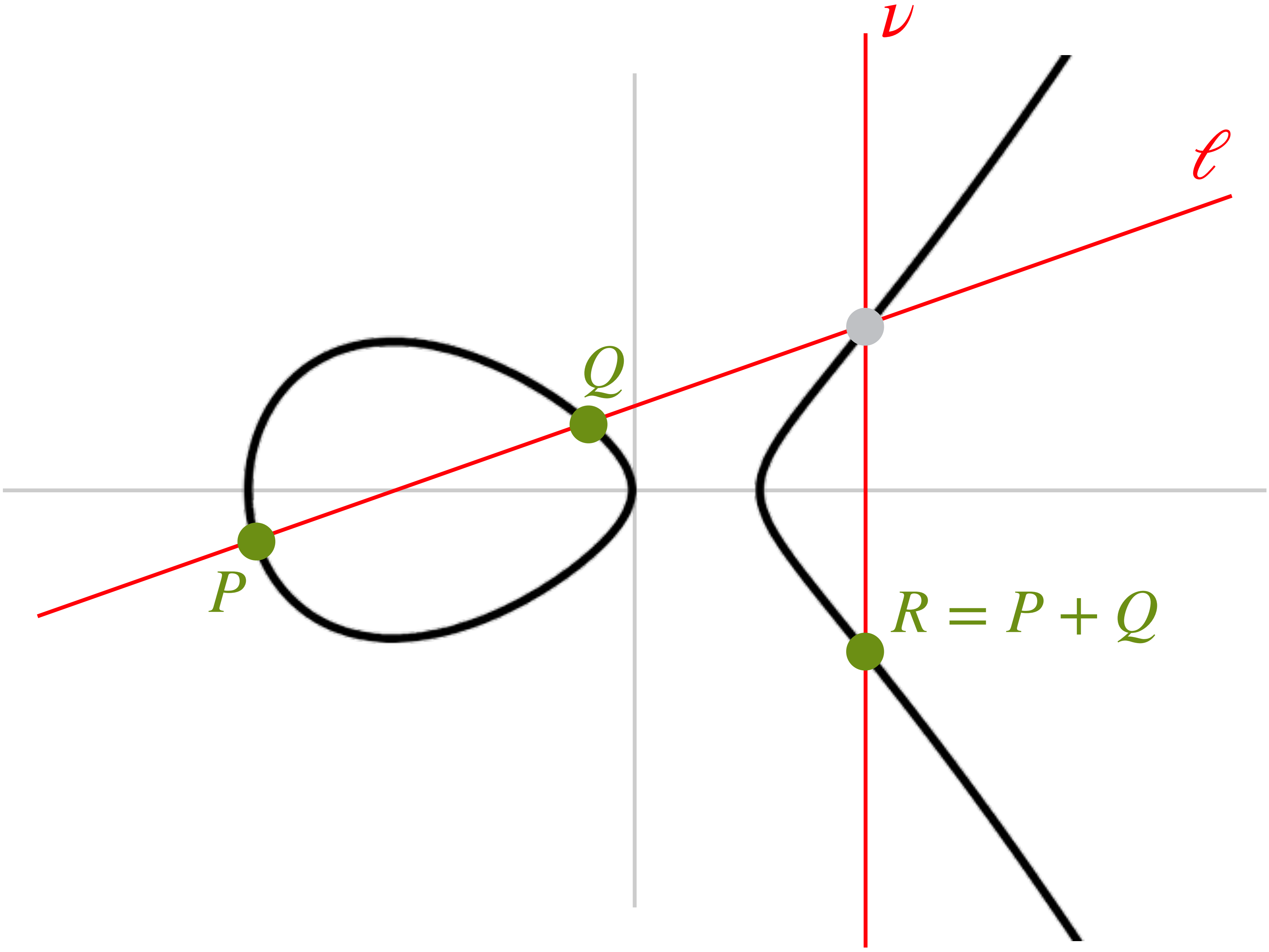
$$E : y^2 = x^3 + ax + b$$



Dimension

1

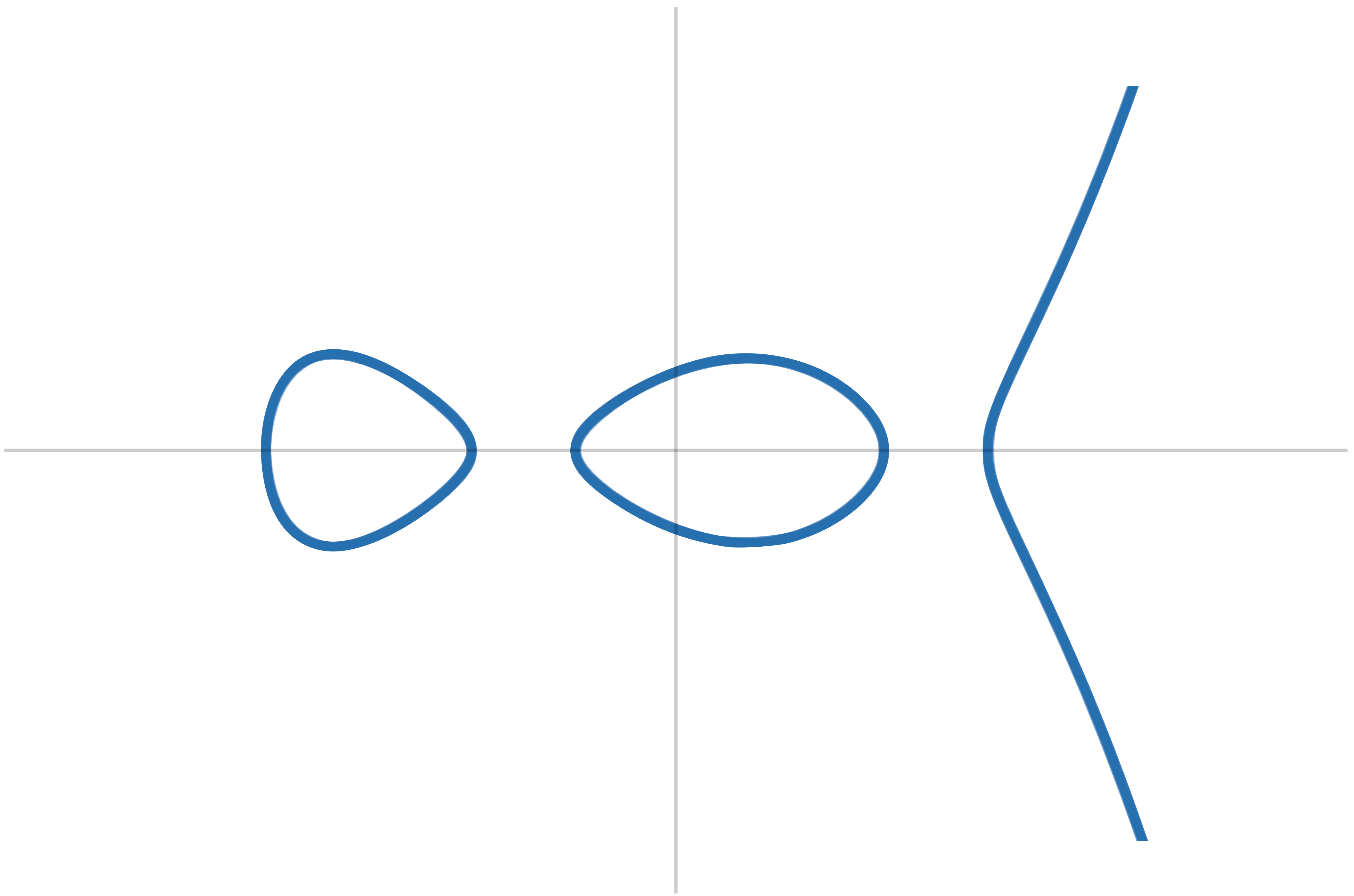
$$E : y^2 = x^3 + ax + b$$



Dimension

2

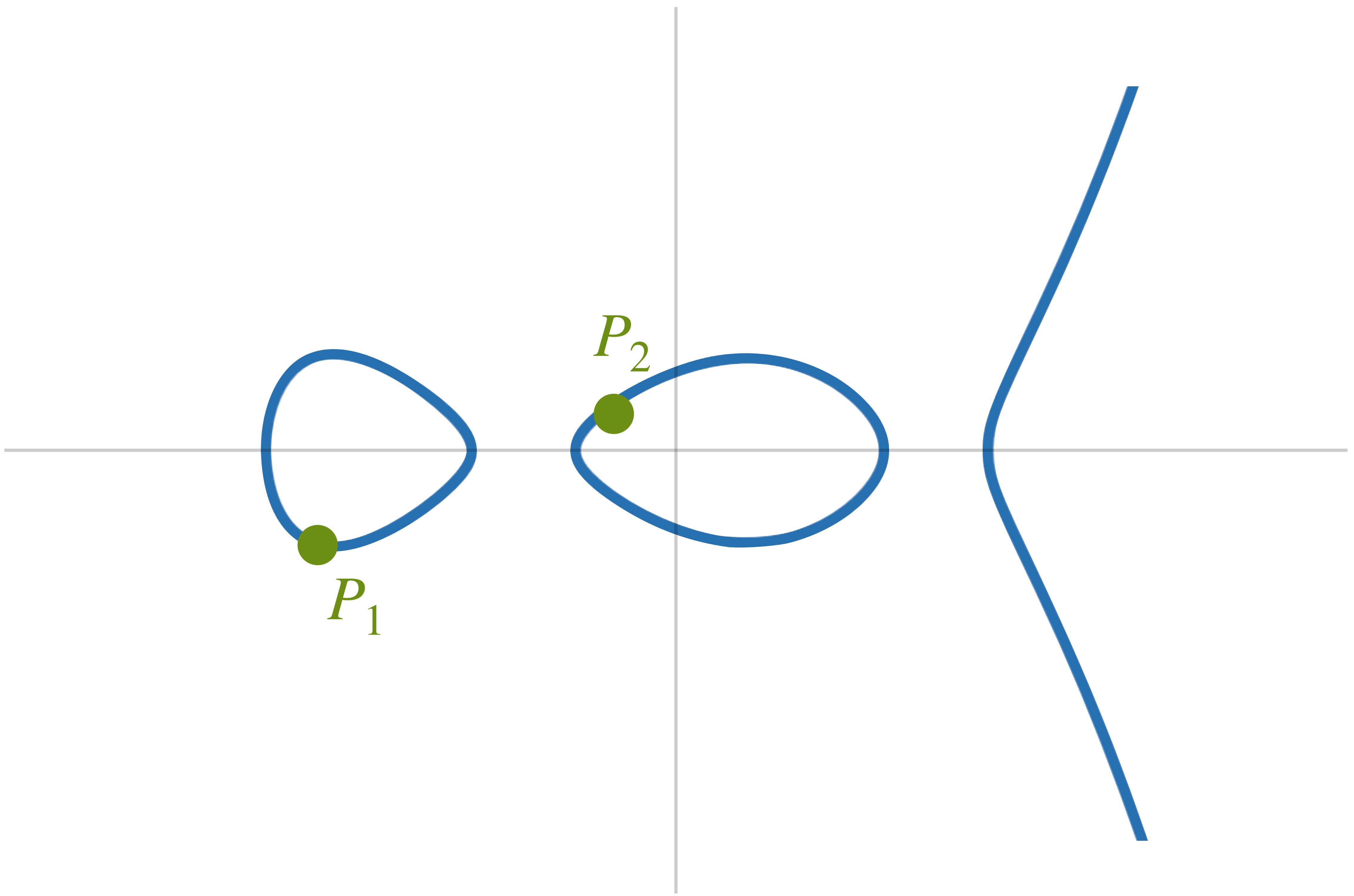
$$C : y^2 = x^5 + ax^3 + bx^2 + cx + d$$



Dimension

2

$$C : y^2 = x^5 + ax^3 + bx^2 + cx + d$$

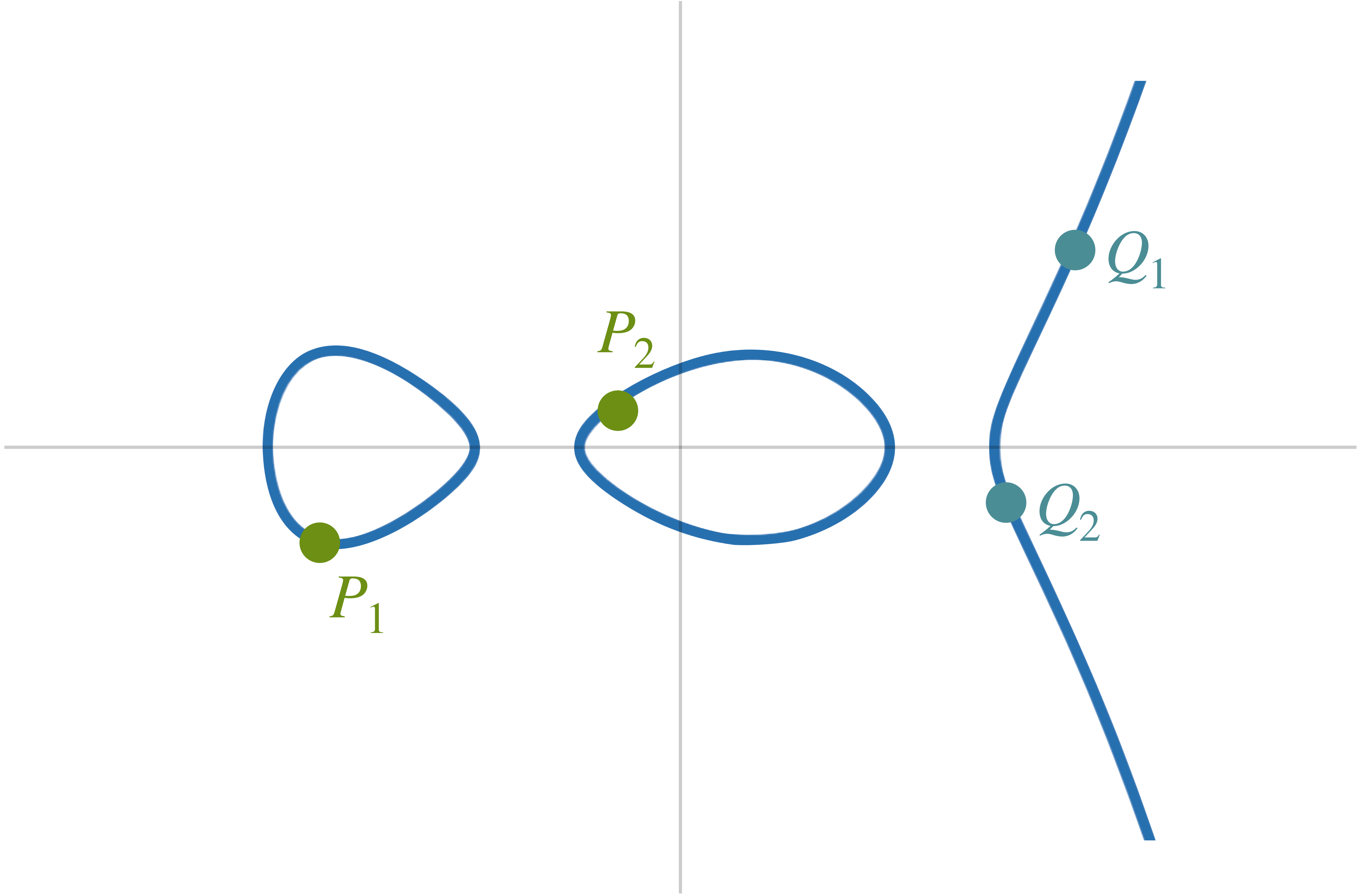


$D_P \in J_C \quad \leftrightarrow \quad (P_1) \oplus (P_2)$

Dimension

2

$$C : y^2 = x^5 + ax^3 + bx^2 + cx + d$$



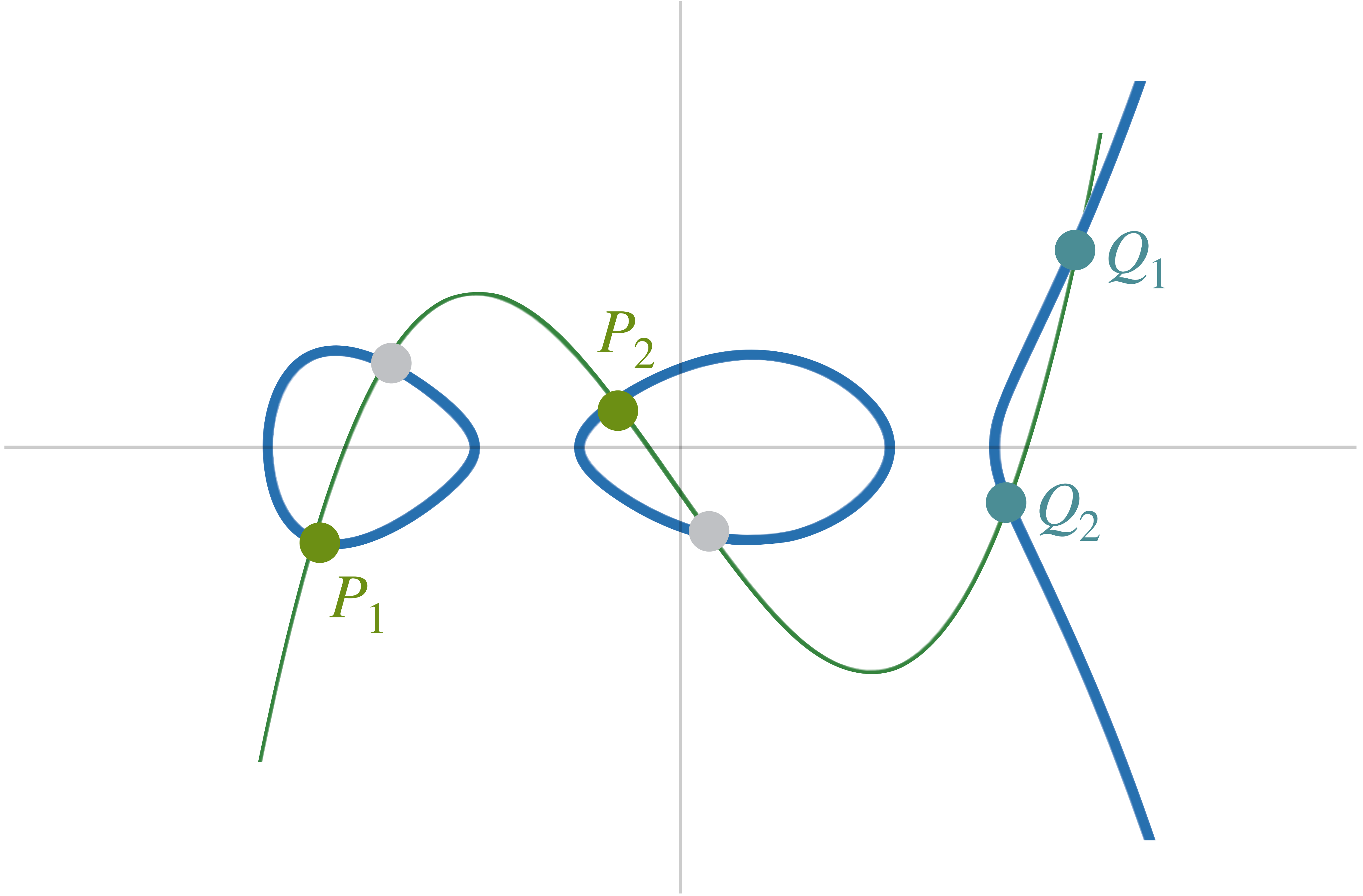
$D_P \in J_C \quad \leftrightarrow \quad (P_1) \oplus (P_2)$

$D_Q \in J_C \quad \leftrightarrow \quad (Q_1) \oplus (Q_2)$

Dimension

2

$$C : y^2 = x^5 + ax^3 + bx^2 + cx + d$$



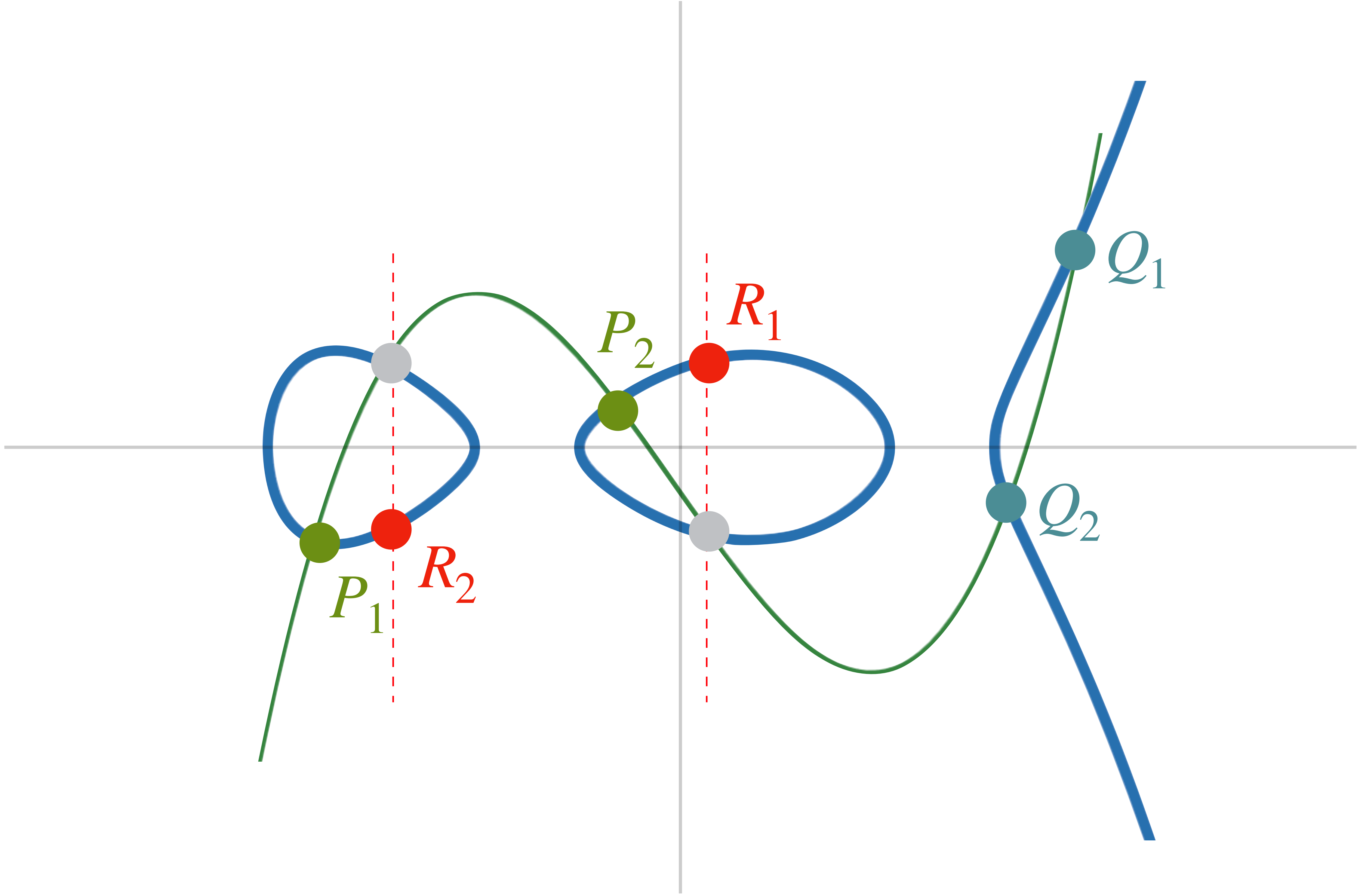
$D_P \in J_C \quad \leftrightarrow \quad (P_1) \oplus (P_2)$

$D_Q \in J_C \quad \leftrightarrow \quad (Q_1) \oplus (Q_2)$

Dimension

2

$$C : y^2 = x^5 + ax^3 + bx^2 + cx + d$$



$D_P \in J_C \quad \leftrightarrow \quad (P_1) \oplus (P_2)$

$D_Q \in J_C \quad \leftrightarrow \quad (Q_1) \oplus (Q_2)$

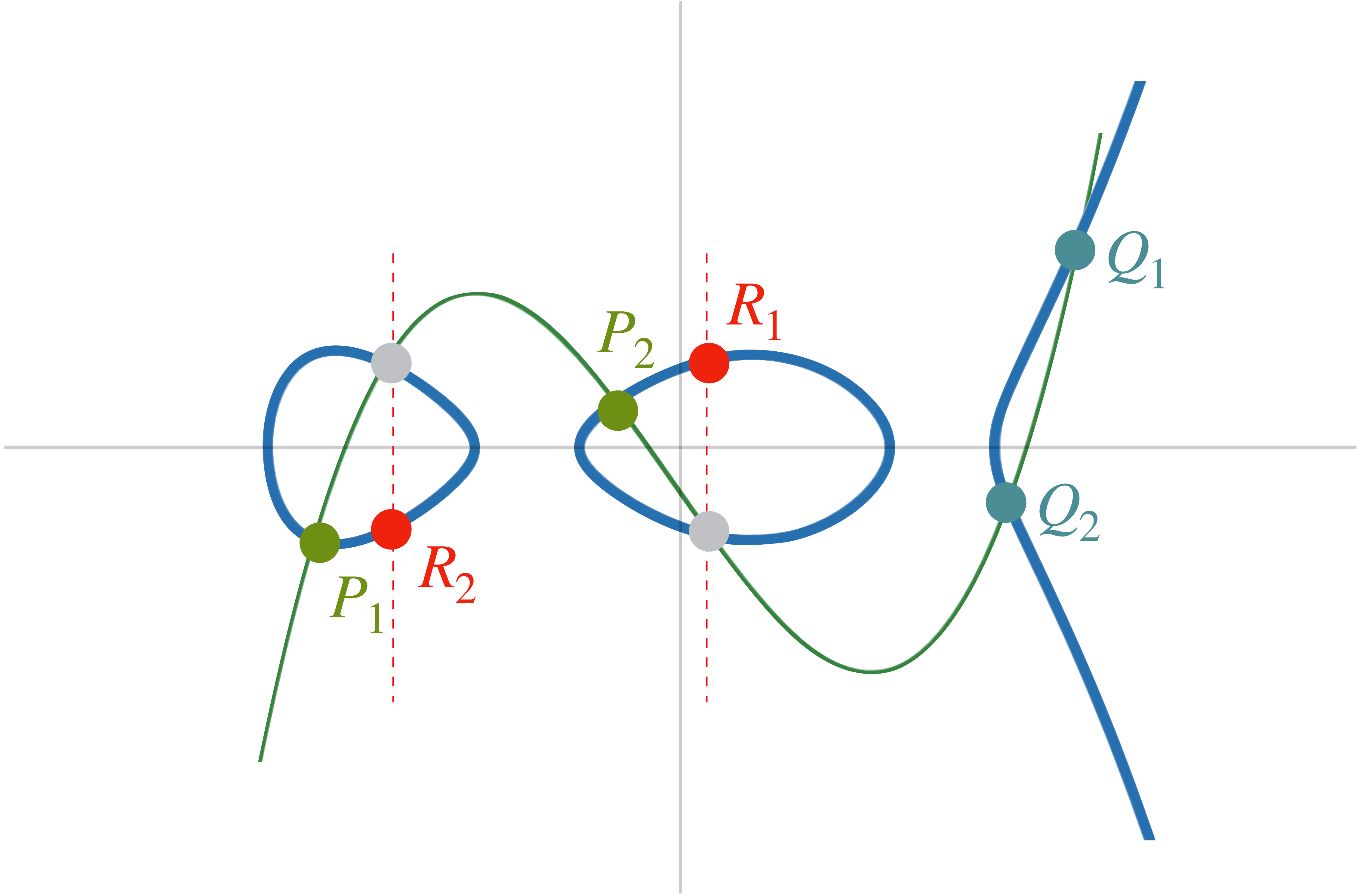
$D_R \in J_C \quad \leftrightarrow \quad (R_1) \oplus (R_2)$

KU LEUVEN

Dimension

2

$$C : y^2 = x^5 + ax^3 + bx^2 + cx + d$$



$D_P \in J_C \quad \leftrightarrow \quad (P_1) \oplus (P_2)$

$D_Q \in J_C \quad \leftrightarrow \quad (Q_1) \oplus (Q_2)$

$D_R \in J_C \quad \leftrightarrow \quad (R_1) \oplus (R_2)$

$$D_R := D_P + D_Q$$

(addition on the Jacobian J_C,
NOT on the curve itself!!)

KU LEUVEN

Dimension

1

Elliptic curves
(genus-1 curves)

$$\varphi : E_1 \to E_2$$

Dimension

1

Elliptic curves
(genus-1 curves)

$$\varphi : E_1 \to E_2$$

1

For this talk, assume
$\deg \varphi = |\ker \varphi|$.

(that is, φ is separable)

Dimension

1

Elliptic curves
(genus-1 curves)

$$\varphi : E_1 \to E_2$$

1

For this talk, assume
$\deg \varphi = |\ker \varphi|$.

(that is, φ is separable)

2

An ℓ**-isogeny** is an
isogeny of degree ℓ.

$\ker \ell \cong \mathbb{Z}/\ell\mathbb{Z}$

Dimension

1

Elliptic curves
(genus-1 curves)

$$\varphi : E_1 \to E_2$$

1

For this talk, assume
$\deg \varphi = |\ker \varphi|$.

(that is, φ is separable)

2

An ℓ**-isogeny** is an
isogeny of degree ℓ.

$\ker \ell \cong \mathbb{Z}/\ell\mathbb{Z}$

3

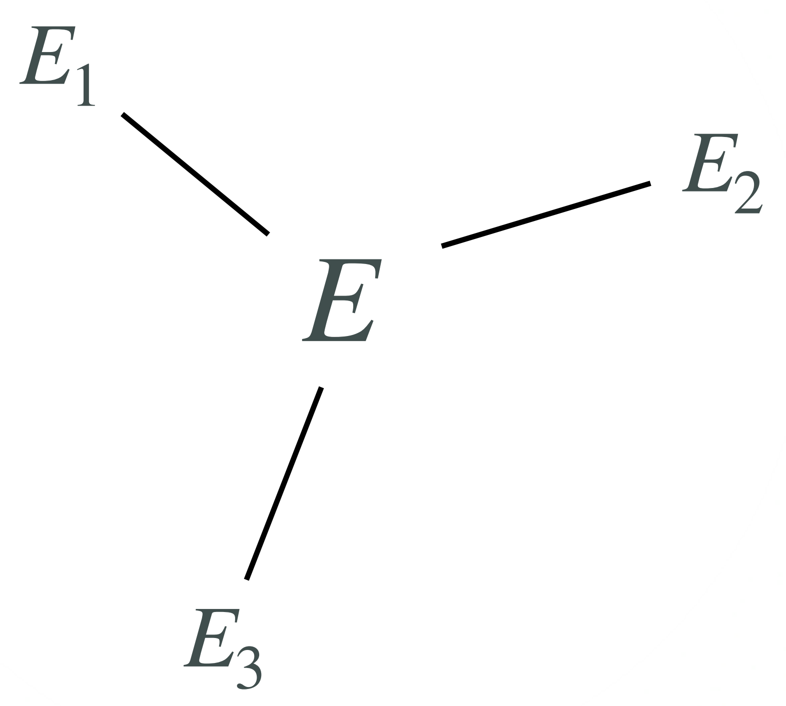
Every ell. curve E has
$\ell + 1$
ℓ-isogenies

KU LEUVEN

Dimension

1

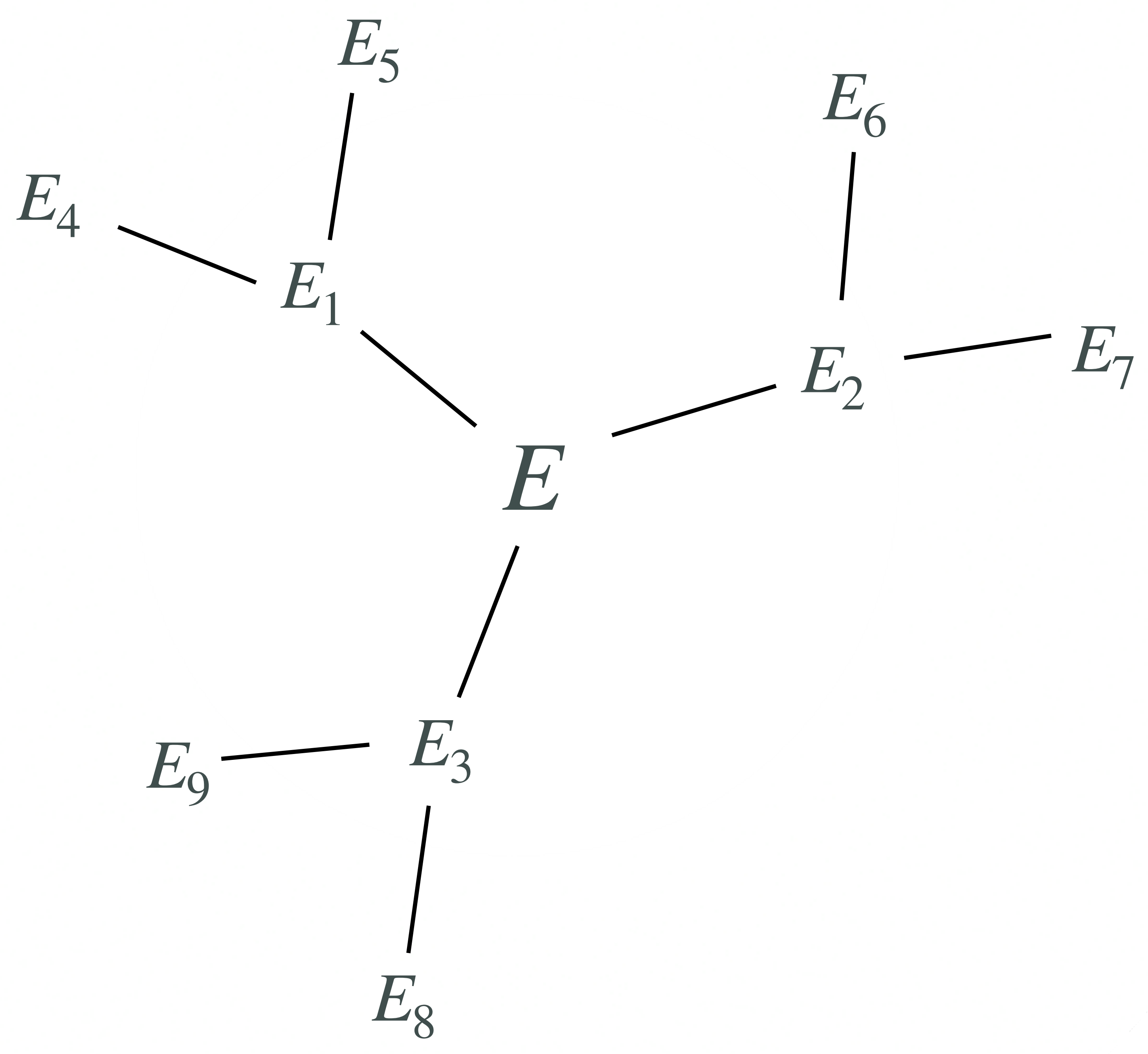
$\ell = 2$



Dimension

1

$\ell = 2$

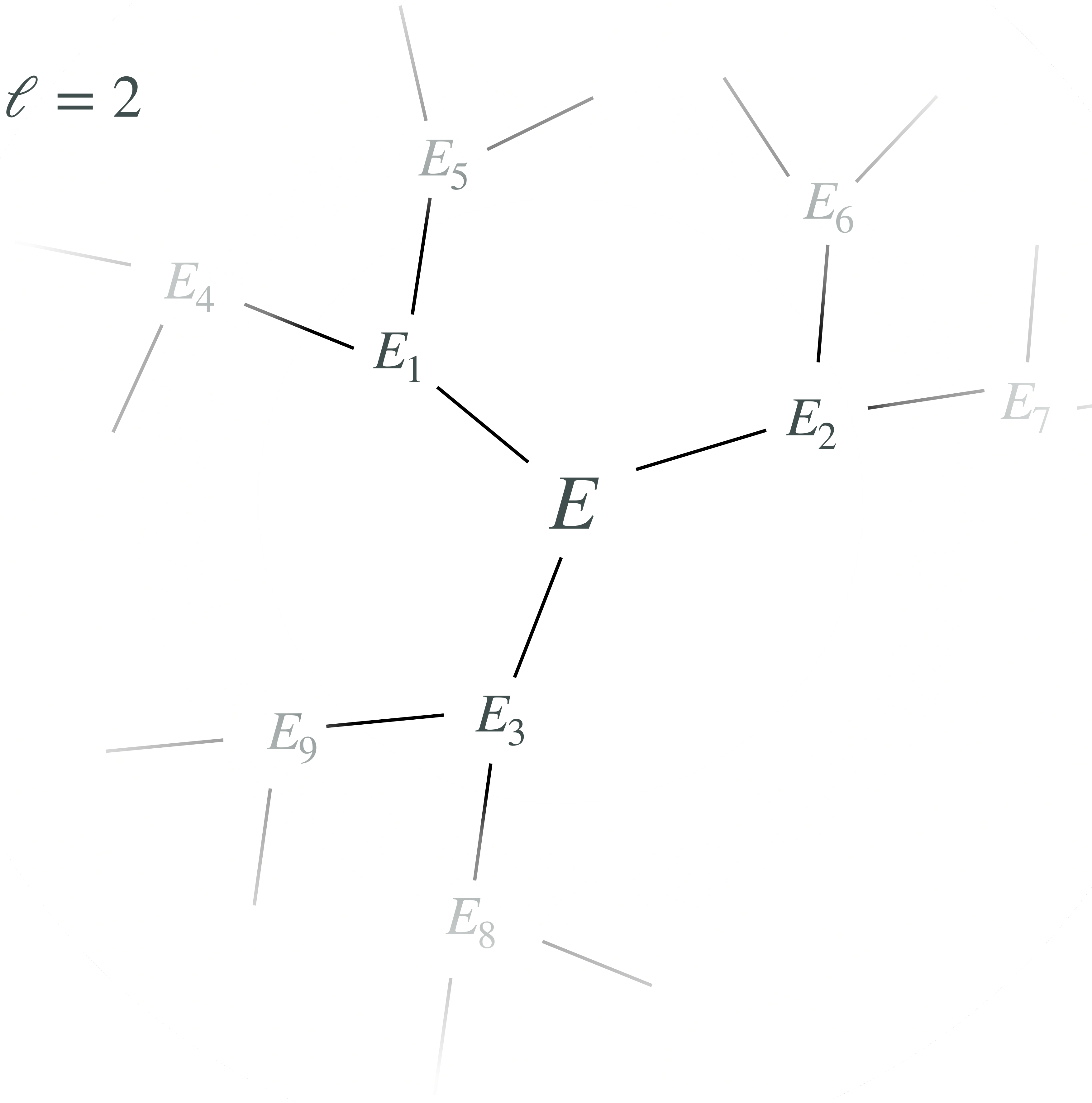


KU LEUVEN

Dimension

1

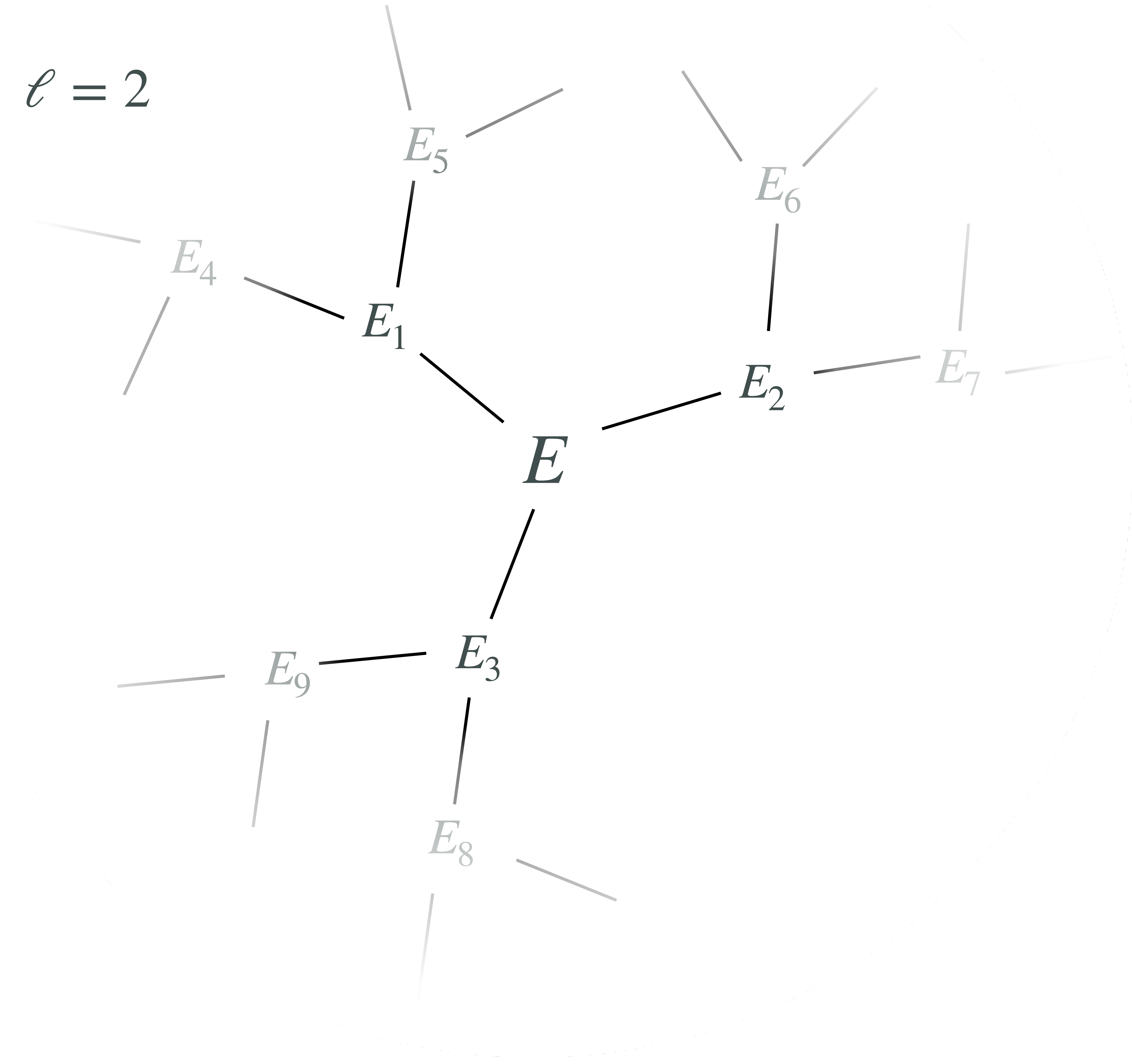
$\ell = 2$



Dimension

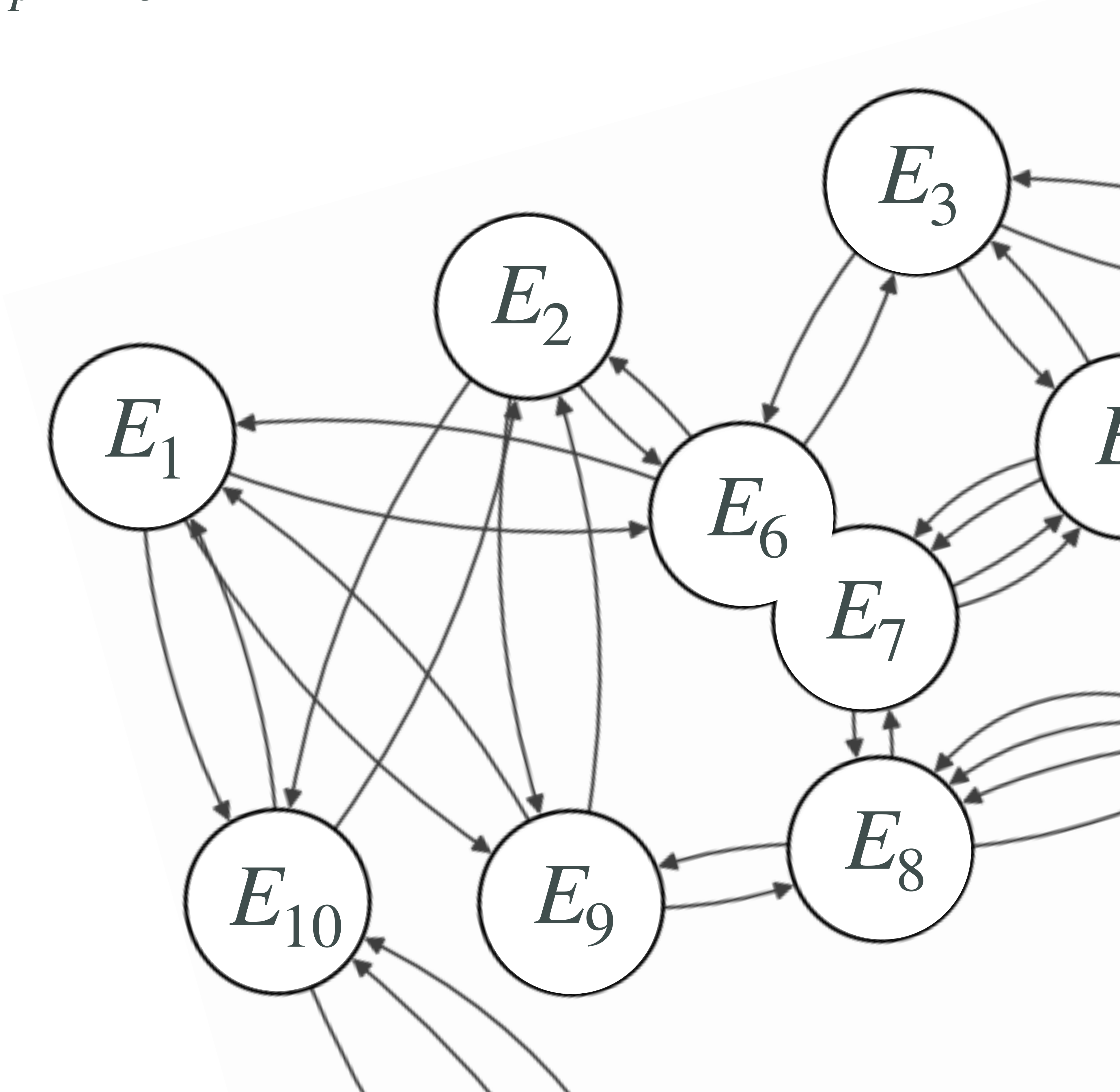
1

$\ell = 2$



$\mathbb{F}_{p^2}$ with $p = 131$

$\ell = 2$



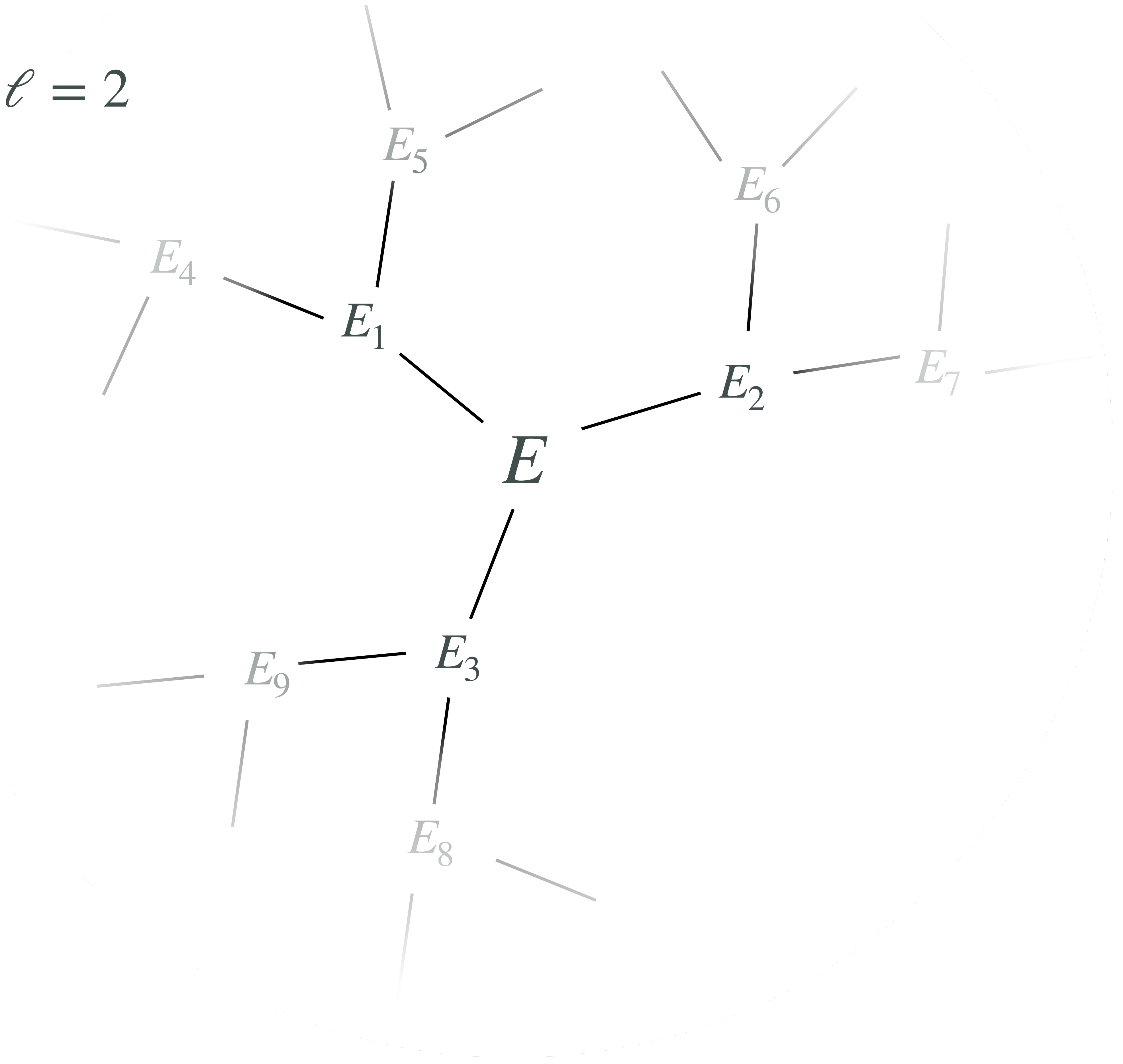
Dimension 1

1 $\ell + 1$ regular

2 Connected!

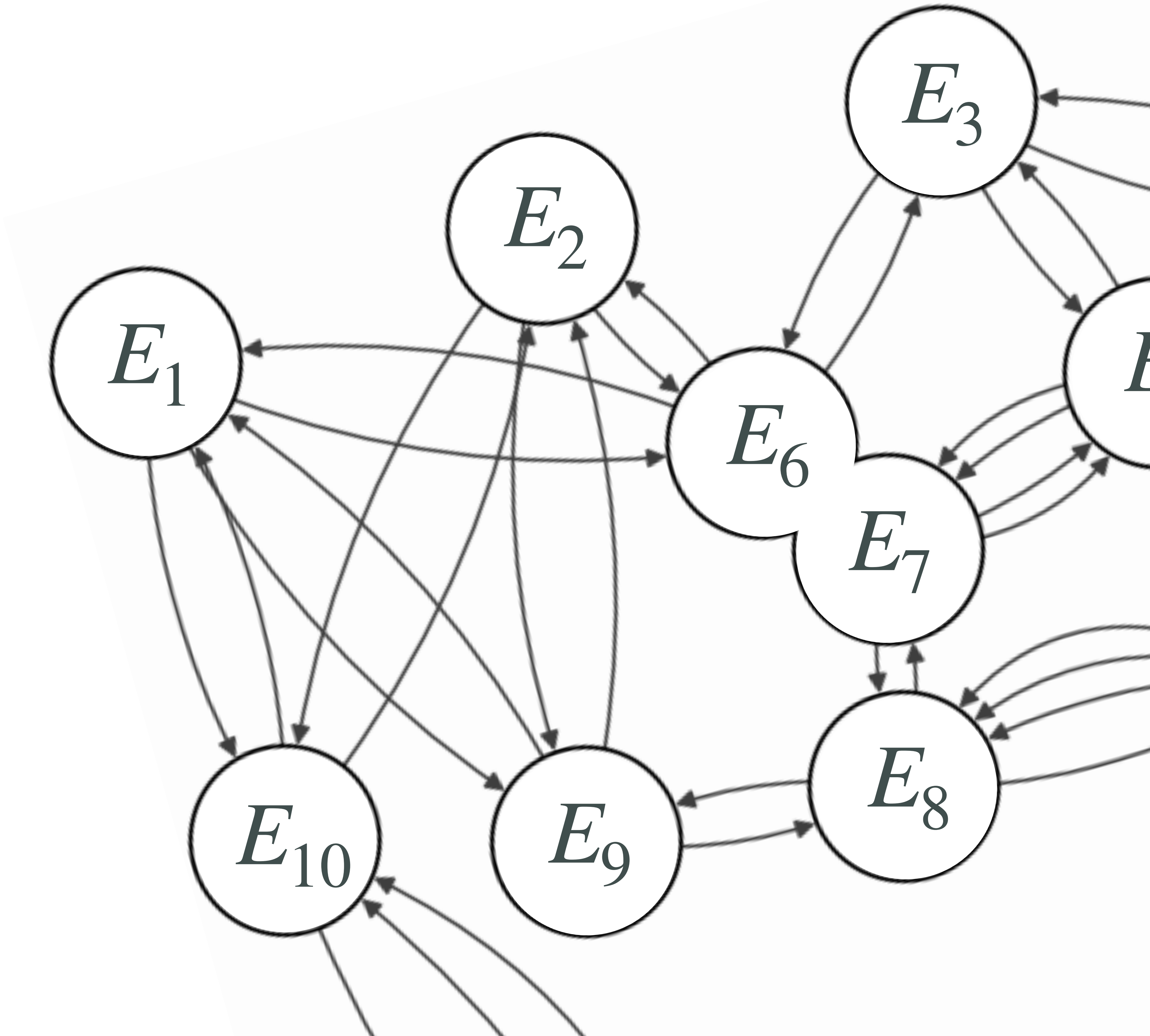
3 **Ramanujan!!**

$\ell = 2$



$\mathbb{F}_{p^2}$ with $p = 131$

$\ell = 2$



Dimension

2

Jacobians
(of genus-2 curves)

$$\Phi : J_1 \to J_2$$

KU LEUVEN

Dimension

2

Jacobians
(of genus-2 curves)

$$\Phi : J_1 \to J_2$$

1

An (ℓ, ℓ)-isogeny is
an isogeny $\Phi : J \to J'$
s.t. $\ker \Phi \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$

Dimension 2

Jacobians
(of genus-2 curves)

$$\Phi : J_1 \to J_2$$

1

An (ℓ, ℓ)-isogeny is
an isogeny $\Phi : J \to J'$
s.t. $\ker \Phi \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$

2

.. but this kernel must
also be **isotropic:**

$e_\ell(P, Q) = 1$ for
$P, Q \in \ker \Phi$

KU LEUVEN

Dimension

2

Jacobians
(of genus-2 curves)

$$\Phi : J_1 \to J_2$$

1

An (ℓ, ℓ)-isogeny is
an isogeny $\Phi : J \to J'$
s.t. $\ker \Phi \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$

2

.. but this kernel must
also be **isotropic:**

$e_\ell(P, Q) = 1$ for
$P, Q \in \ker \Phi$

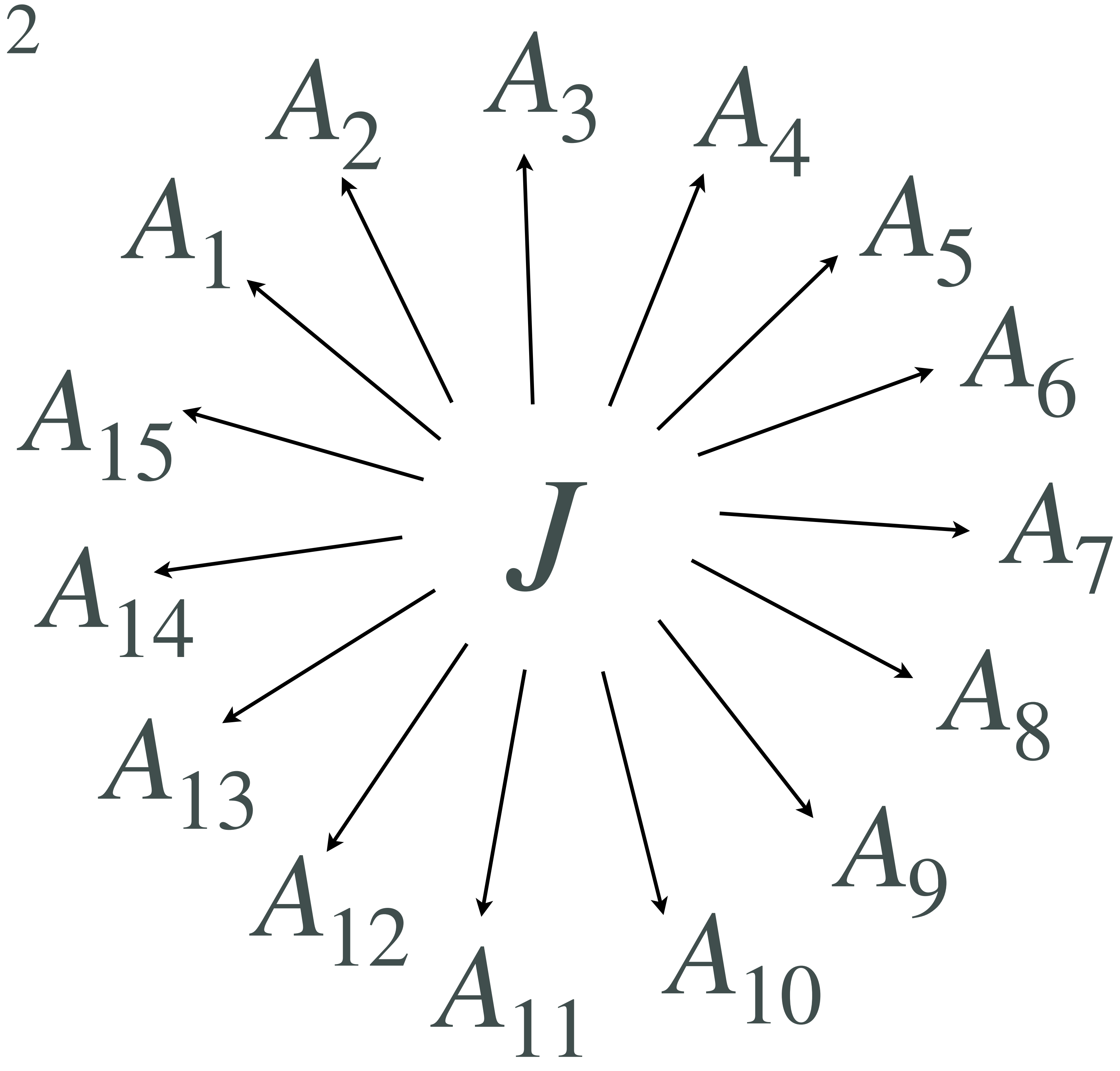
3

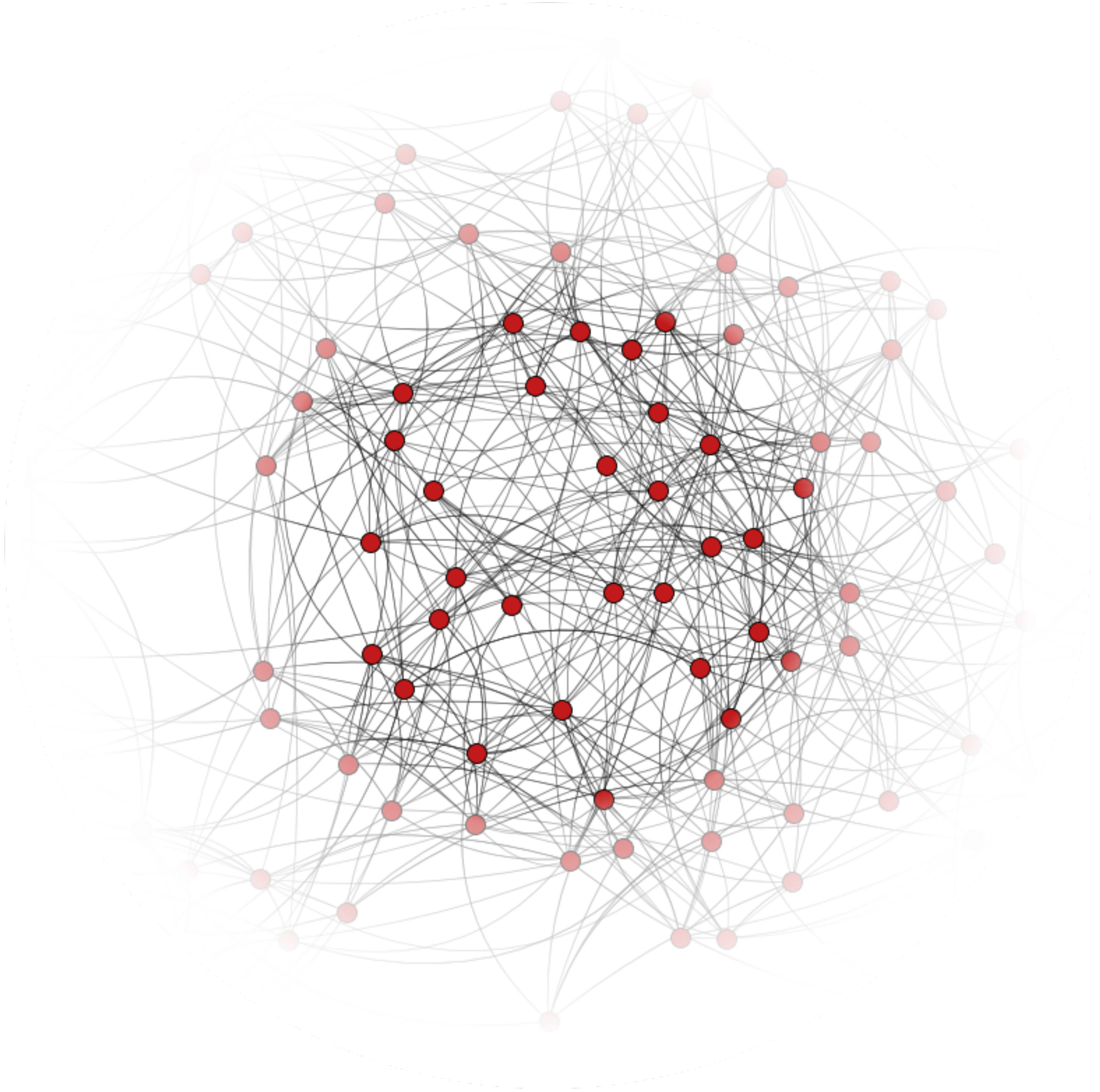
A 2-dimensional
Jacobian has
$\ell^3 + \ell^2 + \ell + 1$
(ℓ, ℓ)-isogenies

Dimension

2

$\ell = 2$





Dimension

2

1

$\ell^3 + \ell^2 + \ell + 1$
regular

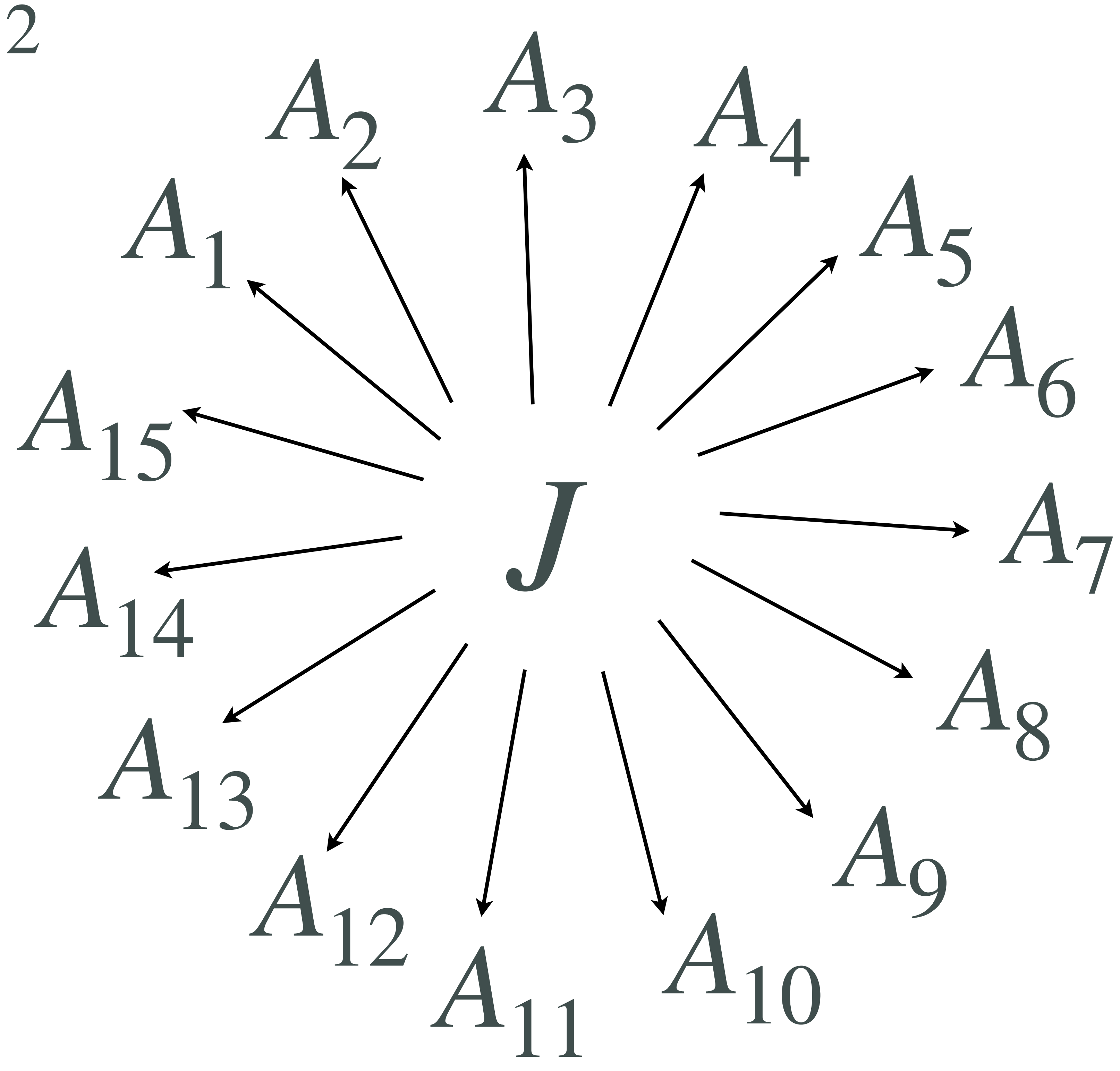
2

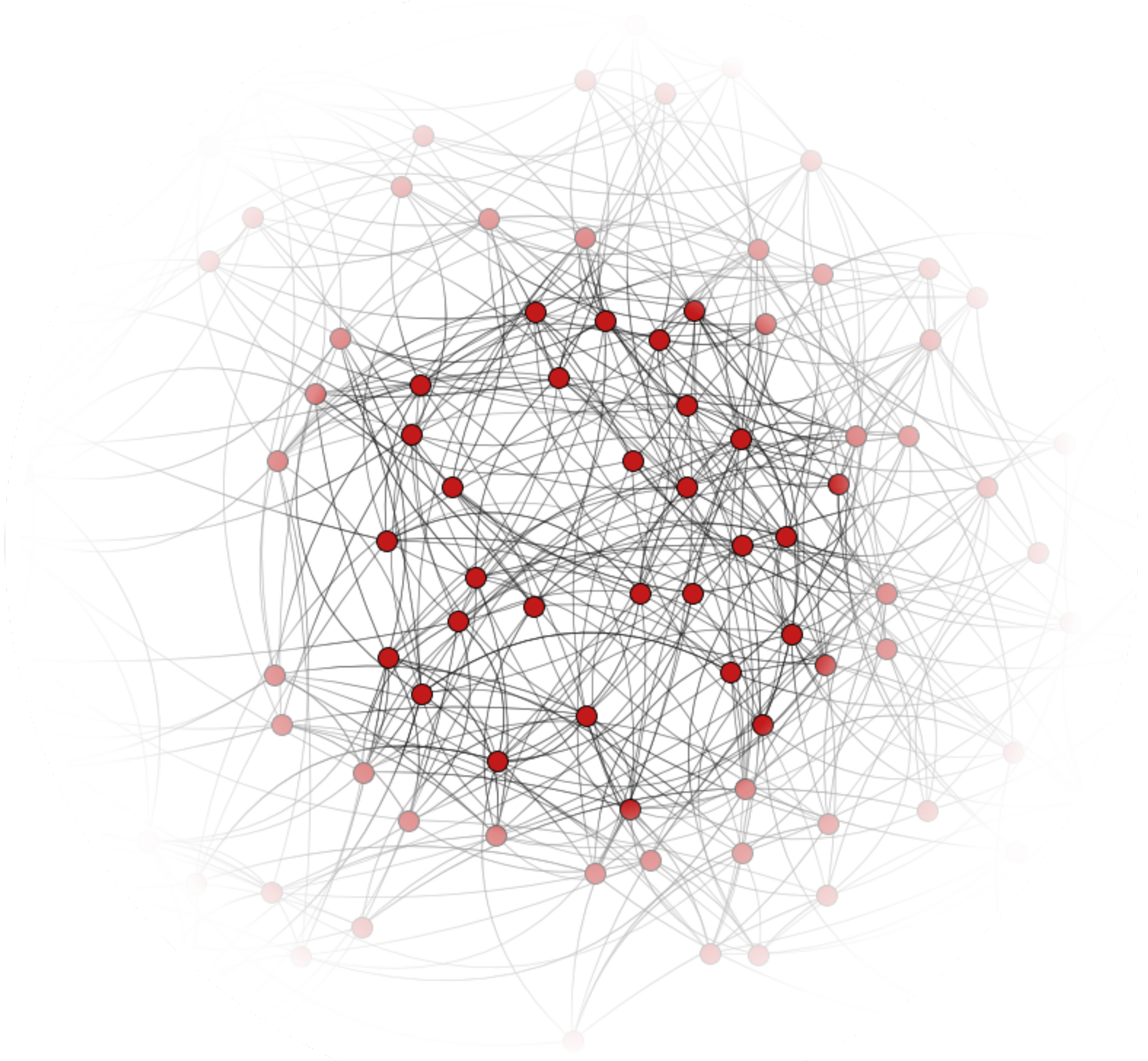
Connected!

3

NOT
Ramanujan**!!**

$\ell = 2$





Main Problem

Higher-dimensional isogenies are much more complicated

Q

MAIN QUESTION

"Correct" analogue of dim-1 graphs for isogeny-based cryptography?

Q

MAIN QUESTION

“Correct” analogue of dim-1 graphs for isogeny-based cryptography?

A

OUR ANSWER

1. Fix “bad cycles” using level structure
2. Analysis of action of automorphisms

PART 1
GRAPHS

PART 2
CYCLES

PART 3
AUTOMS.

PART 2
CYCLES

Isogeny composition in dimension 1 is easy!

$$E \xrightarrow{\varphi_1} E' \xrightarrow{\varphi_2} E''$$

1

Composition $\varphi = \varphi_2 \circ \varphi_1$
is an ℓ^2-isogeny:

$$\ker \varphi \cong \mathbb{Z}/\ell^2\mathbb{Z}$$

Isogeny composition in dimension 1 is easy!

$$E \xrightarrow{\varphi_1} E' \xrightarrow{\varphi_2} E''$$

$$\begin{tikzcd} E \arrow[r, bend left, "\varphi_1"] & E' \arrow[l, bend left, "\varphi_2"] \end{tikzcd}$$

1

Composition $\varphi = \varphi_2 \circ \varphi_1$
is an ℓ^2-isogeny:

$$\ker \varphi \cong \mathbb{Z}/\ell^2\mathbb{Z}$$

2

Composition $\varphi = \varphi_2 \circ \varphi_1$
is scalar multiplication $[\ell]$ on E

$$\ker[\ell] = E[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$$

Isogeny composition in dimension 2 is hard!

$$
\begin{tikzcd}
J \arrow[r, bend left, "\Phi_1"] & J' \arrow[l, bend left, "\Phi_2"]
\end{tikzcd}
$$

3

Composition is scalar multiplication $[\ell]$ on J

$$\ker[\ell] = J[\ell] \cong \left(\mathbb{Z}/\ell\mathbb{Z}\right)^4$$

Isogeny composition in dimension 2 is hard!

$$J \xrightarrow{\Phi_1} J' \xrightarrow{\Phi_2} J''$$

$$\begin{tikzcd} J \arrow[r, bend left, "\Phi_1"] & J' \arrow[l, bend left, "\Phi_2"] \end{tikzcd}$$

3

Composition is scalar multiplication $[\ell]$ on J

$$\ker[\ell] = J[\ell] \cong \left(\mathbb{Z}/\ell\mathbb{Z}\right)^4$$

PART 2
CYCLES

Isogeny composition in dimension 2 is hard!

$$J \xrightarrow{\Phi_1} J' \xrightarrow{\Phi_2} J''$$

$$\begin{tikzcd} J \arrow[r, bend left, "\Phi_1"] & J' \arrow[l, bend left, "\Phi_2"] \end{tikzcd}$$

1

GOOD EXTENSION

Kernels don't "overlap",
we get an (ℓ^2, ℓ^2)-isogeny.

$$\ker \Phi = \mathbb{Z}/\ell^2\mathbb{Z} \times \mathbb{Z}/\ell^2\mathbb{Z}$$

3

Composition is scalar multiplication $[\ell]$ on J

$$\ker[\ell] = J[\ell] \cong \left(\mathbb{Z}/\ell\mathbb{Z}\right)^4$$

Isogeny composition in dimension 2 is hard!

$$J \xrightarrow{\Phi_1} J' \xrightarrow{\Phi_2} J''$$

$$\begin{tikzcd} J \arrow[r, bend left, "\Phi_1"] & J' \arrow[l, bend left, "\Phi_2"] \end{tikzcd}$$

1

GOOD EXTENSION

Kernels don't "overlap",
we get an (ℓ^2, ℓ^2)-isogeny.

$$\ker \Phi = \mathbb{Z}/\ell^2\mathbb{Z} \times \mathbb{Z}/\ell^2\mathbb{Z}$$

2

BAD EXTENSION

Kernels do "overlap",
composition is not (ℓ^2, ℓ^2)

$$\ker \Phi = \mathbb{Z}/\ell^2\mathbb{Z} \times \left(\mathbb{Z}/\ell\mathbb{Z}\right)^2$$

3

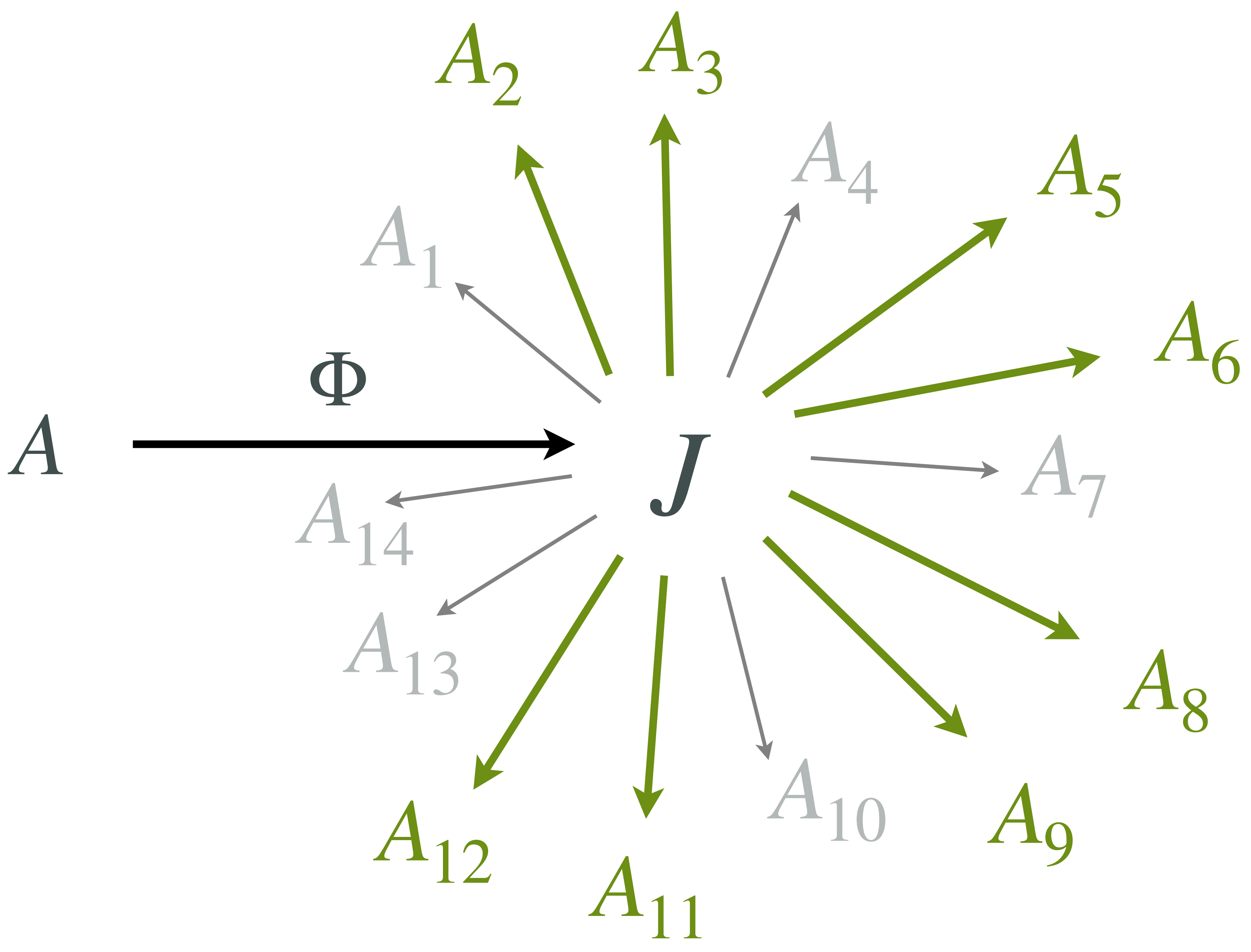
Composition is scalar
multiplication $[\ell]$ on J

$$\ker[\ell] = J[\ell] \cong \left(\mathbb{Z}/\ell\mathbb{Z}\right)^4$$

PART 2
CYCLES

Fix graph: yeet bad cycles using level structure

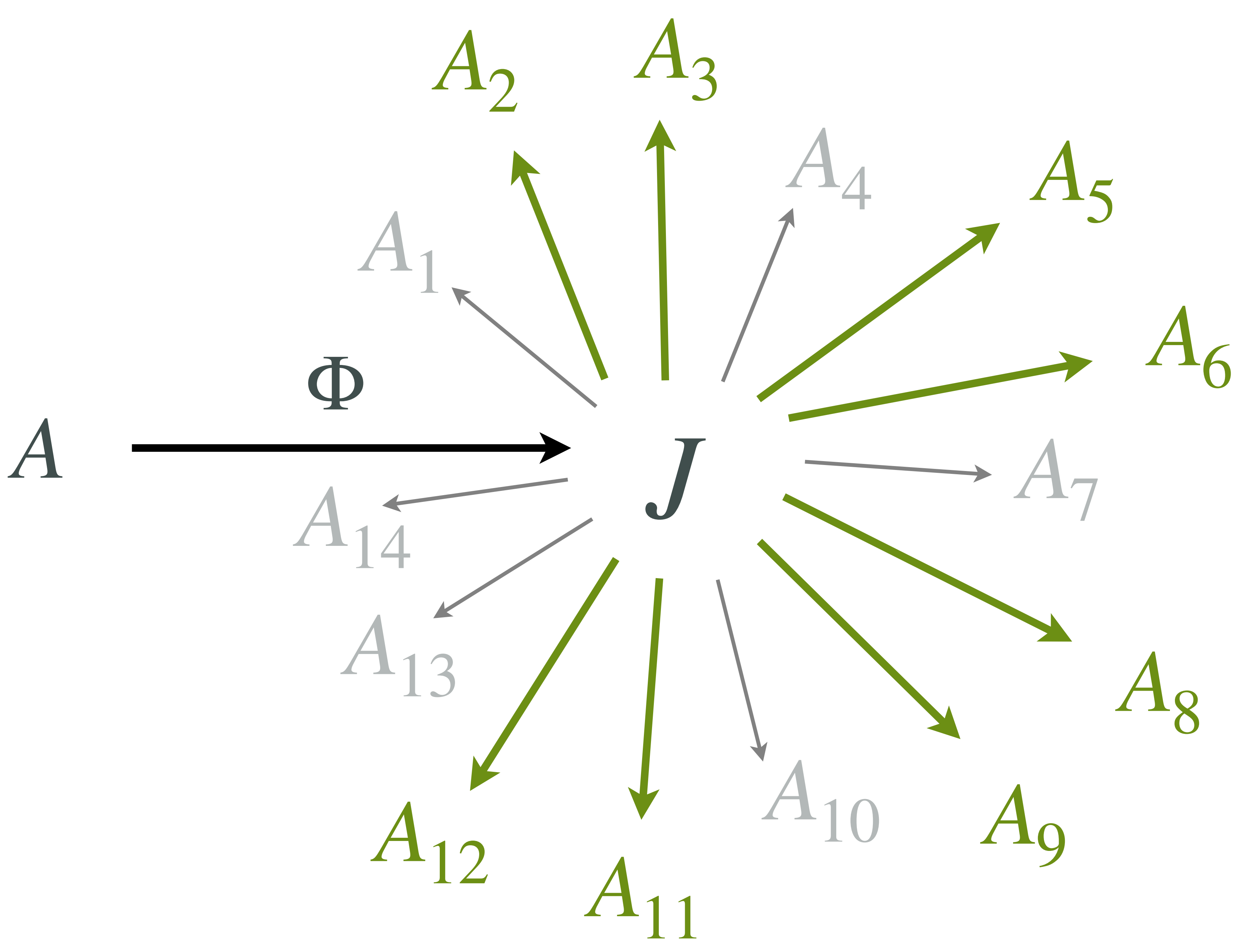
$\ell = 2$



PART 2
CYCLES

Fix graph: yeet bad cycles using level structure

$\ell = 2$

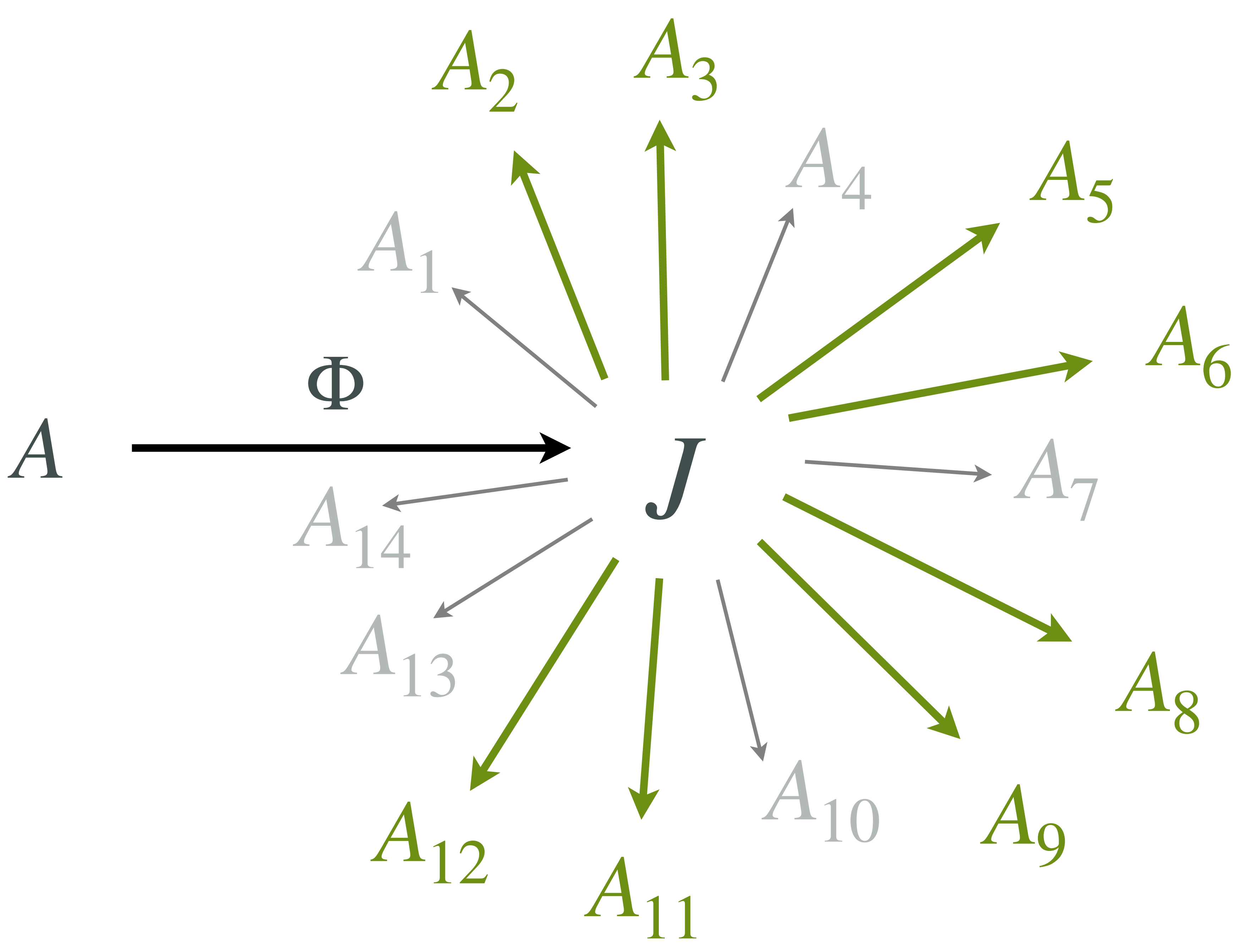


!

Given $\Phi : A \to J$, out of the 15 $(2,2)$-isogenies only **8** are good extensions

Fix graph: yeet bad cycles using level structure

$\ell = 2$



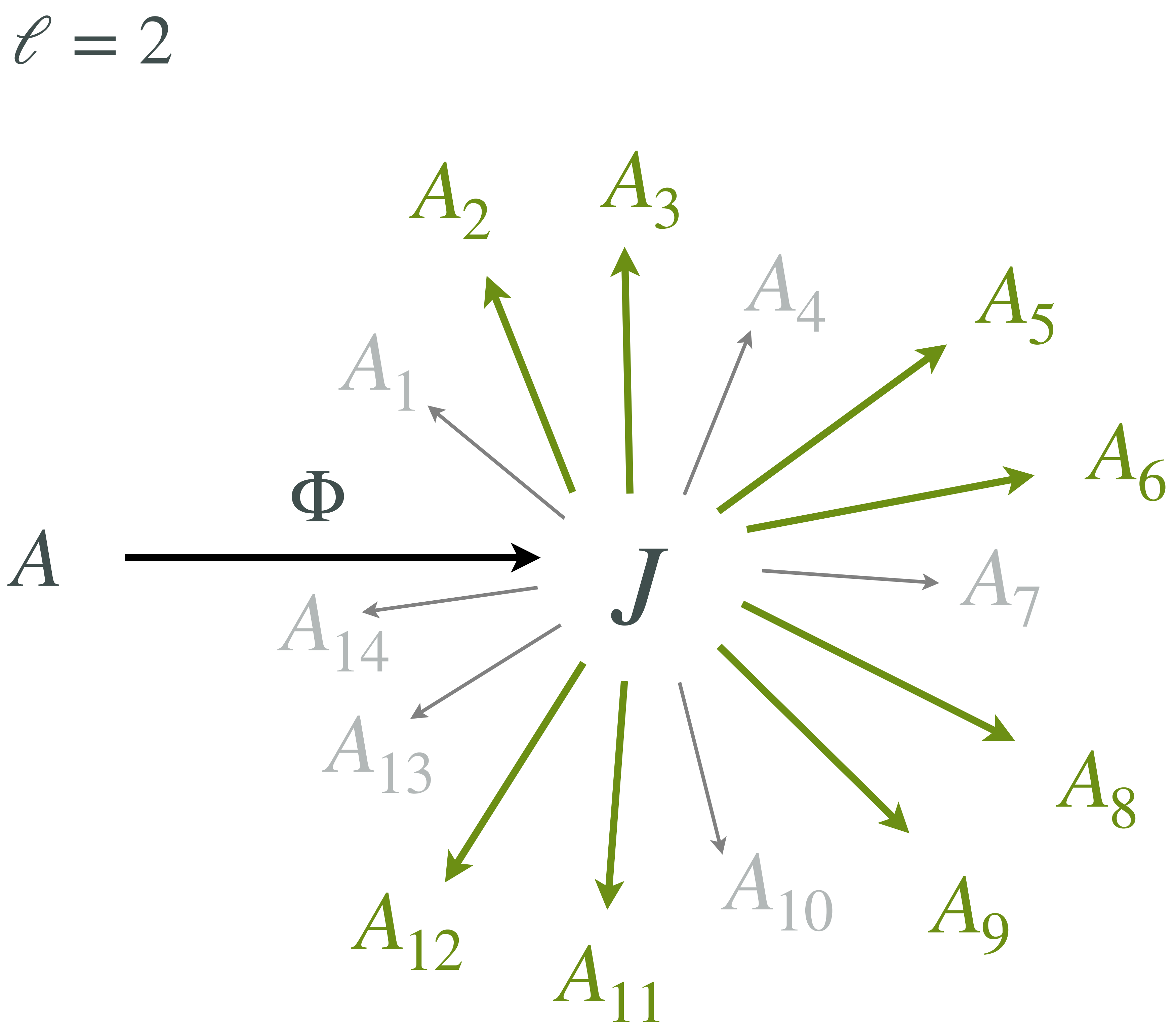
!

Given $\Phi : A \to J$, out of the 15 $(2,2)$-isogenies only **8** are good extensions

1

make nodes **level structure** (J, G) where G represents $\Phi : A \to J$ by $G = \ker \hat{\Phi}$

Fix graph: yeet bad cycles using level structure



! Given $\Phi : A \to J$, out of the 15 $(2,2)$-isogenies only **8** are good extensions

1 make nodes **level structure** (J, G) where G represents $\Phi : A \to J$ by $G = \ker \hat{\Phi}$

2 make edges **good** by only accepting $\Phi' : J \to J'$ with $\ker \Phi' \cap G = \{0_J\}$

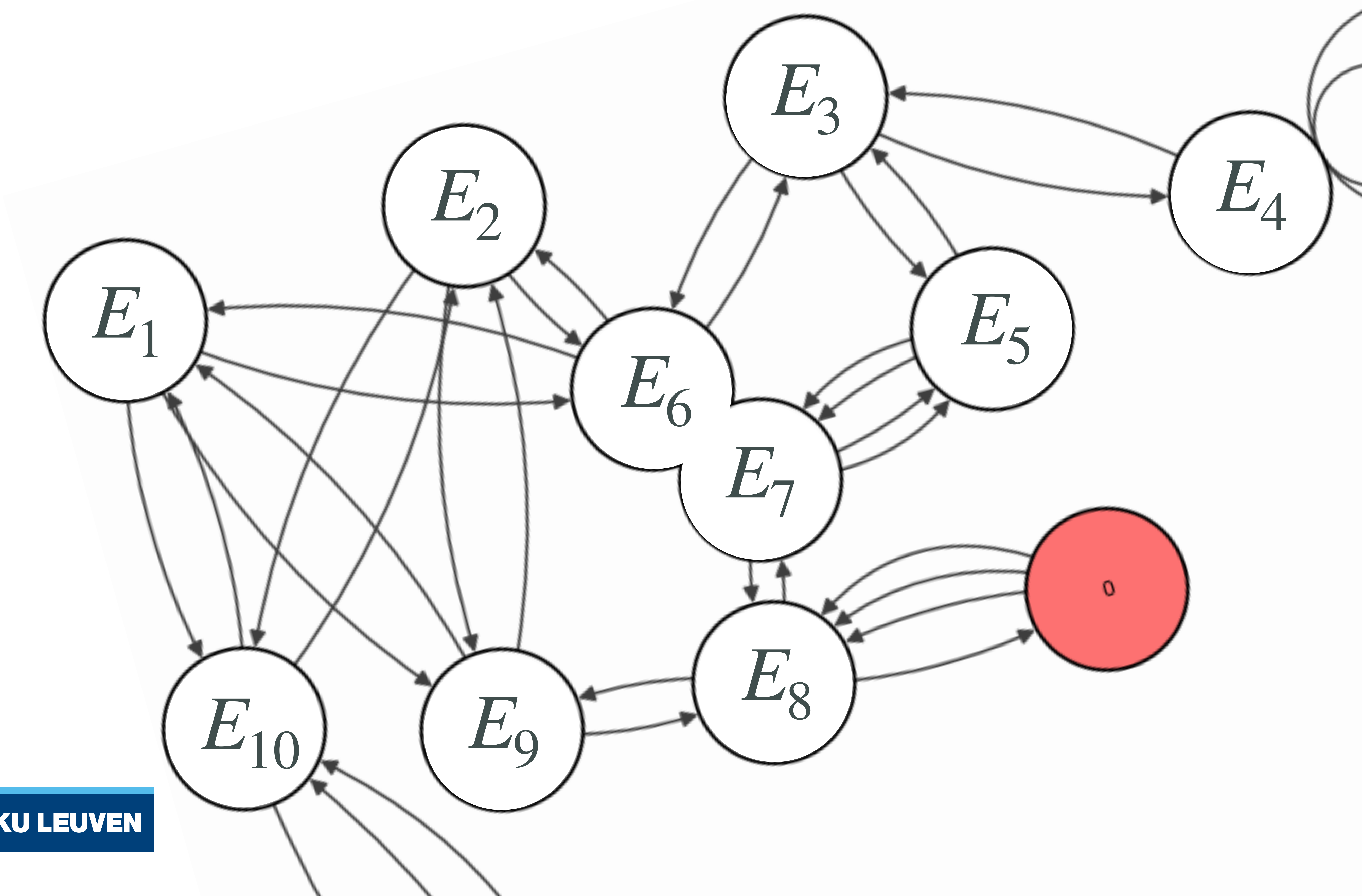
PART 1
GRAPHS

PART 2
CYCLES

PART 3
AUTOMS.

PART 3
AUTOMS.

Automorphisms ruin the regularity of the graph

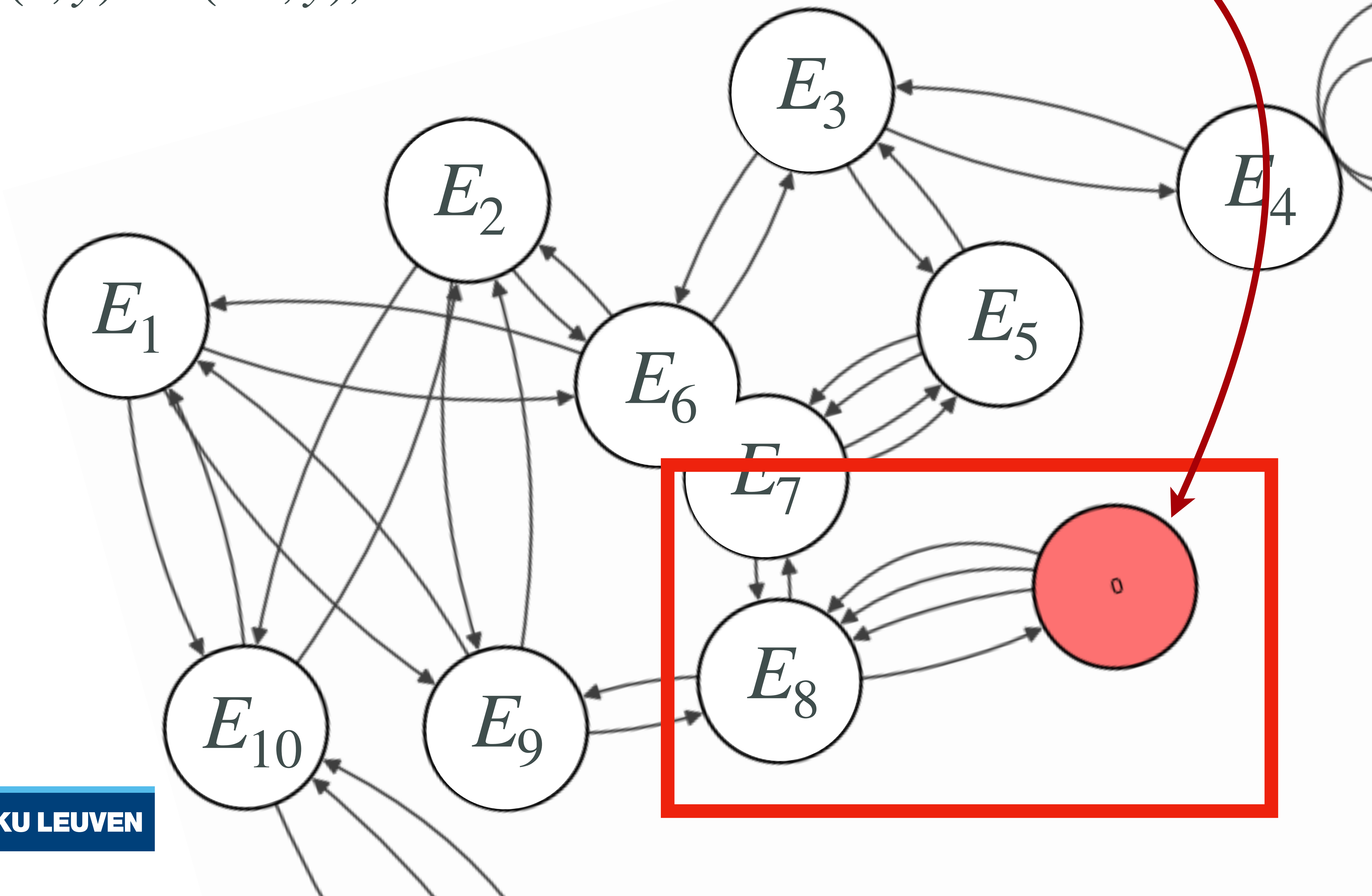


PART 3
AUTOMS.

Automorphisms ruin the regularity of the graph

$$E_0 : y^2 = x^3 + 1$$

$$\omega : (x, y) \mapsto (\omega x, y), \quad \omega^3 = 1$$



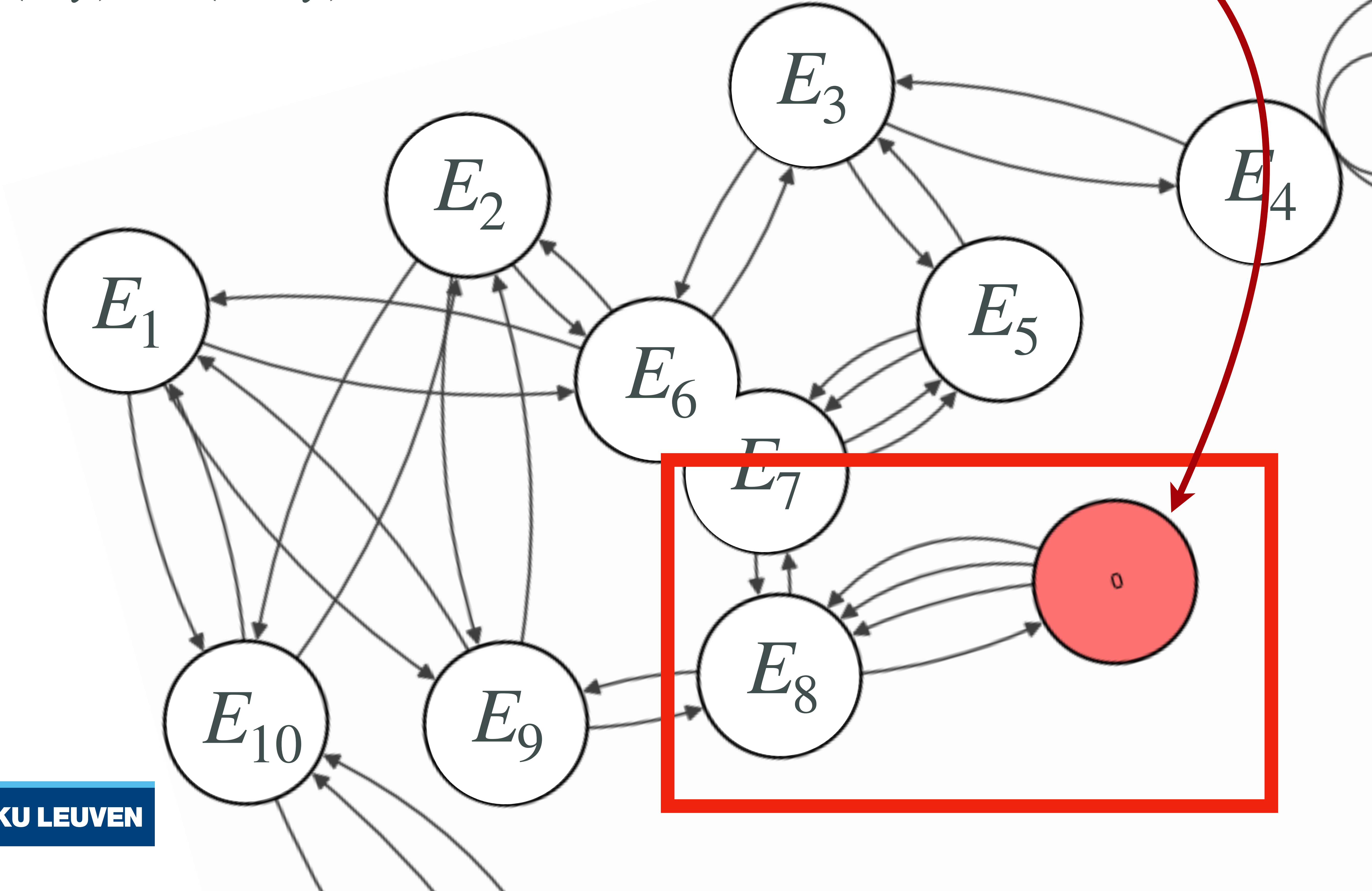
Automorphisms ruin the regularity of the graph

AUTOMORPHISM

Degree-1 isogeny $\alpha : E \to E$
(isomorphism to itself)

$E_0 : y^2 = x^3 + 1$

$\omega : (x, y) \mapsto (\omega x, y), \quad \omega^3 = 1$



PART 3
AUTOMS.

Automorphisms ruin the regularity of the graph

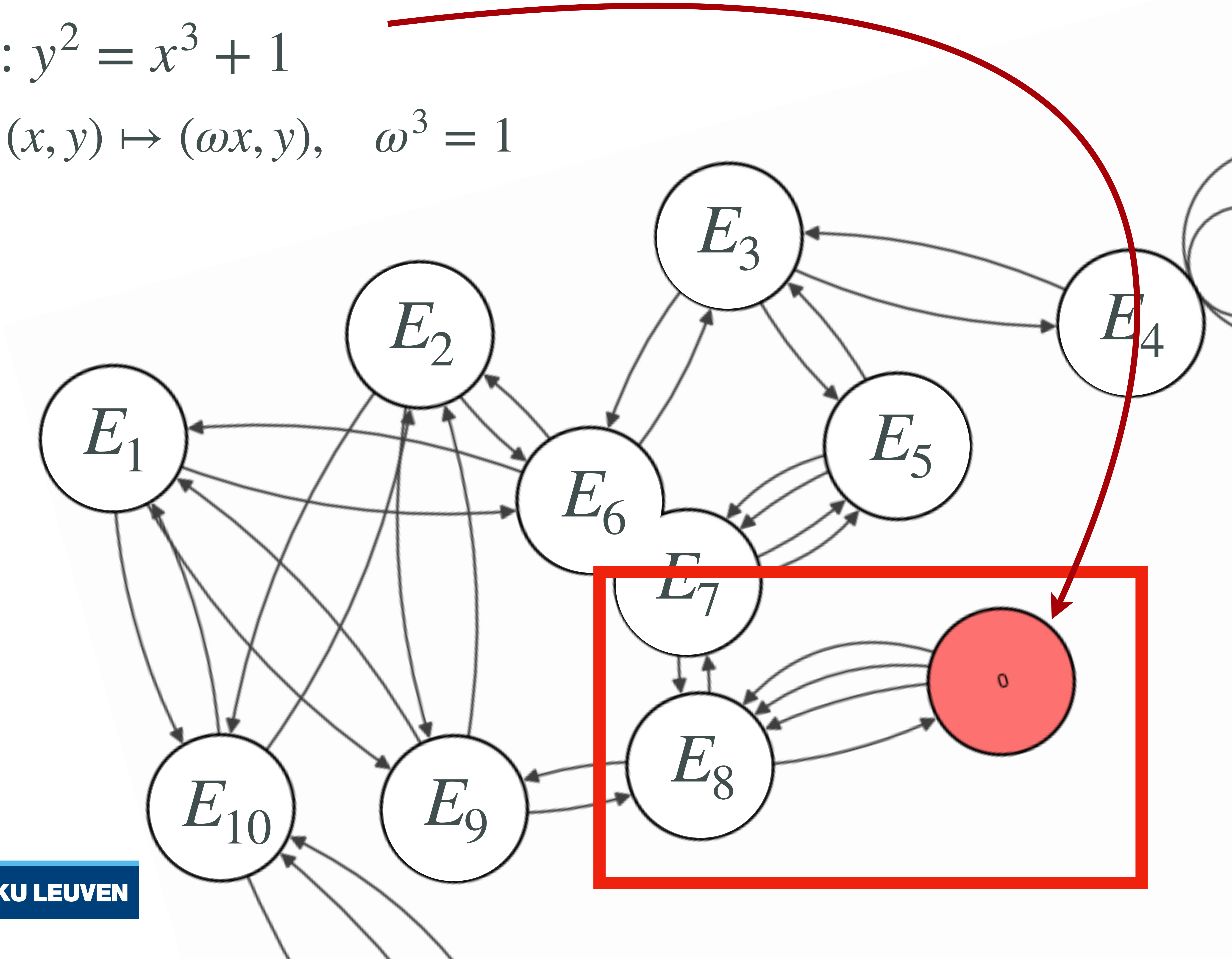
AUTOMORPHISM

Degree-1 isogeny $\alpha : E \to E$
(isomorphism to itself)

!

ω ruins edges:
induces isomorphism on
kernels of 2-isogenies,
$\ker \varphi_1 \cong \ker \varphi_2 \cong \ker \varphi_3$

$$E_0 : y^2 = x^3 + 1$$
$$\omega : (x, y) \mapsto (\omega x, y), \quad \omega^3 = 1$$



PART 3
AUTOMS.

Dimension 2 has non-negligible automorphisms!

Dimension
1

Dimension
2

PART 3
AUTOMS.

Dimension 2 has non-negligible automorphisms!

Dimension 1

out of approx. p curves in graph,
only **2** have non-trivial autom.

Dimension 2

Dimension 2 has non-negligible automorphisms!

Dimension 1

out of approx. p curves in graph, only **2** have non-trivial autom.

✓ **essentially no impact!**

✓ **just ignore!**

Dimension 2

PART 3
AUTOMS.

Dimension 2 has non-negligible automorphisms!

Dimension 1

out of approx. p curves in graph, only **2** have non-trivial autom.

✓ essentially no impact!

✓ just ignore!

Dimension 2

out of approx. p^3 nodes in graph, at least p^2 have non-triv. autom.

PART 3
AUTOMS.

Dimension 2 has non-negligible automorphisms!

Dimension 1

out of approx. p curves in graph, only **2** have non-trivial autom.

✓ essentially no impact!

✓ just ignore!

Dimension 2

out of approx. p^3 nodes in graph, at least p^2 have non-triv. autom.

✗ significant impact!

PART 3
AUTOMS.

Dimension 2 has non-negligible automorphisms!

Dimension 1

out of approx. p curves in graph,
only **2** have non-trivial autom.

essentially no impact!

just ignore!

Dimension 2

out of approx. p^3 nodes in graph,
at least p^2 have non-triv. autom.

significant impact!

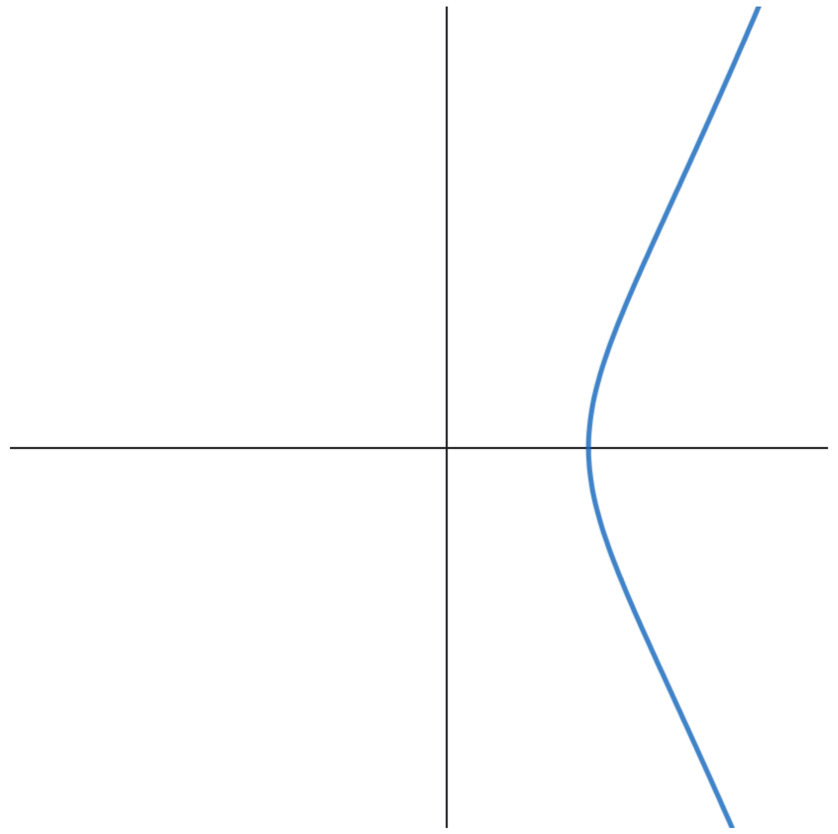
careful analysis!

Example: the Jacobian with $\mathrm{RA}(J) = \mathbb{Z}/5\mathbb{Z}$

$$C : y^2 = x^5 - 1$$

$$\zeta \in \mu_5$$

$$\zeta^{(5)} : (x, y) \mapsto (\zeta x, y)$$

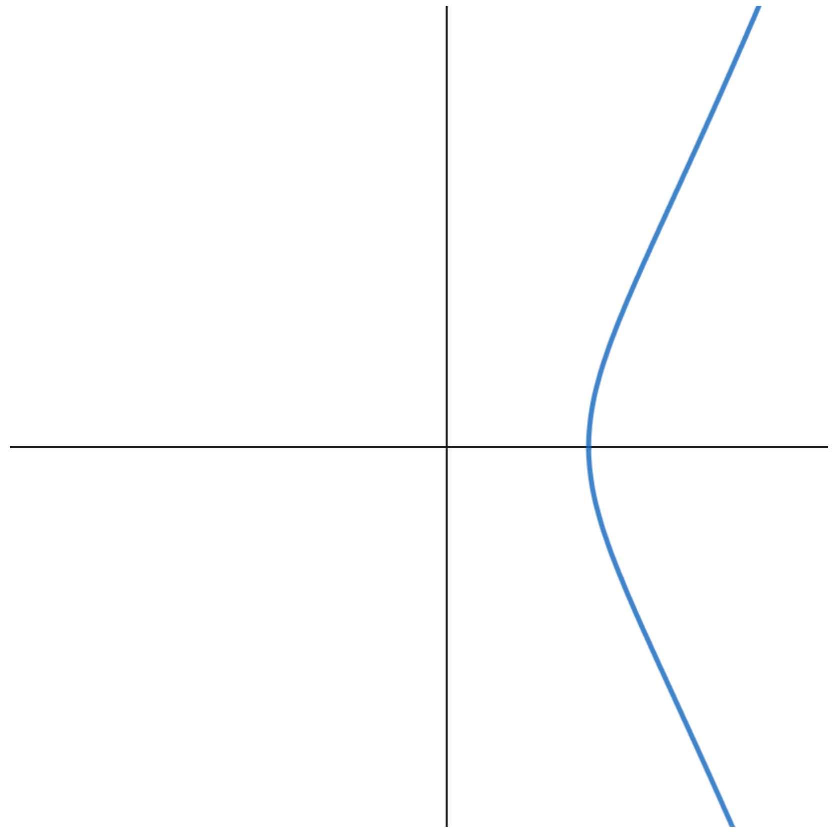


Example: the Jacobian with $\mathrm{RA}(J) = \mathbb{Z}/5\mathbb{Z}$

$$C : y^2 = x^5 - 1$$

$$\zeta \in \mu_5$$

$$\zeta^{(5)} : (x, y) \mapsto (\zeta x, y)$$



Q

How does the induced automorphism

$$\zeta_*^{(5)} : J_C \to J_C$$

act on level structures (J_C, G)?

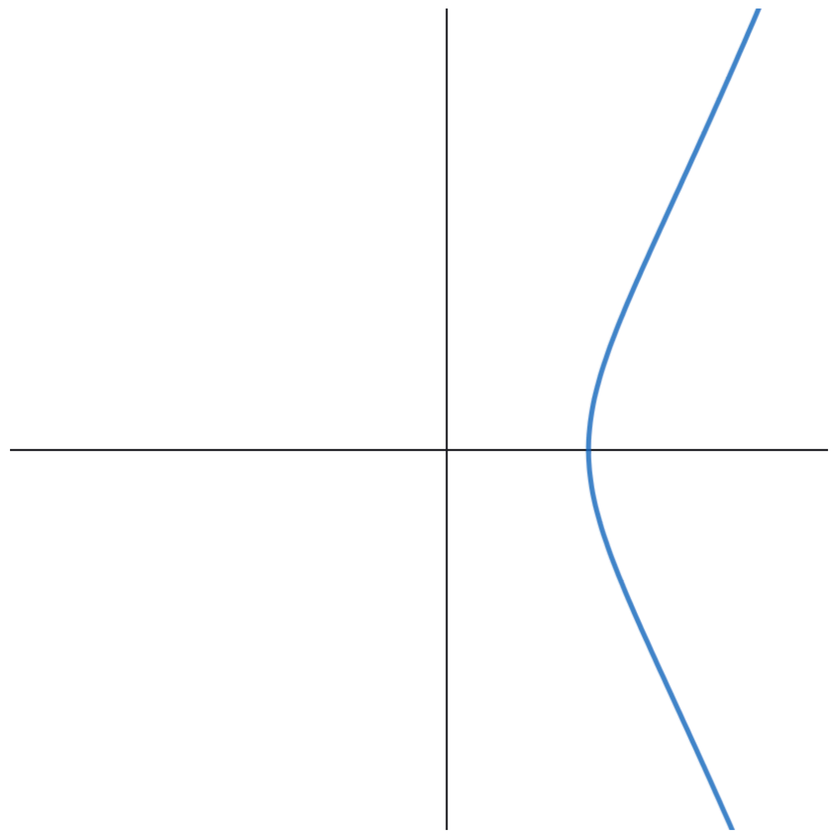
($G \subset J[\ell]$ max isotropic)

Example: the Jacobian with $\mathrm{RA}(J) = \mathbb{Z}/5\mathbb{Z}$

$$C : y^2 = x^5 - 1$$

$$\zeta \in \mu_5$$

$$\zeta^{(5)} : (x, y) \mapsto (\zeta x, y)$$



Q

How does the induced automorphism

$$\zeta_*^{(5)} : J_C \to J_C$$

act on level structures (J_C, G)?

($G \subset J[\ell]$ max isotropic)

Theorem. Can represent $\zeta_*^{(5}$ on $J[\ell]$ as $M \in \mathrm{GL}_4(\mathbb{F}_\ell)$.

Given M, can derive number of (ℓ, ℓ)-level structures up to isomorphism

$$\frac{1}{5}(\ell^3 + \ell^2 + \ell + 17) \quad \text{if } \ell \equiv 1 \bmod 5$$

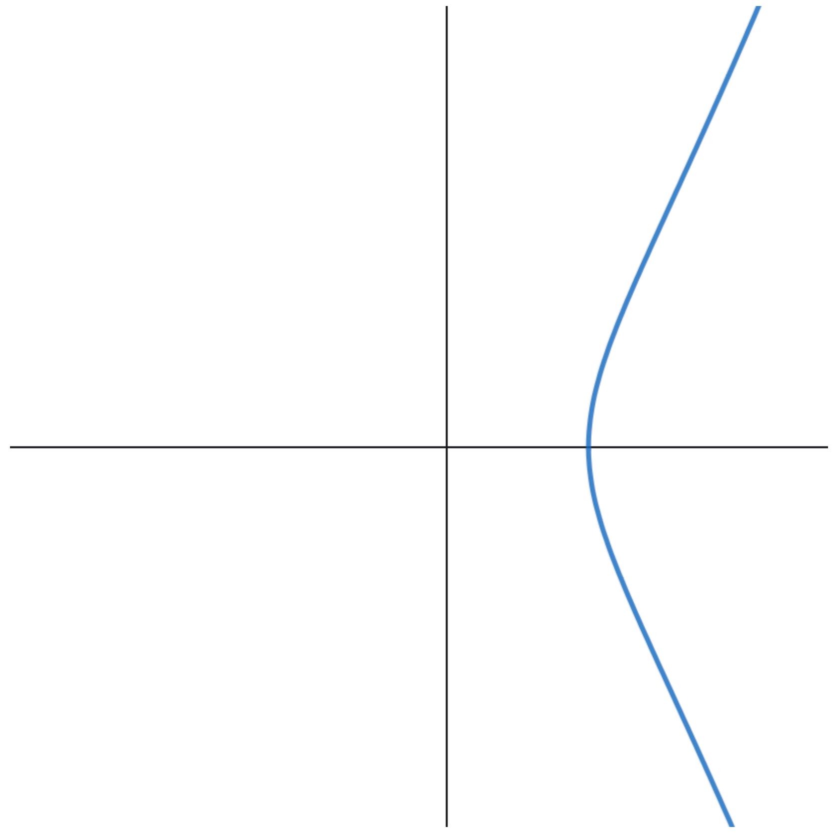
$$\frac{1}{5}(\ell^3 + \ell^2 + \ell + 1) \quad \text{if } \ell \equiv 4 \bmod 5$$

Example: the Jacobian with $\mathrm{RA}(J) = \mathbb{Z}/5\mathbb{Z}$

$$C : y^2 = x^5 - 1$$

$$\zeta \in \mu_5$$

$$\zeta^{(5)} : (x, y) \mapsto (\zeta x, y)$$



Q

How does the induced automorphism

$$\zeta_*^{(5)} : J_C \to J_C$$

act on level structures (J_C, G)?

($G \subset J[\ell]$ max isotropic)

Theorem. Can represent $\zeta_*^{(5}$ on $J[\ell]$ as $M \in \mathrm{GL}_4(\mathbb{F}_\ell)$.

Given M, can derive number of (ℓ, ℓ)-level structures up to isomorphism

$$\frac{1}{5}(\ell^3 + \ell^2 + \ell + 17) \quad \text{if } \ell \equiv 1 \bmod 5$$

$$\frac{1}{5}(\ell^3 + \ell^2 + \ell + 1) \quad \text{if } \ell \equiv 4 \bmod 5$$

$$\begin{pmatrix} \zeta & 0 & 0 & 0 \\ 0 & \zeta^2 & 0 & 0 \\ 0 & 0 & \zeta^4 & 0 \\ 0 & 0 & 0 & \zeta^3 \end{pmatrix}$$

$\ell \equiv 1 \bmod 5$

$$\begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & \zeta + \zeta^4 & 0 \\ 0 & 1 & 0 & \zeta^2 + \zeta^3 \end{pmatrix}$$

$\ell \equiv 4 \bmod 5$

PART 1
GRAPHS

PART 2
CYCLES

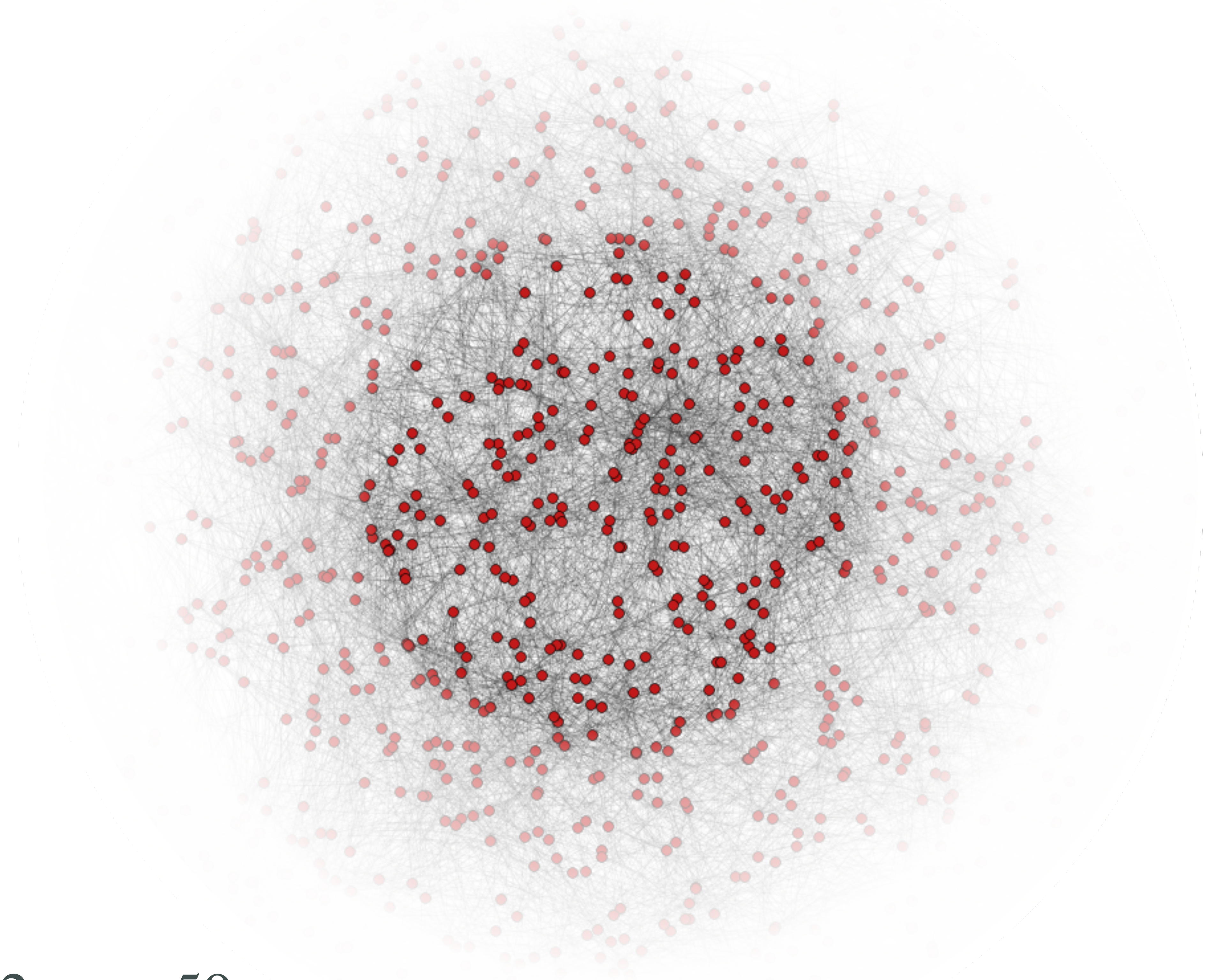
PART 3
AUTOMS.

Definition 11. The superspecial (ℓ, ℓ)-isogeny digraph $\mathbf{G}_{2,p}(\ell)$ is the graph with

- nodes V, the pairs (A, G) with p.p.a.s. A and $G \subset A[\ell]$ max. isotropic, up to isomorphism
- edges E, the **good** (ℓ, ℓ)**-extensions**: isogenies $\Phi : A \to A'$ with $\ker \Phi \cap G = \{\mathbf{0}_A\}$.

Definition 11. The superspecial (ℓ, ℓ)-isogeny digraph $\mathbf{G}_{2,p}(\ell)$ is the graph with

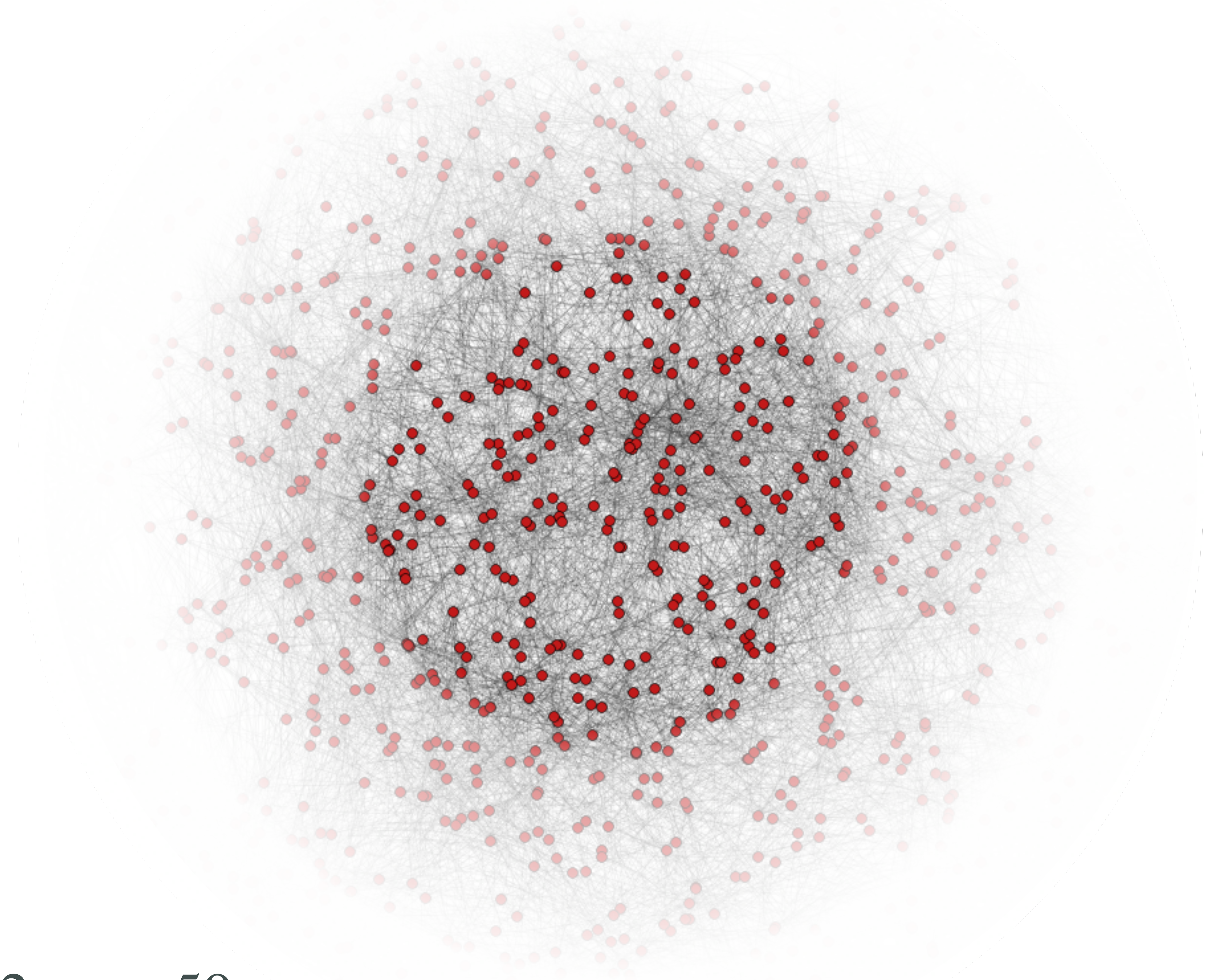
- nodes V, the pairs (A, G) with p.p.a.s. A and $G \subset A[\ell]$ max. isotropic, up to isomorphism
- edges E, the **good** (ℓ, ℓ)**-extensions**: isogenies $\Phi : A \to A'$ with $\ker \Phi \cap G = \{\mathbf{0}_A\}$.



$\ell = 2$, $p = 59$

Definition 11. The superspecial (ℓ, ℓ)-isogeny digraph $\mathbf{G}_{2,p}(\ell)$ is the graph with

- nodes V, the pairs (A, G) with p.p.a.s. A and $G \subset A[\ell]$ max. isotropic, up to isomorphism
- edges E, the **good** (ℓ, ℓ)**-extensions**: isogenies $\Phi : A \to A'$ with $\ker \Phi \cap G = \{\mathbf{0}_A\}$.



$\ell = 2,\ p = 59$

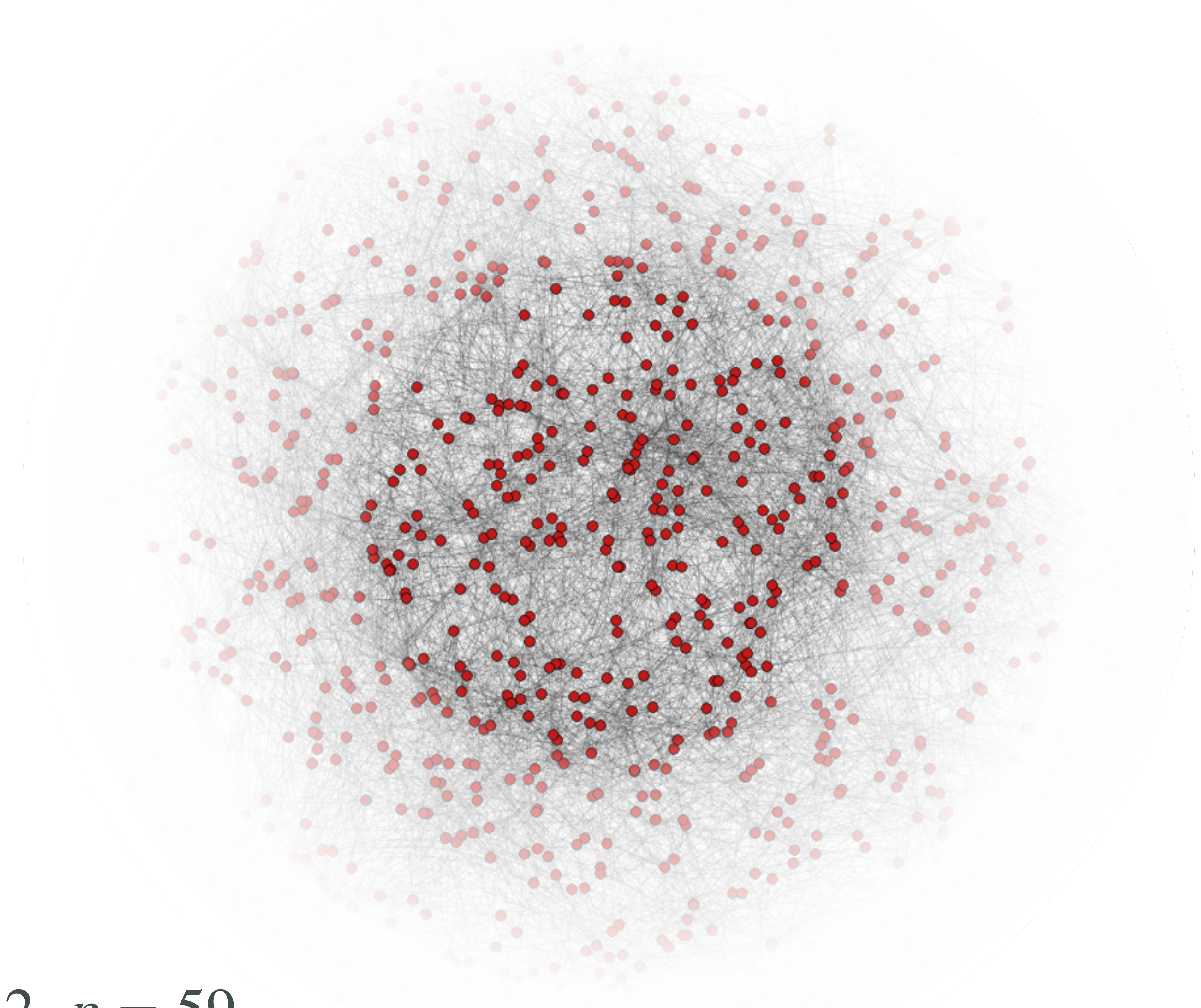
1 Again regular!

2 Connected?

3 Ramanujan, for $\ell = 2\ldots$

Definition 11. The superspecial (ℓ, ℓ)-isogeny digraph $\mathbf{G}_{2,p}(\ell)$ is the graph with

- nodes V, the pairs (A, G) with p.p.a.s. A and $G \subset A[\ell]$ max. isotropic, up to isomorphism
- edges E, the **good** (ℓ, ℓ)**-extensions**: isogenies $\Phi : A \to A'$ with $\ker \Phi \cap G = \{\mathbf{0}_A\}$.



$\ell = 2,\ p = 59$

1 Again regular!

2 Connected?

3 Ramanujan, for $\ell = 2$…

! Graph is **much** larger, harder to compute!

! Eigenvalues are very strange…