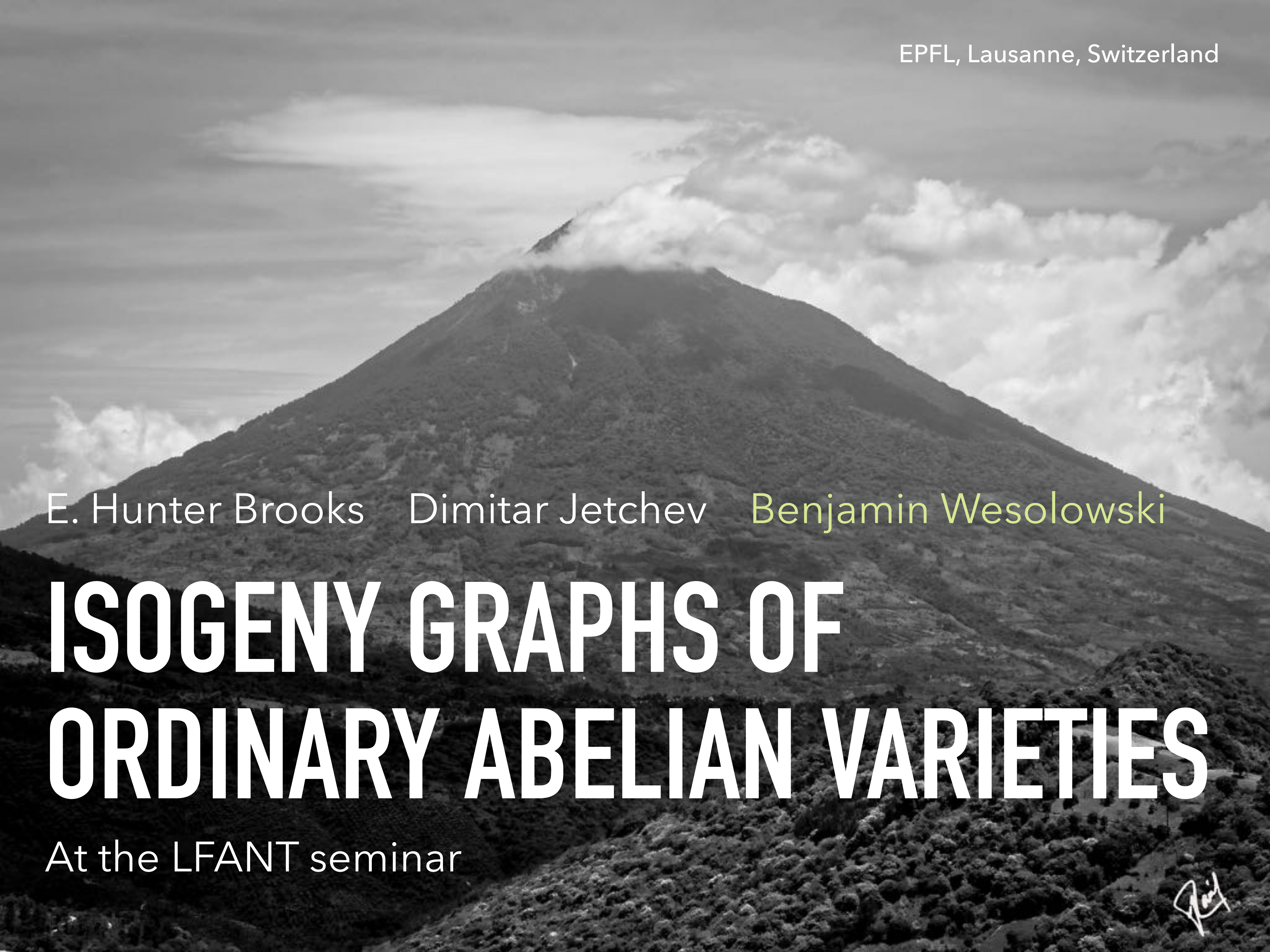


EPFL, Lausanne, Switzerland

E. Hunter Brooks   Dimitar Jetchev   Benjamin Wesolowski

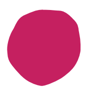
ISOGENY GRAPHS OF ORDINARY ABELIAN VARIETIES

At the LFANT seminar

AN NON-VIOLENT INTRODUCTION TO

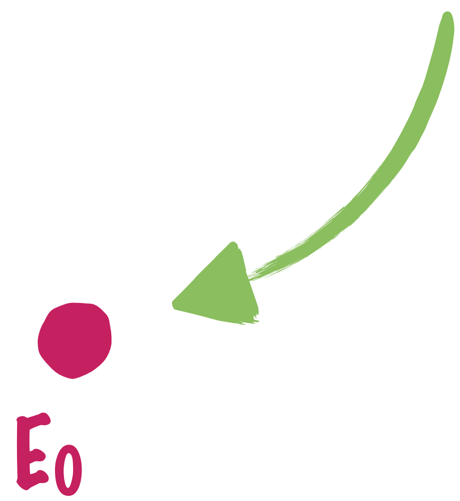
ISOGENY GRAPHS

ISOGENY GRAPHS OF ORDINARY ELLIPTIC CURVES

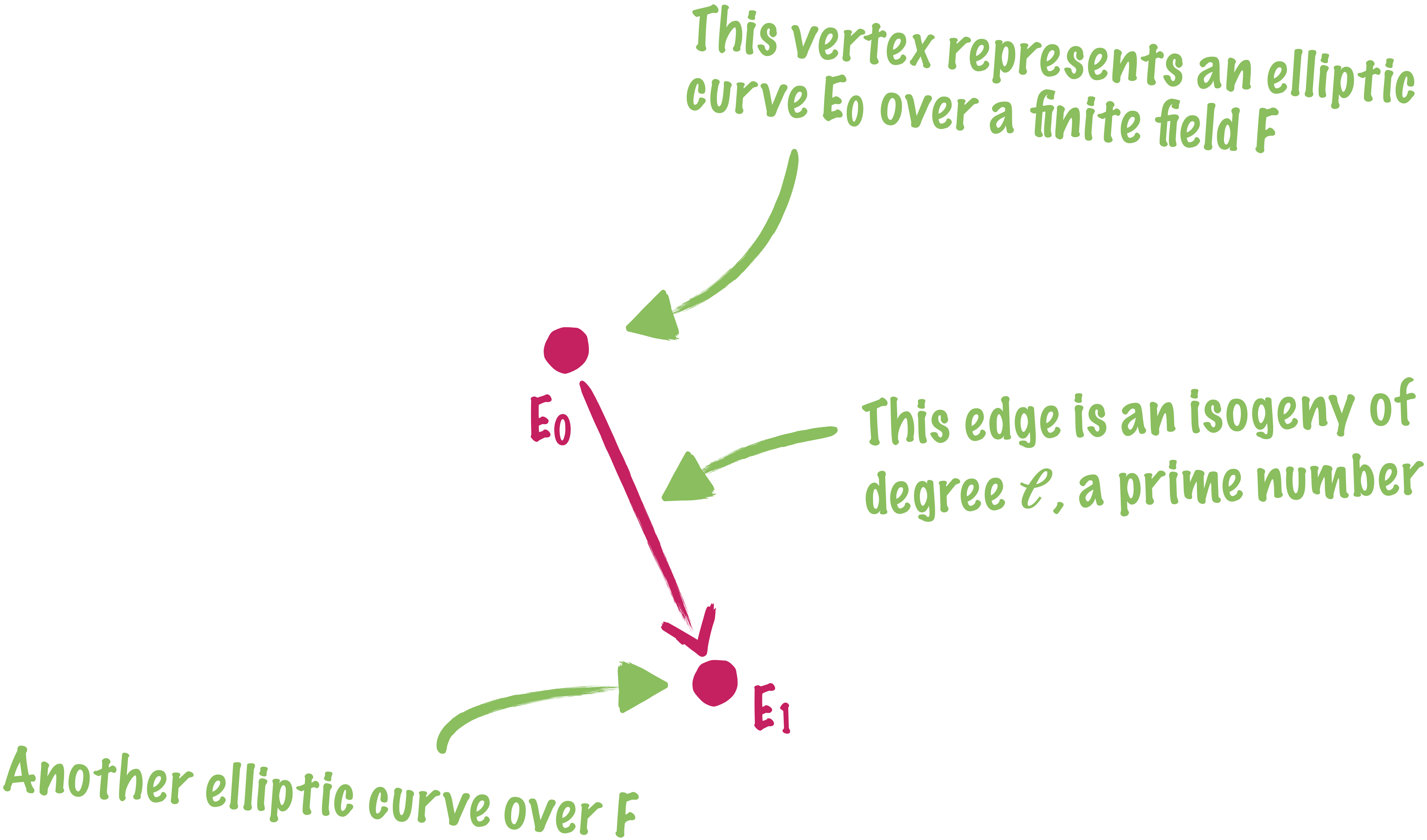


ISOGENY GRAPHS OF ORDINARY ELLIPTIC CURVES

This vertex represents an elliptic curve E_0 over a finite field F



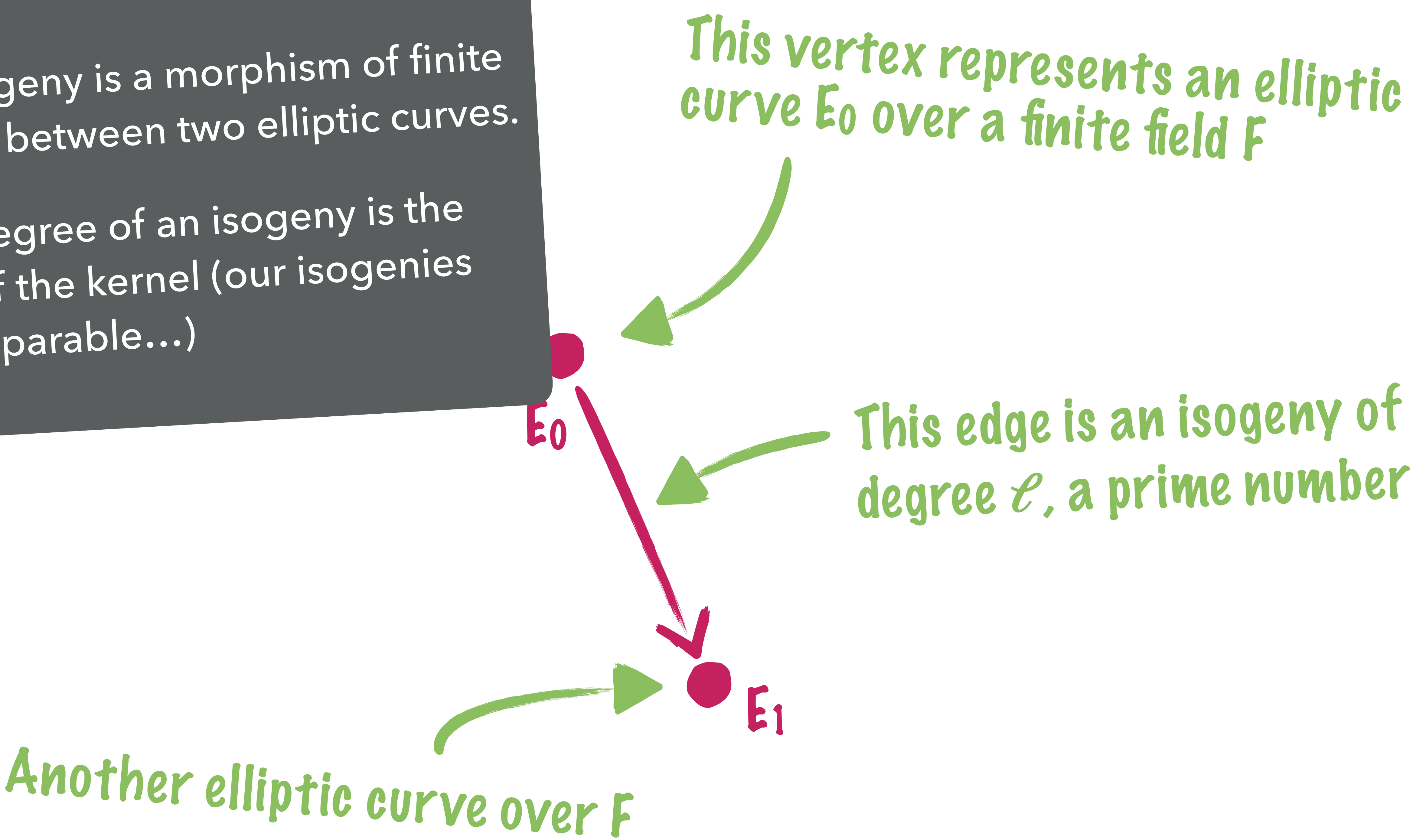
ISOGENY GRAPHS OF ORDINARY ELLIPTIC CURVES



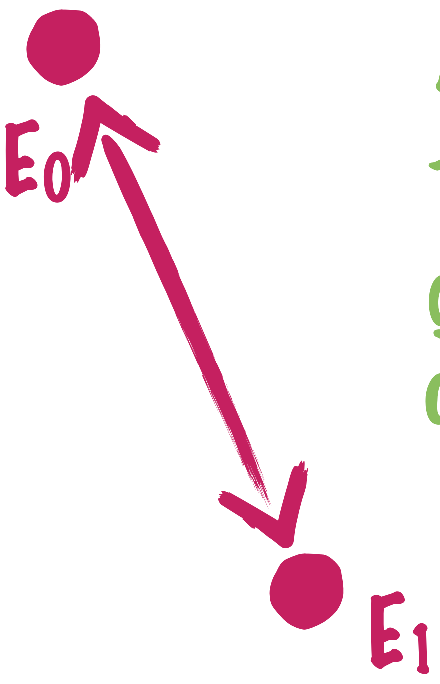
ISOGENY GRAPHS OF ORDINARY ELLIPTIC CURVES

An isogeny is a morphism of finite kernel between two elliptic curves.

The degree of an isogeny is the size of the kernel (our isogenies are separable…)



ISOGENY GRAPHS OF ORDINARY ELLIPTIC CURVES



Any isogeny has a dual of the same degree (here, ℓ) going in the opposite direction

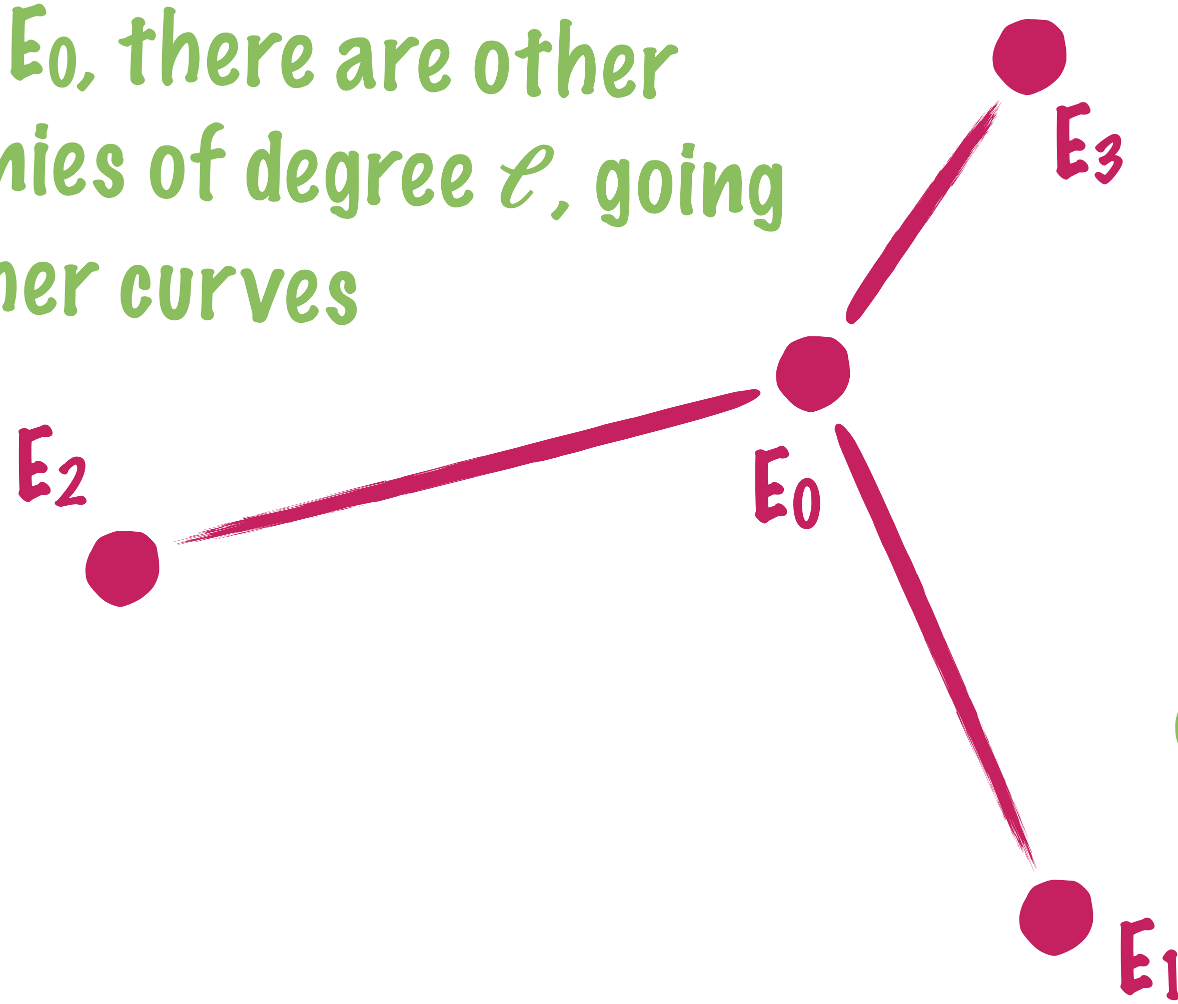
ISOGENY GRAPHS OF ORDINARY ELLIPTIC CURVES

Any isogeny has a dual of the same degree (here, ℓ) going in the opposite direction

So we represent it by a non-directed edge

ISOGENY GRAPHS OF ORDINARY ELLIPTIC CURVES

From E_0, there are other isogenies of degree ℓ, going to other curves



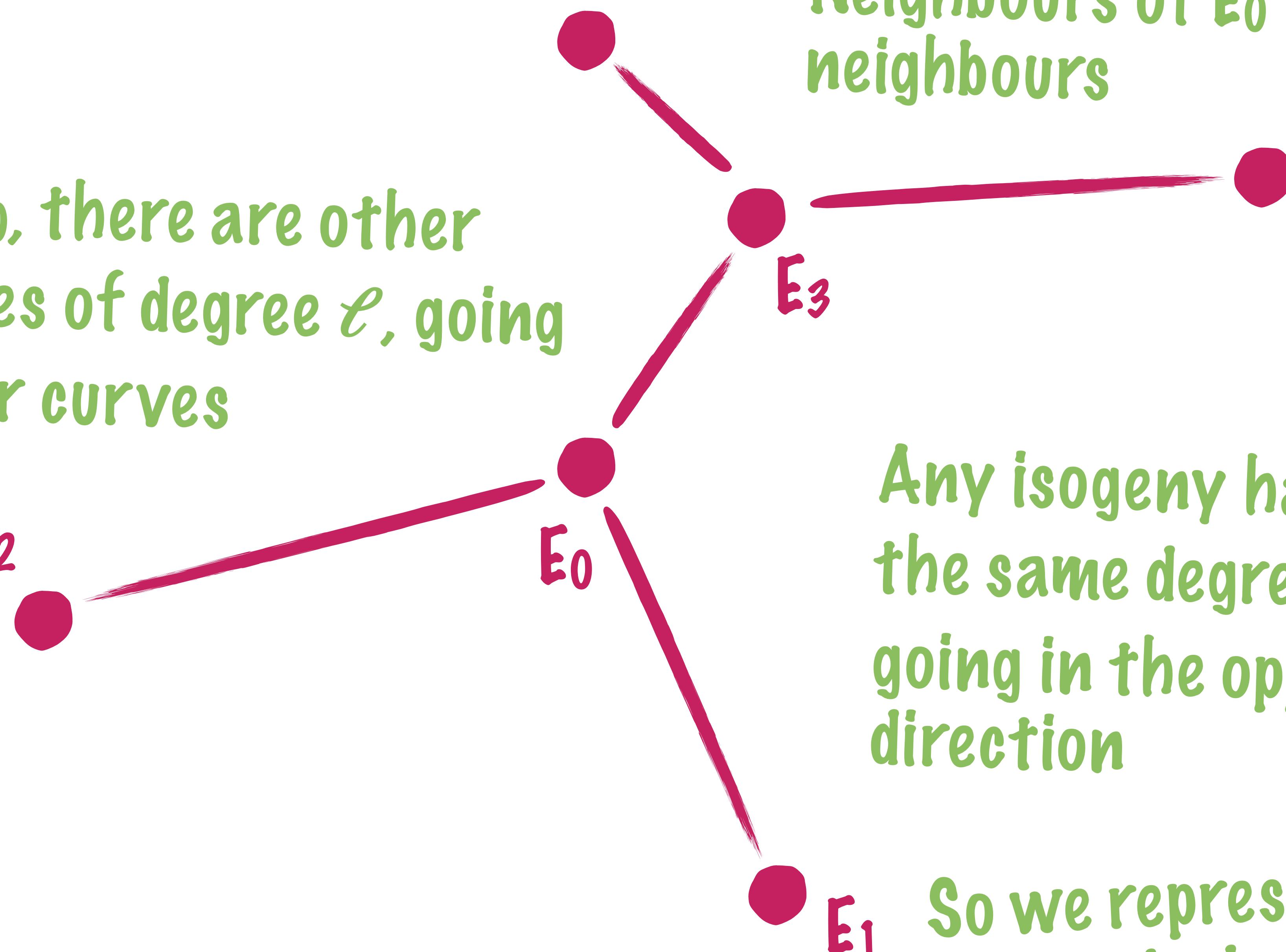
Any isogeny has a dual of the same degree (here, ℓ) going in the opposite direction

So we represent it by a non-directed edge

ISOGENY GRAPHS OF ORDINARY ELLIPTIC CURVES

Neighbours of E_0 have more neighbours

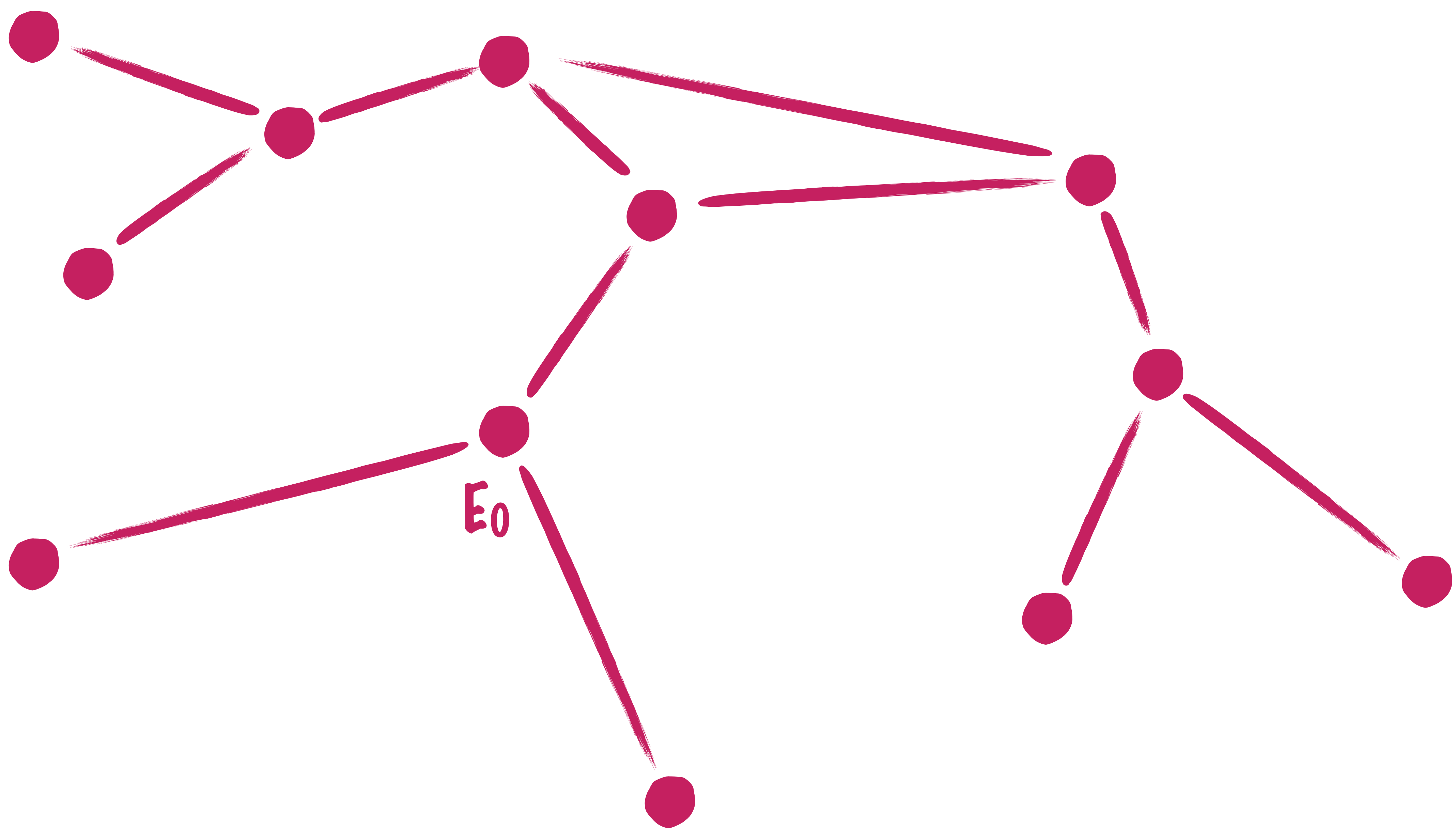
From E_0, there are other isogenies of degree ℓ, going to other curves



Any isogeny has a dual of the same degree (here, ℓ) going in the opposite direction

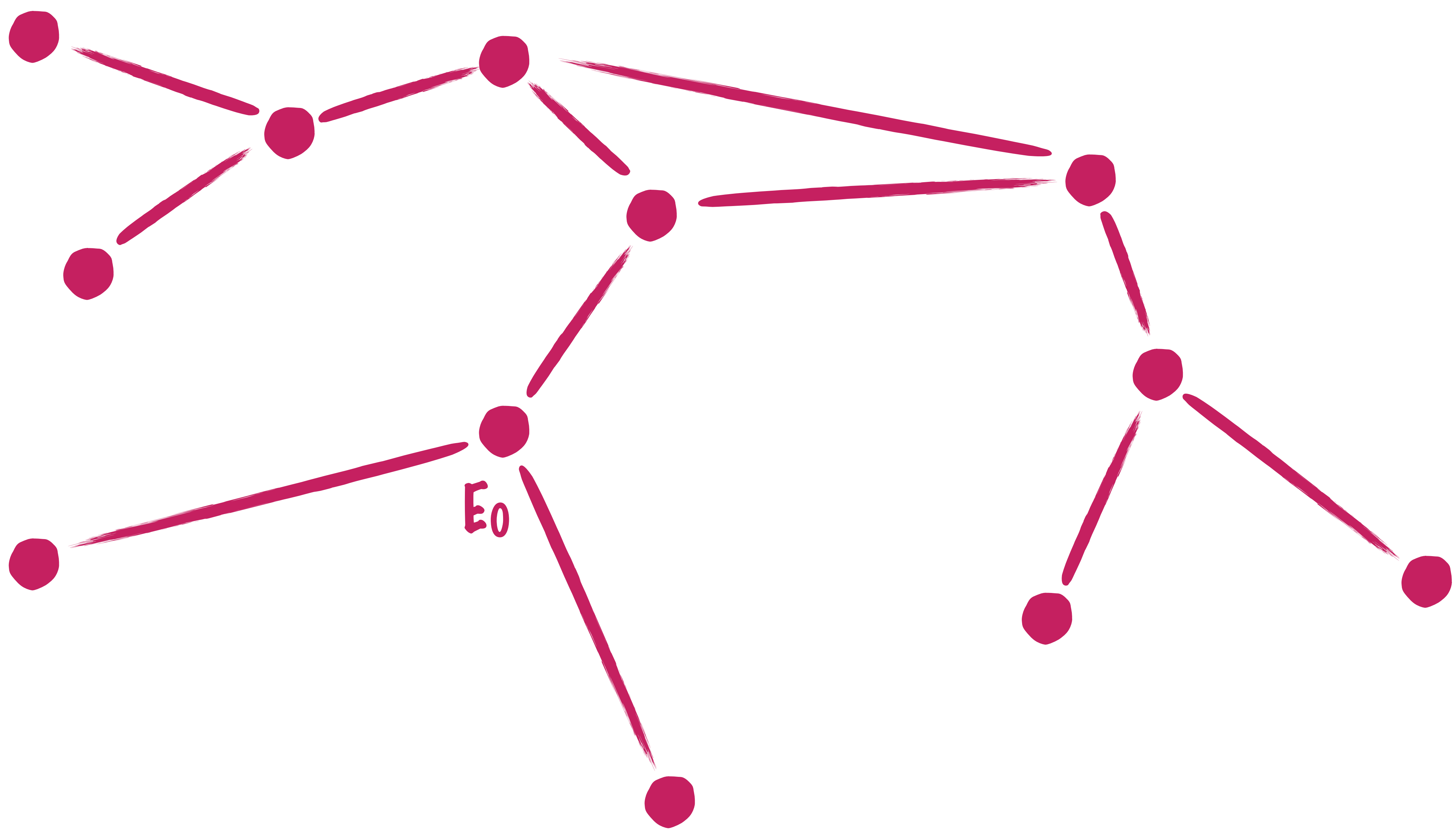
So we represent it by a non-directed edge

ISOGENY GRAPHS OF ORDINARY ELLIPTIC CURVES



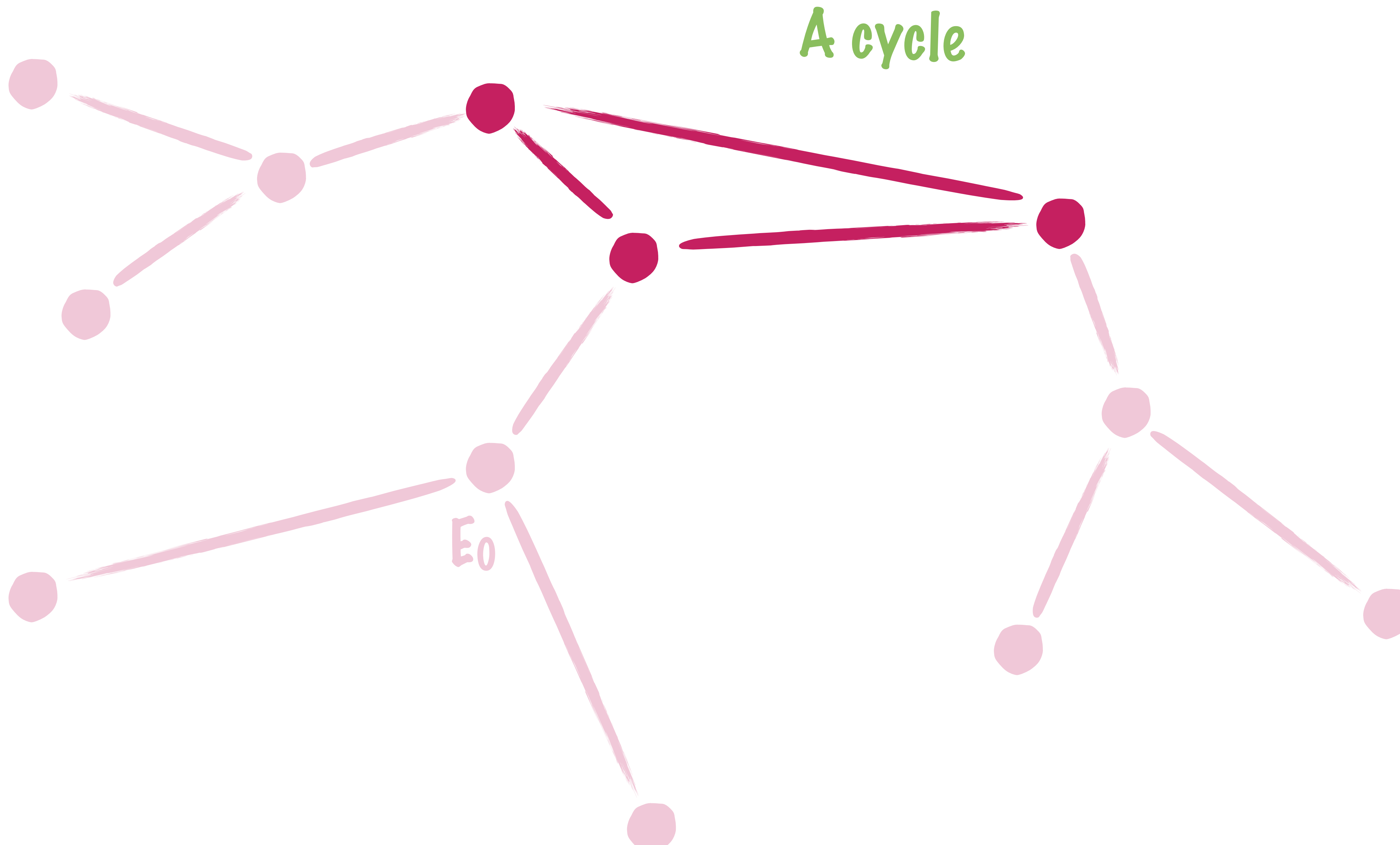
Once all the possible neighbours have been reached, we obtain the connected graph of ℓ-isogenies of E_0

ISOGENY GRAPHS OF ORDINARY ELLIPTIC CURVES



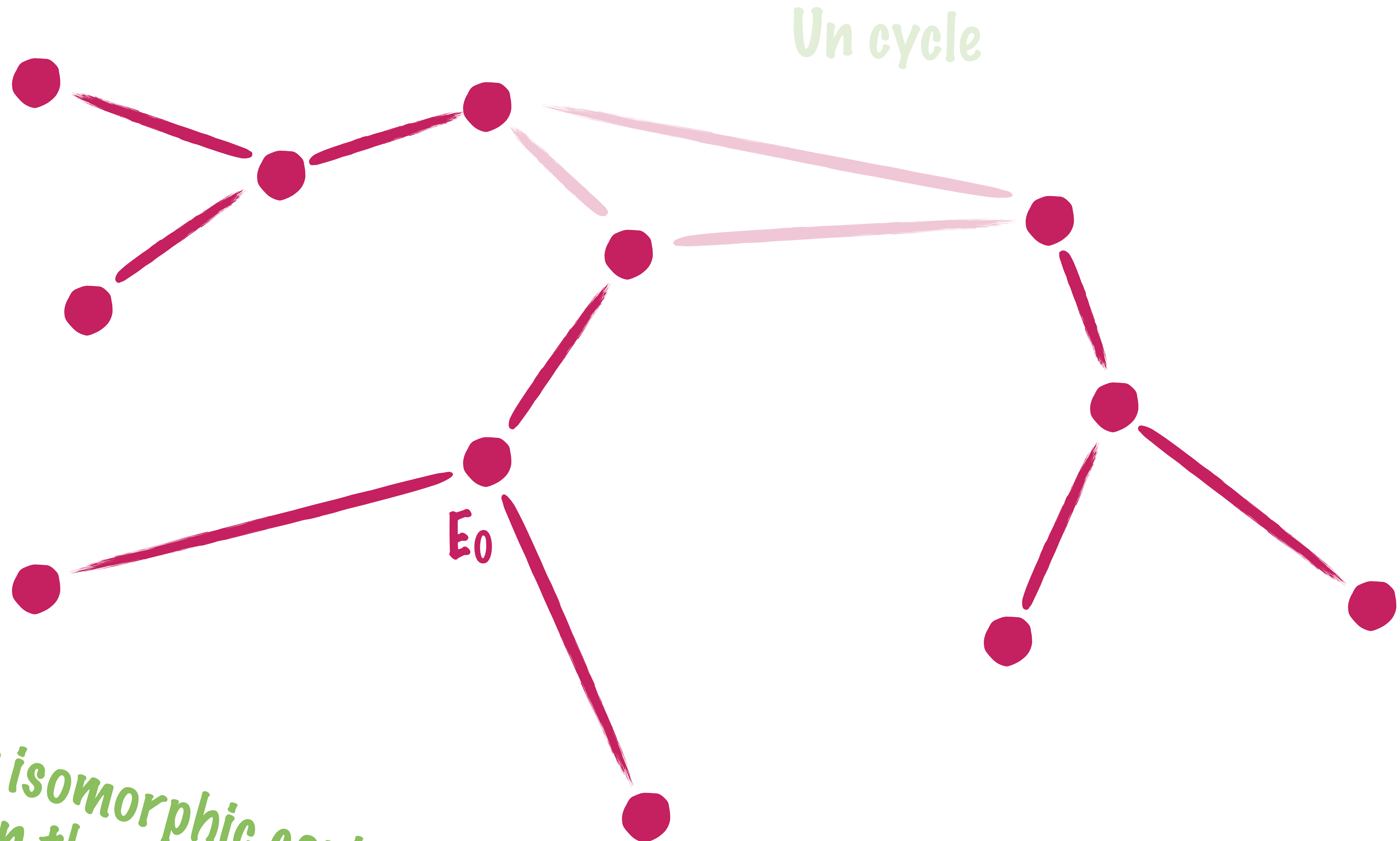
This one is a typical example!

ISOGENY GRAPHS OF ORDINARY ELLIPTIC CURVES



This one is a typical example!

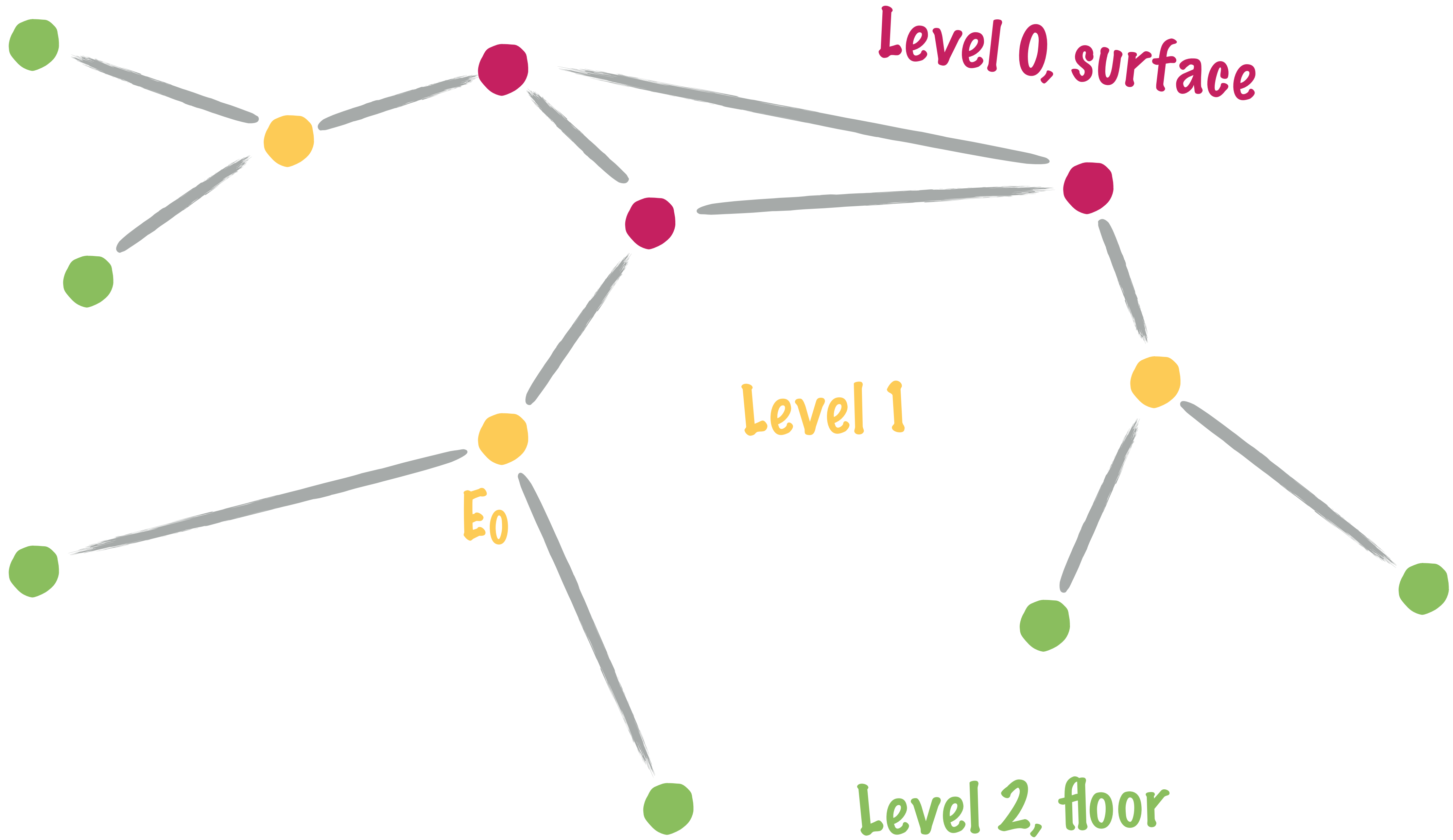
ISOGENY GRAPHS OF ORDINARY ELLIPTIC CURVES

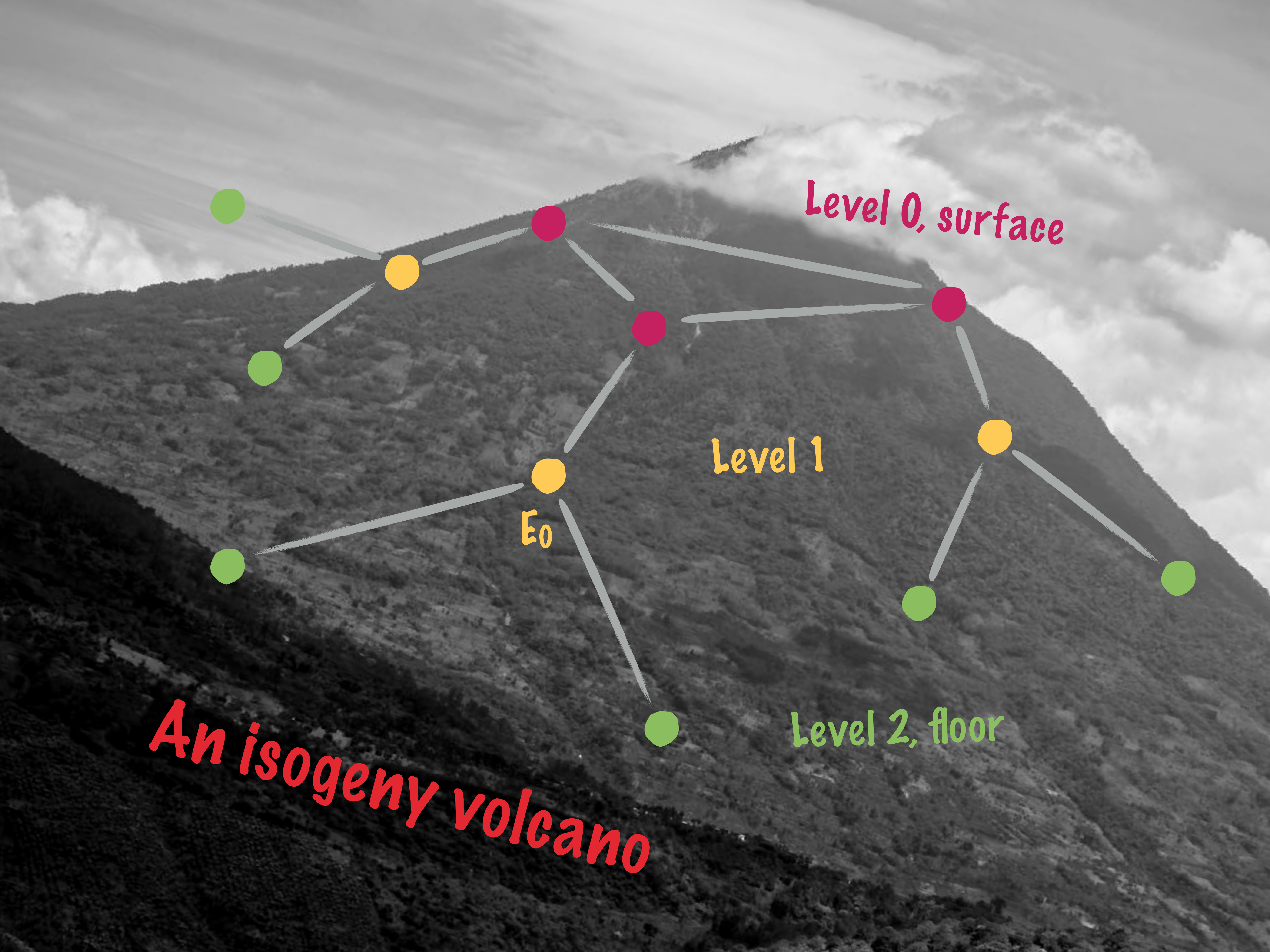


Disjoint isomorphic copies of a tree rooted on the cycle

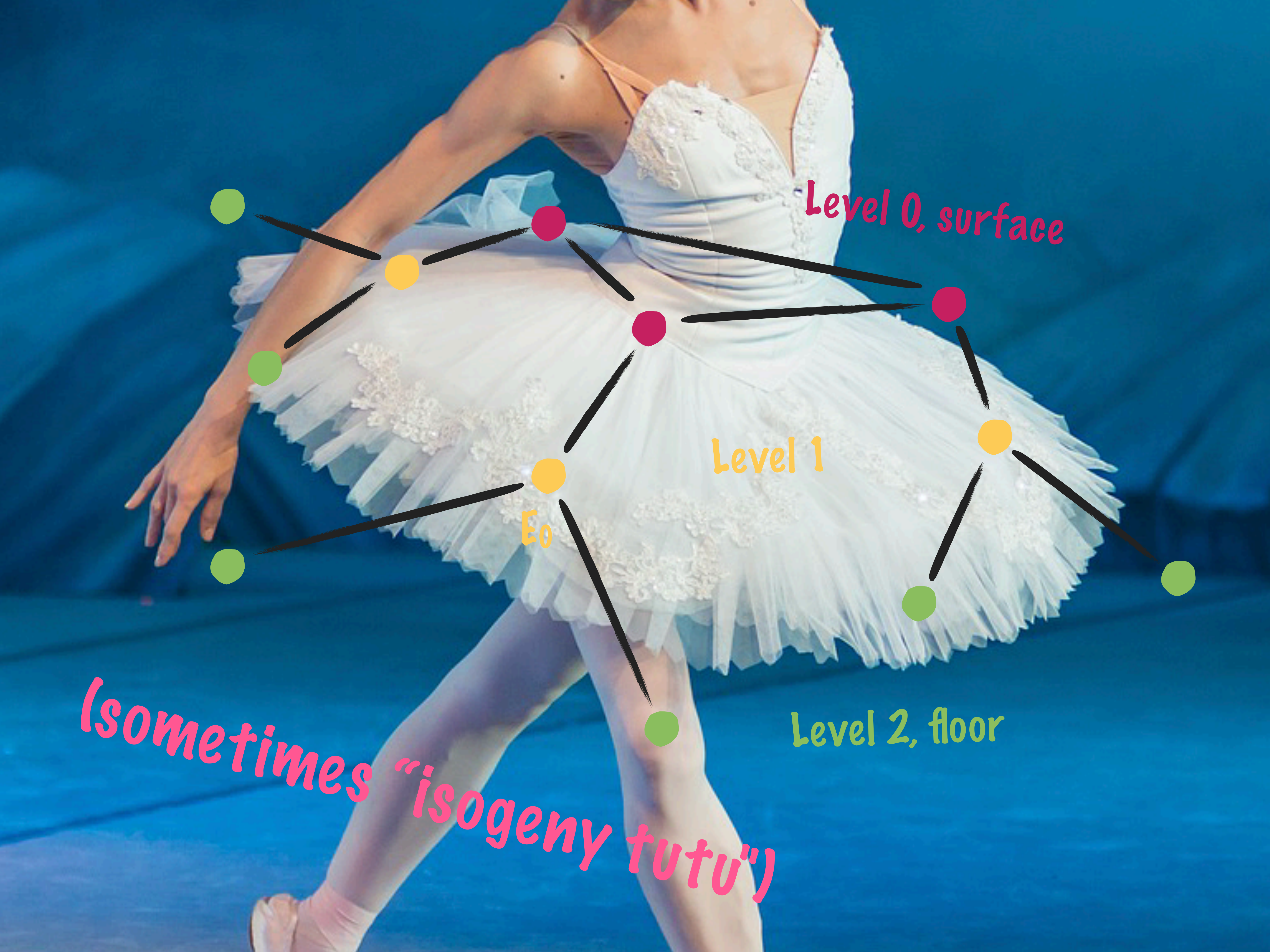
This one is a typical example!

ISOGENY GRAPHS OF ORDINARY ELLIPTIC CURVES



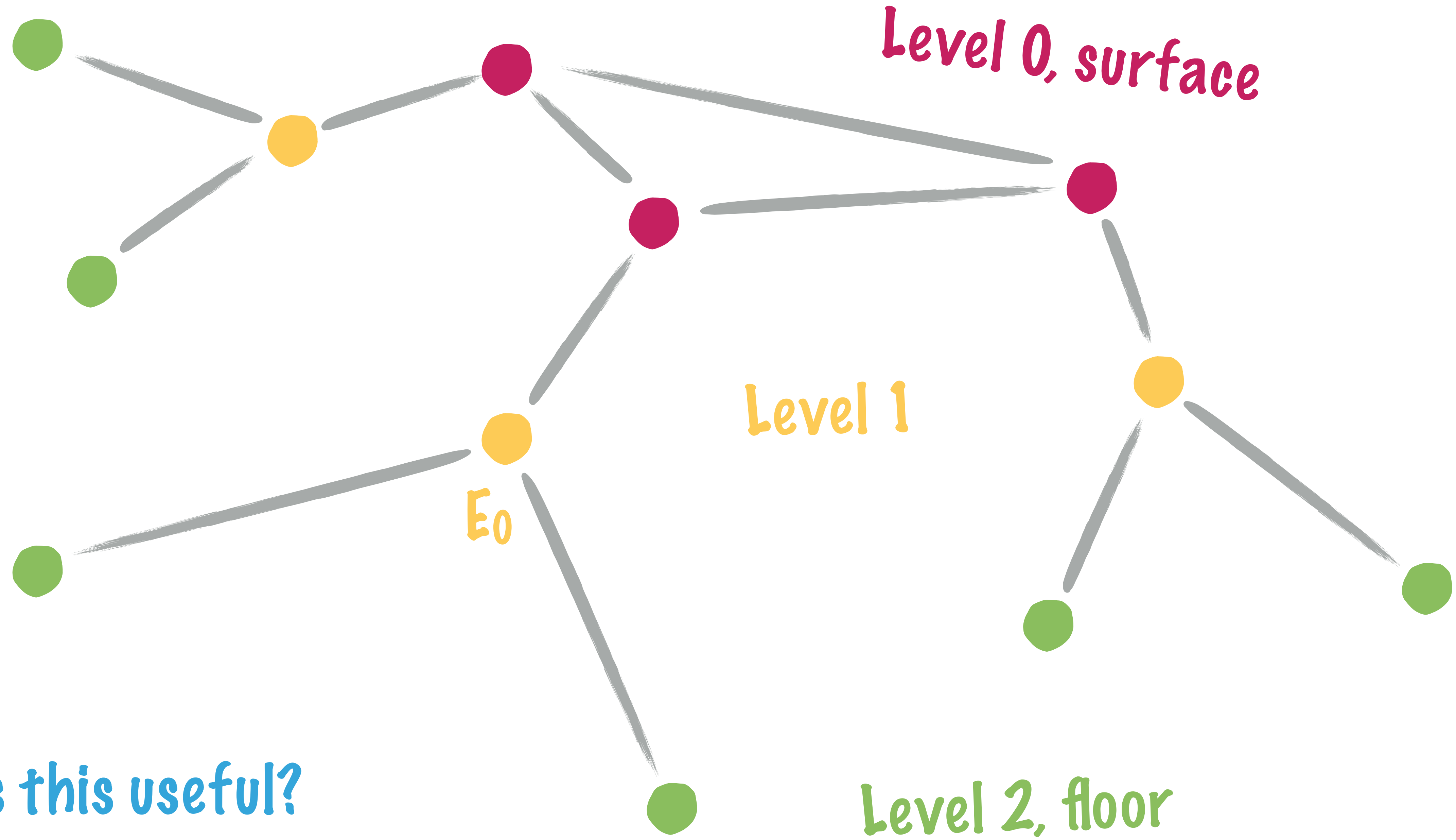


Level 0, surface
Level 1
E_0
Level 2, floor
An isogeny volcano



Level 0, surface
Level 1
E_0
Level 2, floor
(sometimes "isogeny tutu")

ISOGENY GRAPHS OF ORDINARY ELLIPTIC CURVES



Why is this useful?

By inspecting **solely** the structure of the graph, one can infer that E_0 is at "level 1" in ℓ… which tells a lot about the endomorphism ring of E_0!

APPLICATIONS

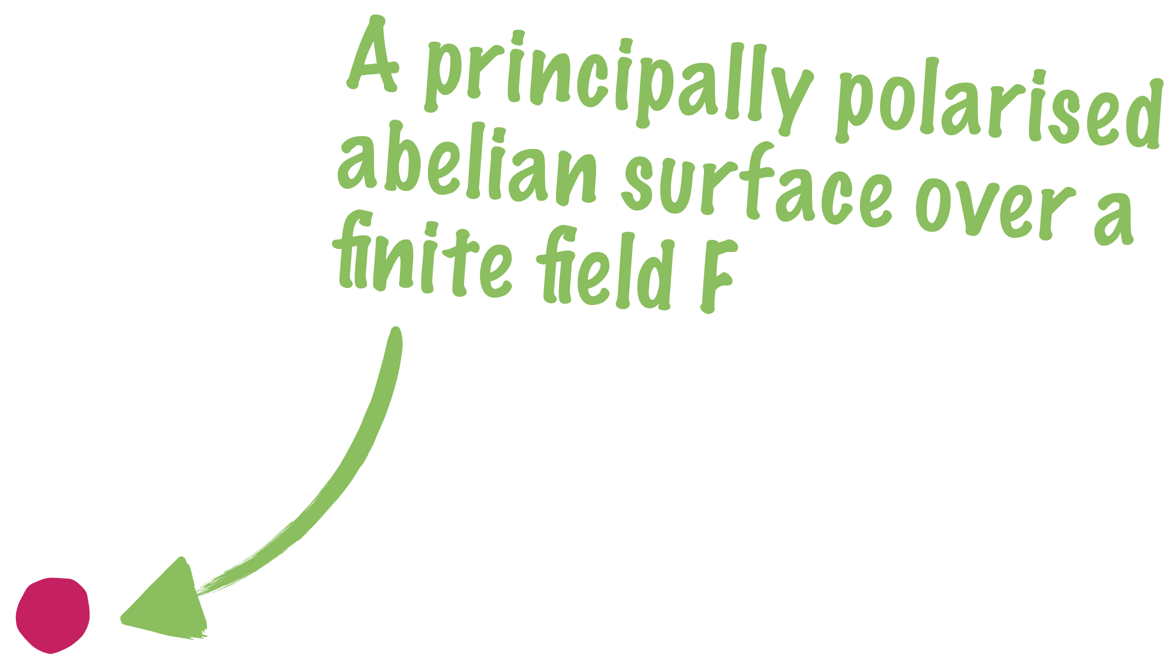
- Computing the endomorphism ring of an elliptic curve [Kohel, 1996],
- Counting points [Fouquet et Morain, 2002],
- Random self-reducibility of the discrete logarithm problem [Jao et al., 2005] (worst case to average case reduction)
- Accelerating the CM method [Sutherland 2012],
- Computing modular polynomials [Bröker et al., 2012]

GENERALISING TO ORDINARY ABELIAN VARIETIES…

- These applications motivate the search for a generalisation to other abelian varieties…

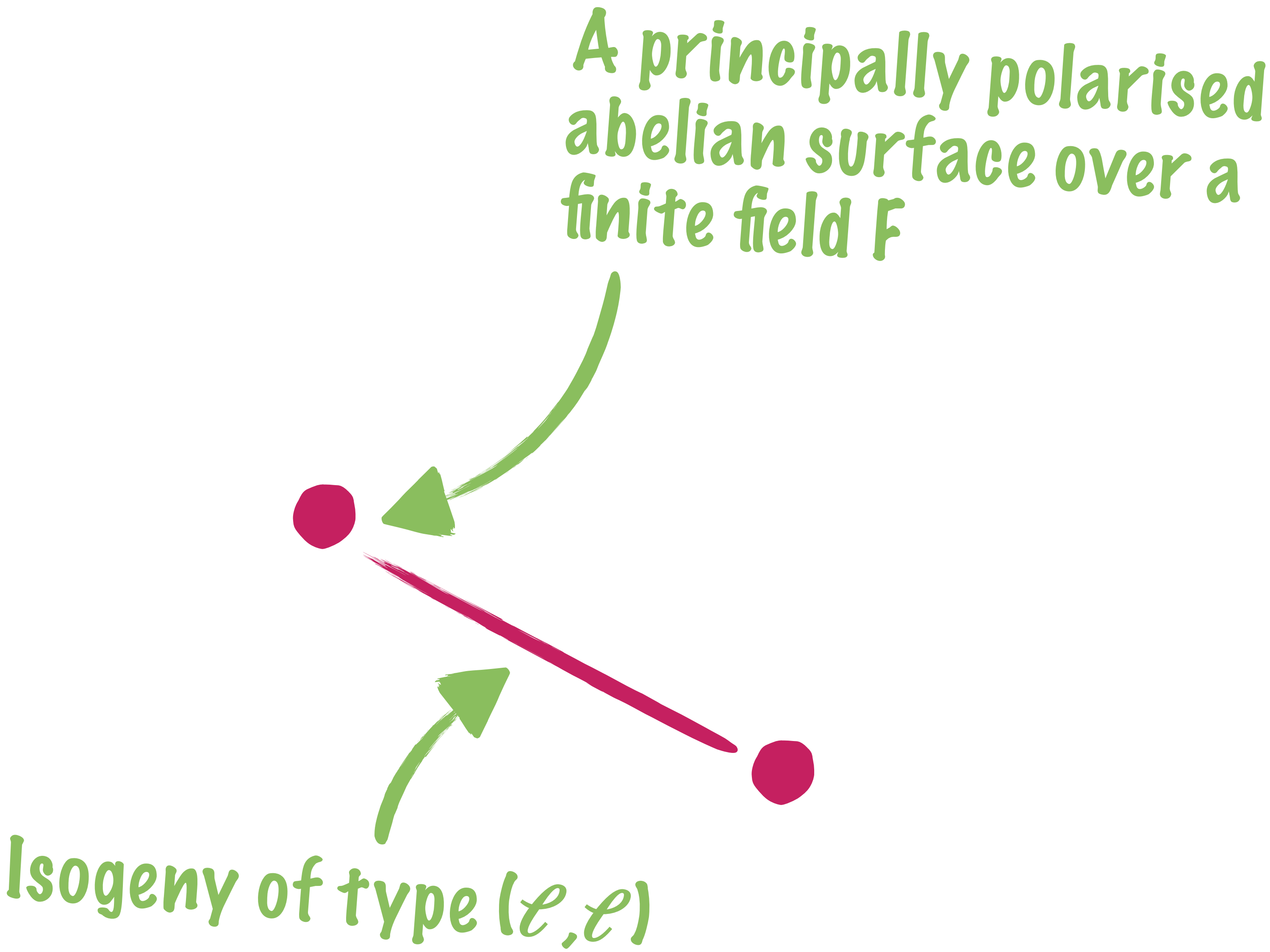
GENERALISING TO ORDINARY ABELIAN VARIETIES…

- These applications motivate the search for a generalisation to other abelian varieties…



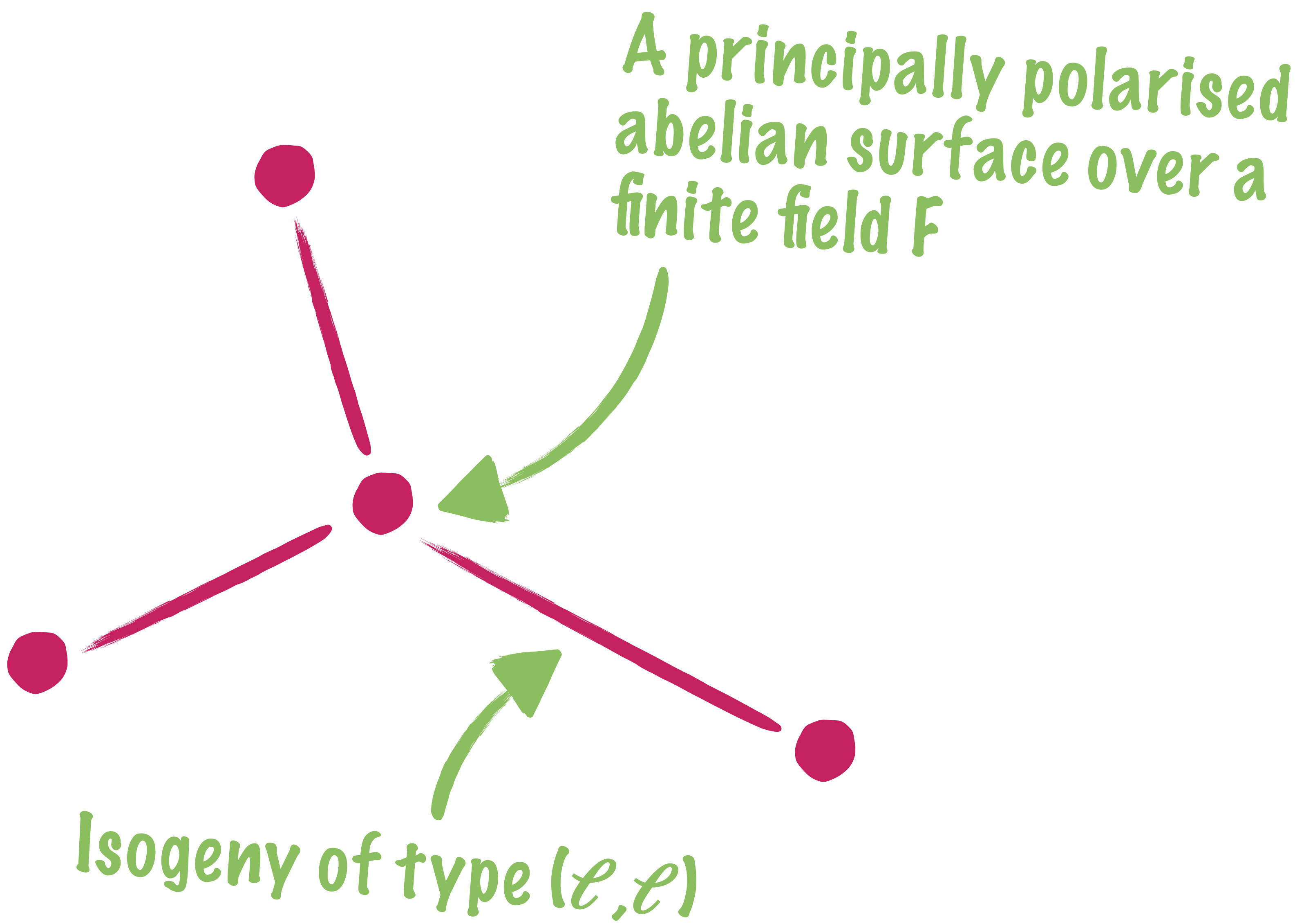
GENERALISING TO ORDINARY ABELIAN VARIETIES…

- These applications motivate the search for a generalisation to other abelian varieties…



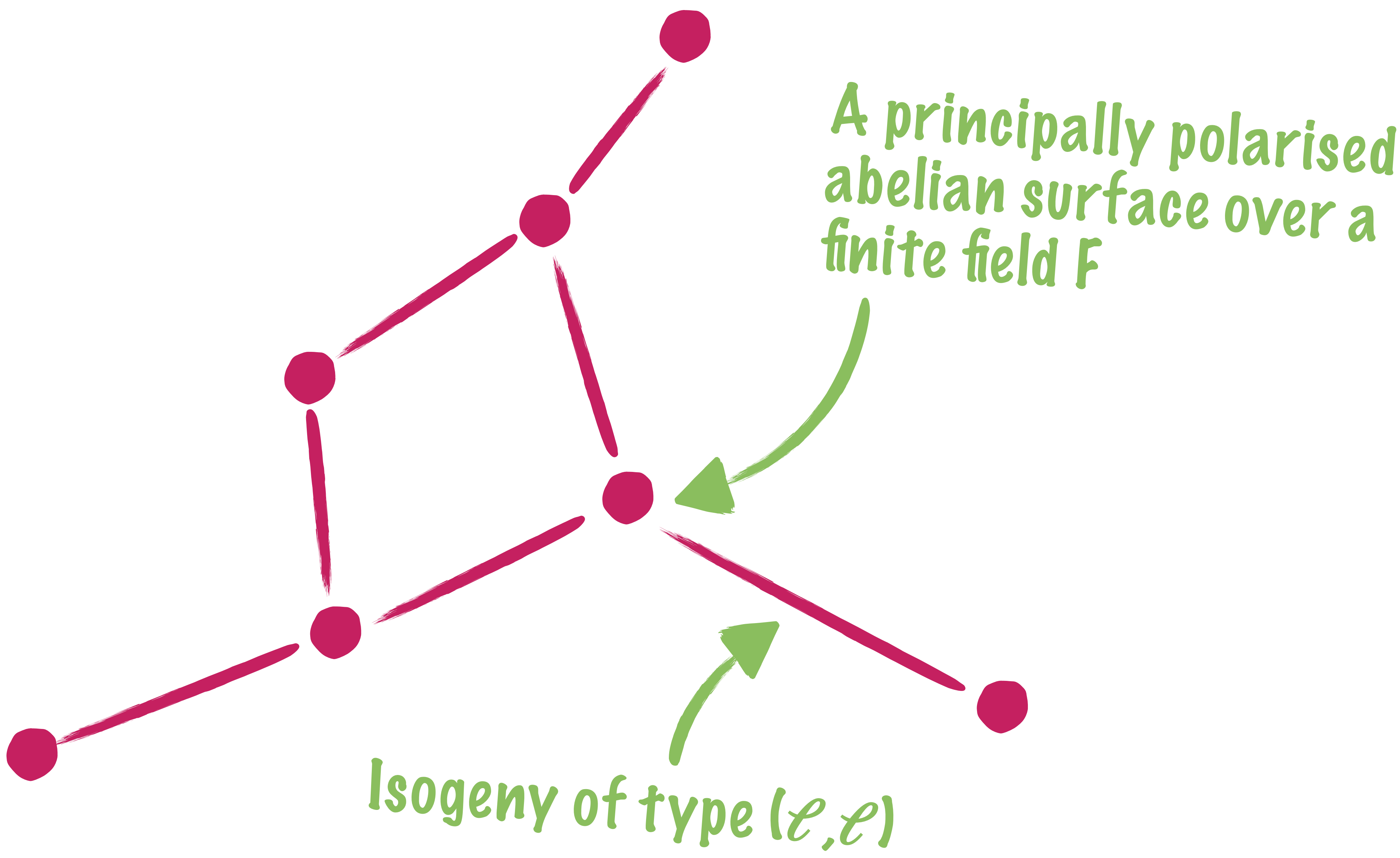
GENERALISING TO ORDINARY ABELIAN VARIETIES…

- These applications motivate the search for a generalisation to other abelian varieties…



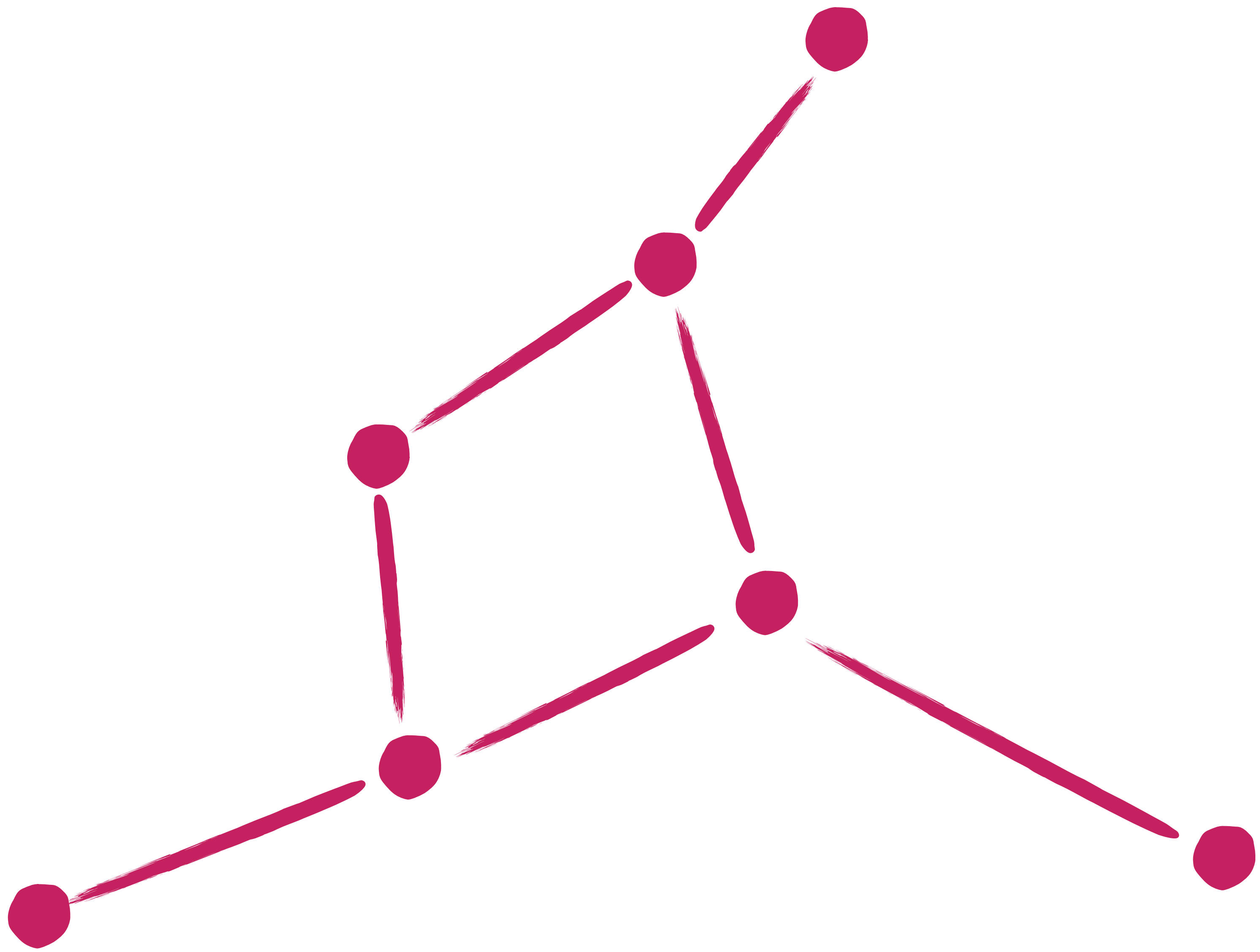
GENERALISING TO ORDINARY ABELIAN VARIETIES…

- These applications motivate the search for a generalisation to other abelian varieties…



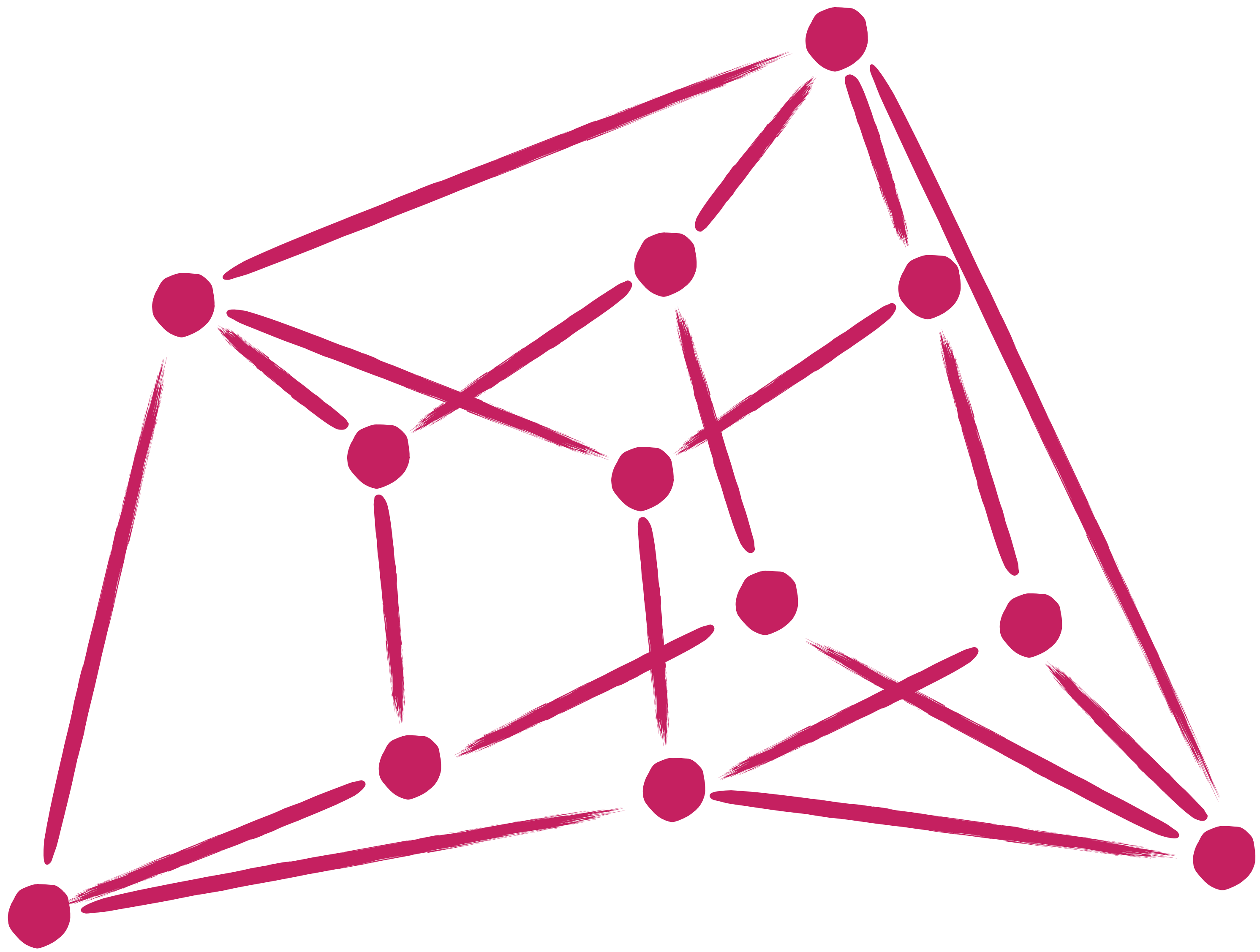
GENERALISING TO ORDINARY ABELIAN VARIETIES…

- These applications motivate the search for a generalisation to other abelian varieties…



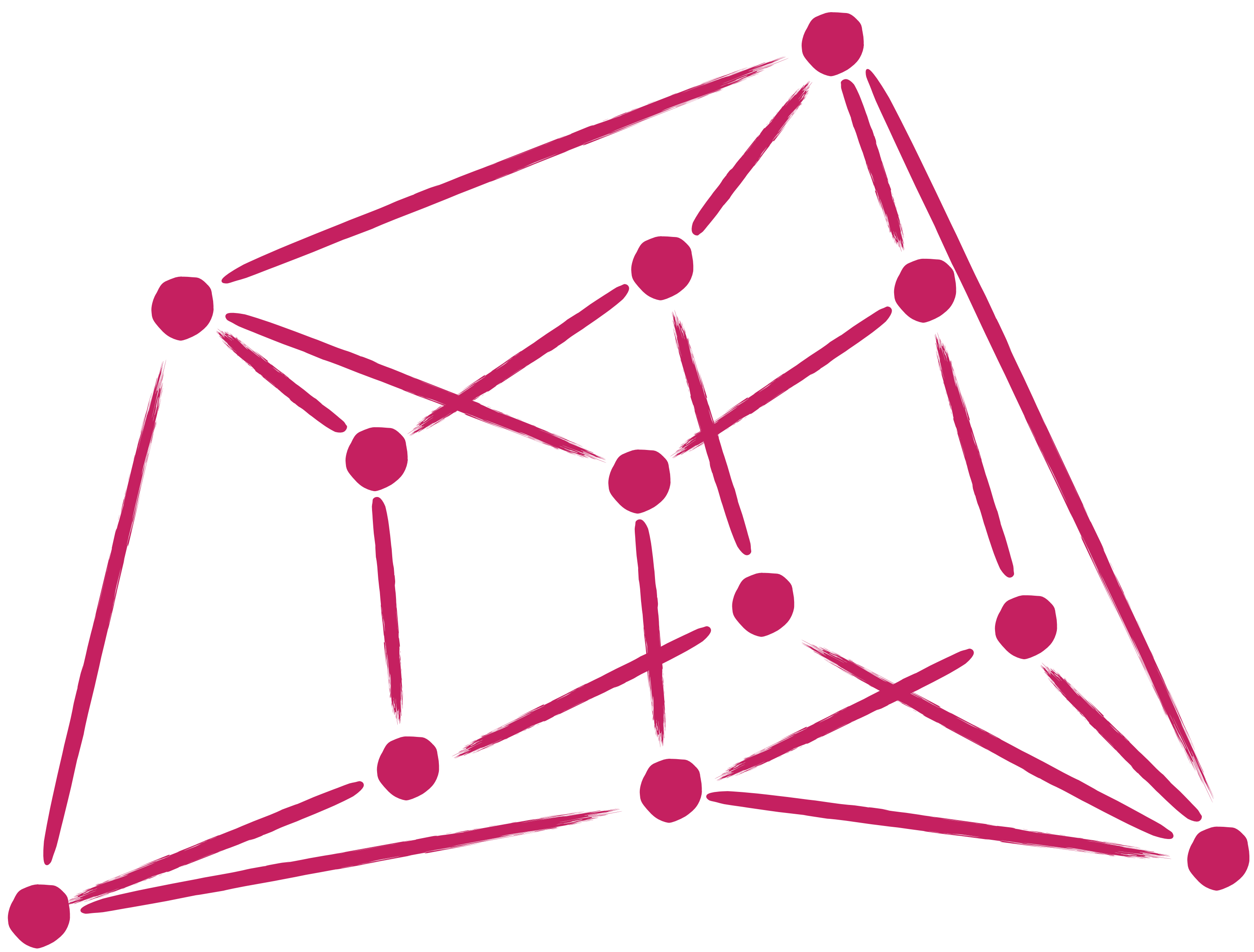
GENERALISING TO ORDINARY ABELIAN VARIETIES…

- These applications motivate the search for a generalisation to other abelian varieties…



GENERALISING TO ORDINARY ABELIAN VARIETIES…

- These applications motivate the search for a generalisation to other abelian varieties…



GENERALISING TO ORDINARY ABELIAN VARIETIES…

- These applications motivate the search for a generalisation to other abelian varieties…

GENERALISING TO ORDINARY ABELIAN VARIETIES…

Maybe we shouldn't focus on (ℓ,ℓ)-isogenies?

Maybe we do not look for the correct structures?

Should we focus on subgraphs?

ENDOMORPHISM RINGS

ENDOMORPHISM RING AND ALGEBRA

- Let $\mathscr{A}$ be an ordinary abelian variety of dimension g over a finite field $F = \mathbb{F}_q$.

ENDOMORPHISM RING AND ALGEBRA

- Let $\mathscr{A}$ be an ordinary abelian variety of dimension g over a finite field $F = \mathbb{F}_q$.
- The endomorphisms of $\mathscr{A}$ form a ring $\mathrm{End}(\mathscr{A})$.

ENDOMORPHISM RING AND ALGEBRA

- Let $\mathscr{A}$ be an ordinary abelian variety of dimension g over a finite field $F = \mathbb{F}_q$.
- The endomorphisms of $\mathscr{A}$ form a ring $\operatorname{End}(\mathscr{A})$.
- The algebra $K = \operatorname{End}(\mathscr{A}) \otimes \mathbb{Q}$ is a number field of degree $2g$ (a CM-field).

$$\begin{array}{rl} & K \supset \mathscr{O} \cong \operatorname{End}(\mathscr{A}) \\ 2 & \Big| \\ & K_0 \\ g & \Big| \\ & \mathbb{Q} \end{array}$$

ENDOMORPHISM RING AND ALGEBRA

- Let $\mathscr{A}$ be an ordinary abelian variety of dimension g over a finite field $F = \mathbb{F}_q$.
- The endomorphisms of $\mathscr{A}$ form a ring $\mathrm{End}(\mathscr{A})$.
- The algebra $K = \mathrm{End}(\mathscr{A}) \otimes \mathbb{Q}$ is a number field of degree $2g$ (a CM-field).
- $\mathrm{End}(\mathscr{A})$ is isomorphic to an order $\mathscr{O}$ of K (i.e., a lattice of dimension $2g$ in K, that is also a subring).

$$\begin{tikzcd}
K \supset \mathscr{O} \cong \mathrm{End}(\mathscr{A}) \arrow[d, dash, "2"'] \\
K_0 \arrow[d, dash, "g"'] \\
\mathbb{Q}
\end{tikzcd}$$

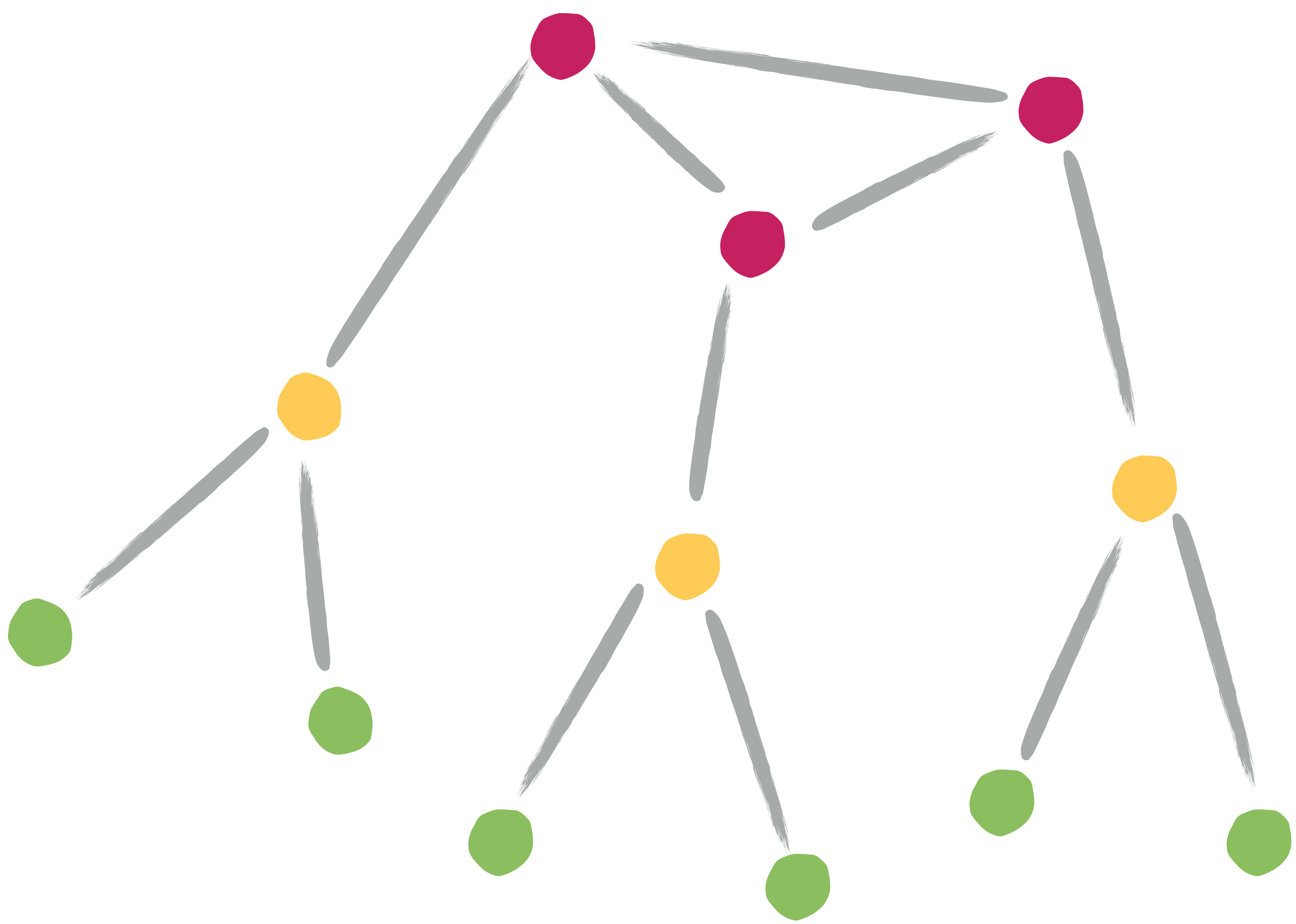
THE CASE OF ELLIPTIC CURVES

- If $\mathscr{A} = E$ is an elliptic curve, the dimension is $g = 1$.
- K has a **maximal order** $\mathcal{O}_K$, the ring of integers of K.
- Any order of K is of the form
$$\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K,$$
for a positive integer f, the **conductor**.

$$\begin{array}{l} K \supset \mathcal{O} \cong \mathrm{End}(E) \\ \quad \Big| \, 2 \\ K_0 = \mathbb{Q} \end{array}$$

THE CASE OF ELLIPTIC CURVES

The “levels” of the volcano of ℓ-isogenies tell how many times ℓ divises the conductor. Here, $(f,\ell) = 1$.



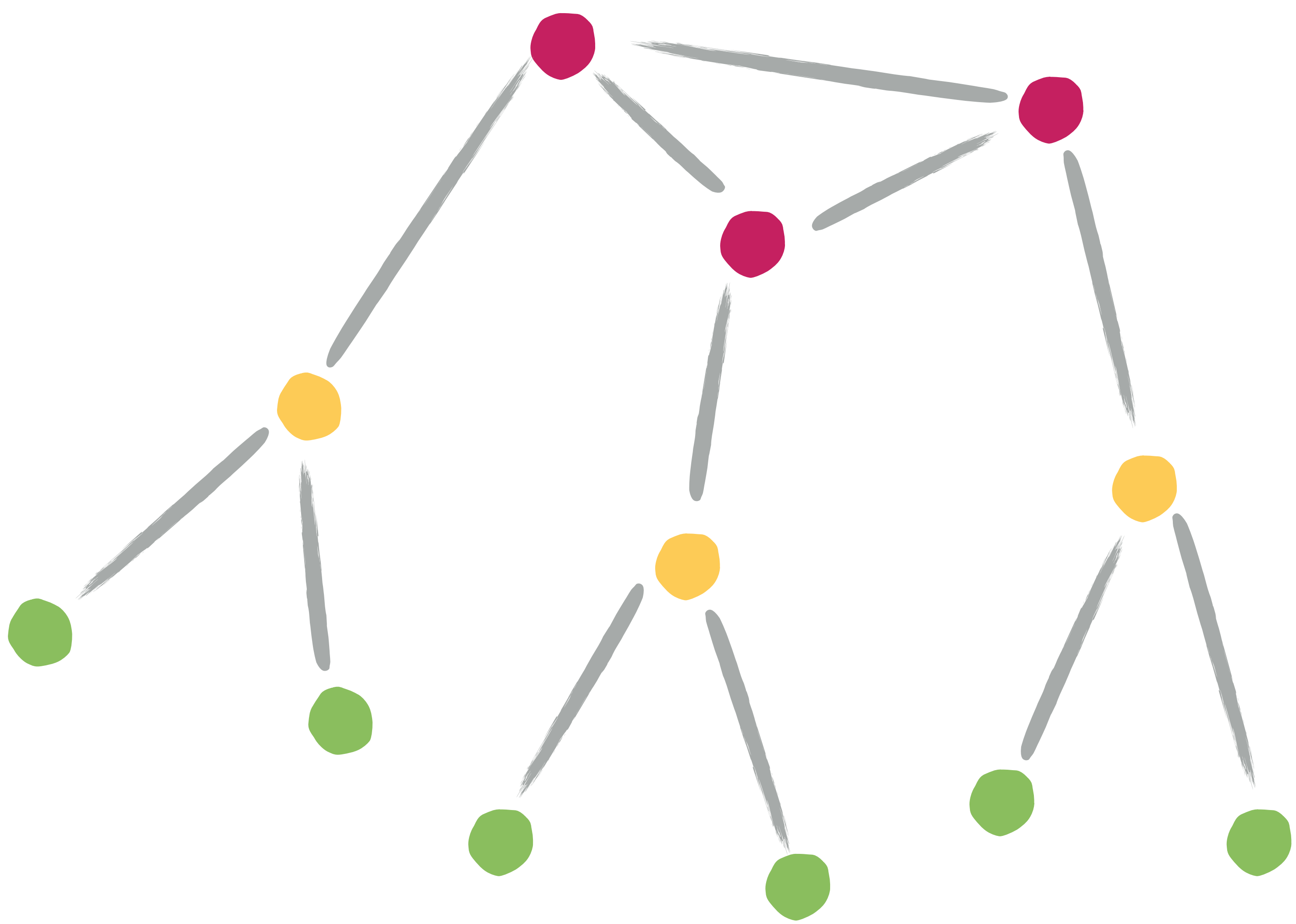
End $\cong \mathbb{Z} + f\mathcal{O}_K$

End $\cong \mathbb{Z} + \ell f\mathcal{O}_K$

End $\cong \mathbb{Z} + \ell^2 f\mathcal{O}_K$

THE CASE OF ELLIPTIC CURVES

Only an ℓ-isogeny can change the valuation at ℓ of the conductor.



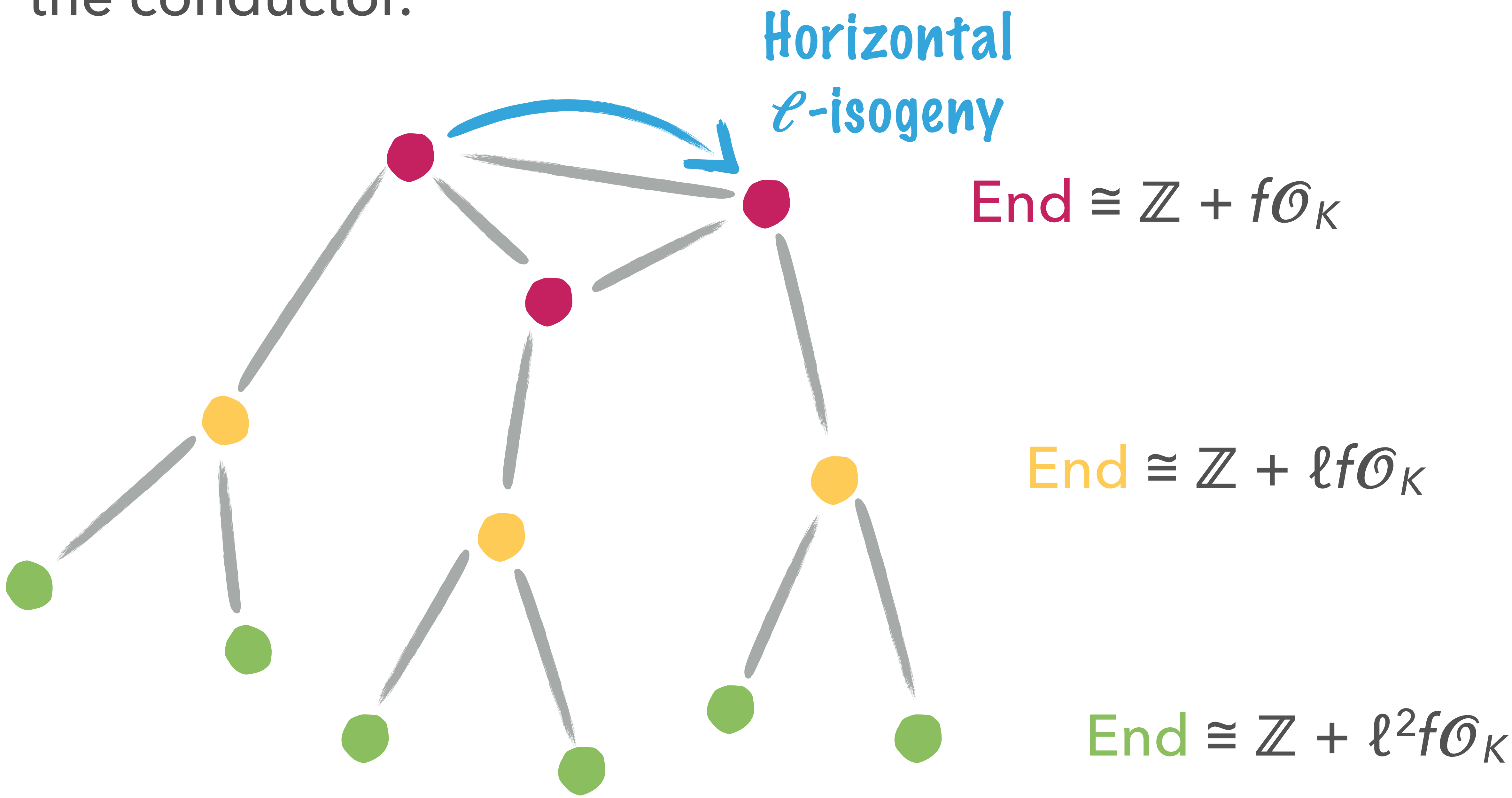
End $\cong \mathbb{Z} + f\mathcal{O}_K$

End $\cong \mathbb{Z} + \ell f\mathcal{O}_K$

End $\cong \mathbb{Z} + \ell^2 f\mathcal{O}_K$

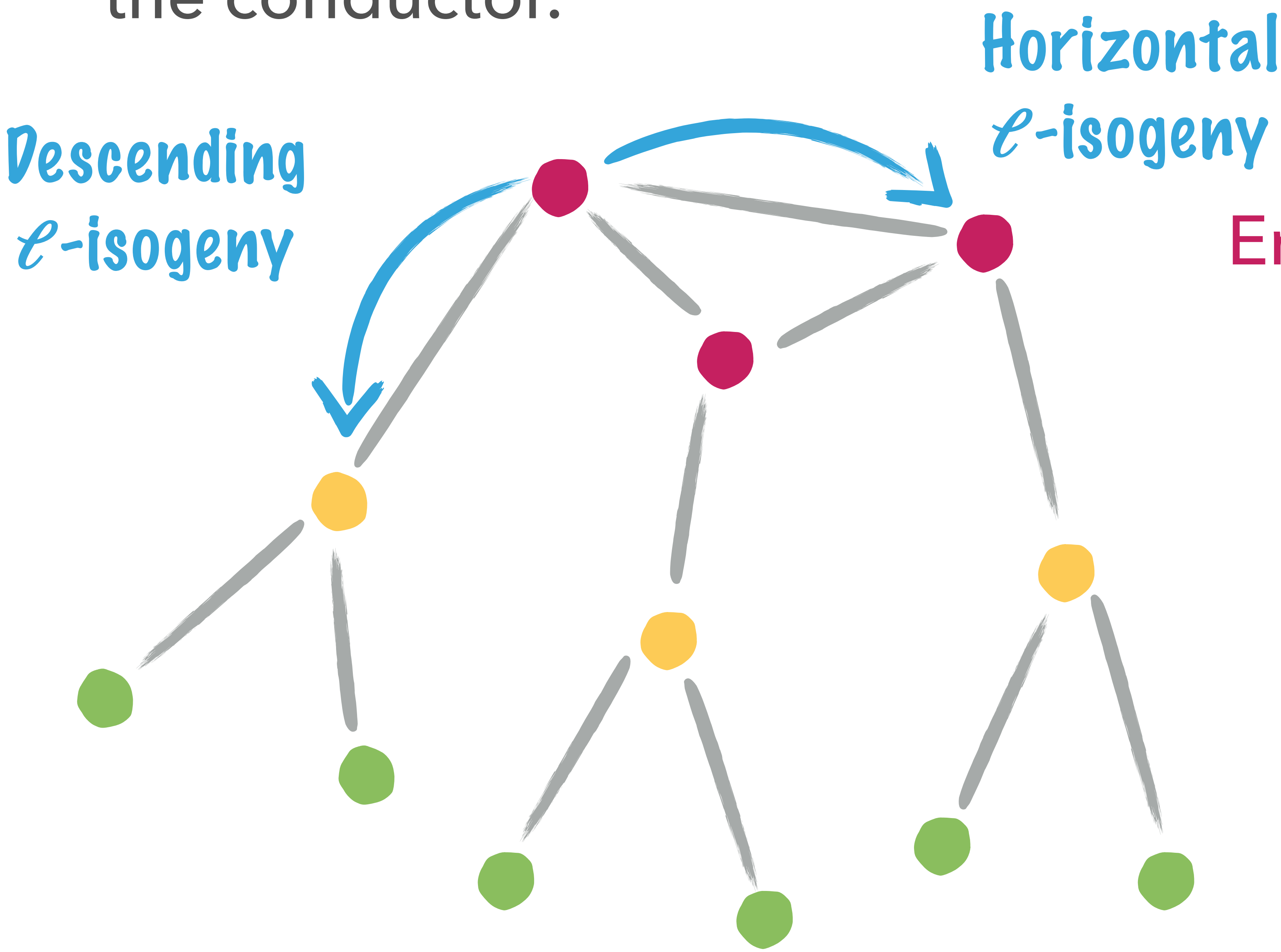
THE CASE OF ELLIPTIC CURVES

Only an ℓ-isogeny can change the valuation at ℓ of the conductor.



THE CASE OF ELLIPTIC CURVES

Only an ℓ-isogeny can change the valuation at ℓ of the conductor.



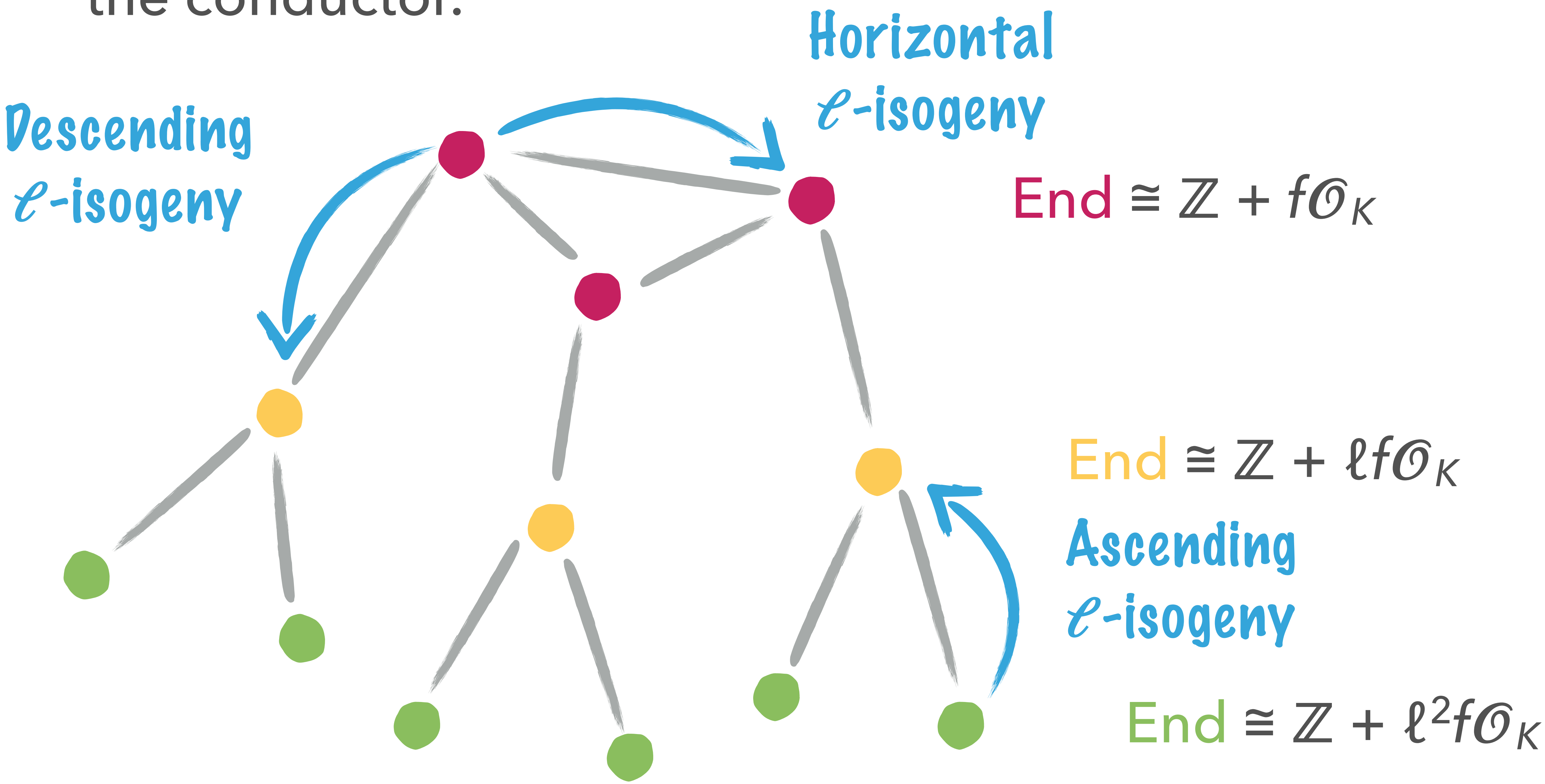
$\mathrm{End} \cong \mathbb{Z} + f\mathcal{O}_K$

$\mathrm{End} \cong \mathbb{Z} + \ell f\mathcal{O}_K$

$\mathrm{End} \cong \mathbb{Z} + \ell^2 f\mathcal{O}_K$

THE CASE OF ELLIPTIC CURVES

Only an ℓ-isogeny can change the valuation at ℓ of the conductor.



CLASSIFICATION OF ORDERS

- This classification of orders in quadratic fields is the key to the volcanic structures for elliptic curves.
- Analog in dimension $g > 1$? For any field K_0 and quadratic extension K/K_0, we prove the following classification

CLASSIFICATION OF ORDERS

- This classification of orders in quadratic fields is the key to the volcanic structures for elliptic curves.
- Analog in dimension $g > 1$? For any field K_0 and quadratic extension K/K_0, we prove the following classification

Any order $\mathcal{O}$ of K containing $\mathcal{O}_{K_0}$ is of the form

$$\mathcal{O} = \mathcal{O}_{K_0} + \mathfrak{f}\mathcal{O}_K$$

for an ideal $\mathfrak{f}$ of $\mathcal{O}_{K_0}$, the **conductor** of $\mathcal{O}$.

CLASSIFICATION OF ORDERS

- This classification of orders in quadratic fields is the key to the volcanic structures for elliptic curves.
- Analog in dimension $g > 1$? For any field K_0 and quadratic extension K/K_0, we prove the following classification

Any order $\mathcal{O}$ of K containing $\mathcal{O}_{K_0}$ is of the form

$$\mathcal{O} = \mathcal{O}_{K_0} + \mathfrak{f}\mathcal{O}_K$$

for an ideal $\mathfrak{f}$ of $\mathcal{O}_{K_0}$, the **conductor** of $\mathcal{O}$.

We actually look at this result "localy" at a prime ℓ, i.e., for the étale algebra $K \otimes \mathbb{Q}_\ell$.

CLASSIFICATION OF ORDERS

Any order $\mathcal{O}$ of K containing $\mathcal{O}_{K_0}$ is of the form

$$\mathcal{O} = \mathcal{O}_{K_0} + \mathfrak{f}\mathcal{O}_K$$

for an ideal $\mathfrak{f}$ of $\mathcal{O}_{K_0}$, the **conductor** of $\mathcal{O}$.

CLASSIFICATION OF ORDERS

Any order $\mathcal{O}$ of K containing $\mathcal{O}_{K_0}$ is of the form

$$\mathcal{O} = \mathcal{O}_{K_0} + \mathfrak{f}\mathcal{O}_K$$

for an ideal $\mathfrak{f}$ of $\mathcal{O}_{K_0}$, the **conductor** of $\mathcal{O}$.

- This is exactly $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$ when $K_0 = \mathbb{Q}$!

CLASSIFICATION OF ORDERS

Any order $\mathcal{O}$ of K containing $\mathcal{O}_{K_0}$ is of the form

$$\mathcal{O} = \mathcal{O}_{K_0} + \mathfrak{f}\mathcal{O}_K$$

for an ideal $\mathfrak{f}$ of $\mathcal{O}_{K_0}$, the **conductor** of $\mathcal{O}$.

- This is exactly $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$ when $K_0 = \mathbb{Q}$!
- When $\mathcal{O}$ contains $\mathcal{O}_{K_0}$, we say that $\mathcal{O}$ has maximal real multiplication (RM).

CLASSIFICATION OF ORDERS

Any order $\mathcal{O}$ of K containing $\mathcal{O}_{K_0}$ is of the form

$$\mathcal{O} = \mathcal{O}_{K_0} + \mathfrak{f}\mathcal{O}_K$$

for an ideal $\mathfrak{f}$ of $\mathcal{O}_{K_0}$, the **conductor** of $\mathcal{O}$.

- This is exactly $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$ when $K_0 = \mathbb{Q}$!
- When $\mathcal{O}$ contains $\mathcal{O}_{K_0}$, we say that $\mathcal{O}$ has maximal real multiplication (RM).
- For $K_0 = \mathbb{Q}$, any order has maximal RM since $\mathcal{O}_{K_0} = \mathbb{Z}$.

VOLCANOES AGAIN

ℓ-ISOGENIES

- For an elliptic curve, the conductor is an integer f, which decomposes as a product of prime numbers: we then look at ℓ-isogenies where ℓ is a prime number

$\mathfrak{l}$-ISOGENIES

- For an elliptic curve, the conductor is an integer f, which decomposes as a product of prime numbers: we then look at ℓ-isogenies where ℓ is a prime number
- For $g > 1$ and maximal RM, the conductor is an ideal $\mathfrak{f}$ of $\mathcal{O}_{K_0}$, and decomposes into prime ideals…

$\mathfrak{l}$-ISOGENIES

- For an elliptic curve, the conductor is an integer f, which decomposes as a product of prime numbers: we then look at ℓ-isogenies where ℓ is a prime number
- For $g > 1$ and maximal RM, the conductor is an ideal $\mathfrak{f}$ of $\mathcal{O}_{K_0}$, and decomposes into prime ideals…
- Notion of $\mathfrak{l}$-isogenies, where $\mathfrak{l}$ is a prime ideal of $\mathcal{O}_{K_0}$?

$\mathfrak{l}$-ISOGENIES

- For an elliptic curve, the conductor is an integer f, which decomposes as a product of prime numbers: we then look at ℓ-isogenies where ℓ is a prime number

- For $g > 1$ and maximal RM, the conductor is an ideal $\mathfrak{f}$ of $\mathcal{O}_{K_0}$, and decomposes into prime ideals…

- Notion of $\mathfrak{l}$-isogenies, where $\mathfrak{l}$ is a prime ideal of $\mathcal{O}_{K_0}$?

An $\mathfrak{l}$-isogeny from $\mathscr{A}$ is an isogeny whose kernel is a cyclic sub-$\mathcal{O}_{K_0}$-module of $\mathscr{A}[\mathfrak{l}]$.

Only an $\mathfrak{l}$-isogeny can change the valuation at $\mathfrak{l}$ of the conductor.

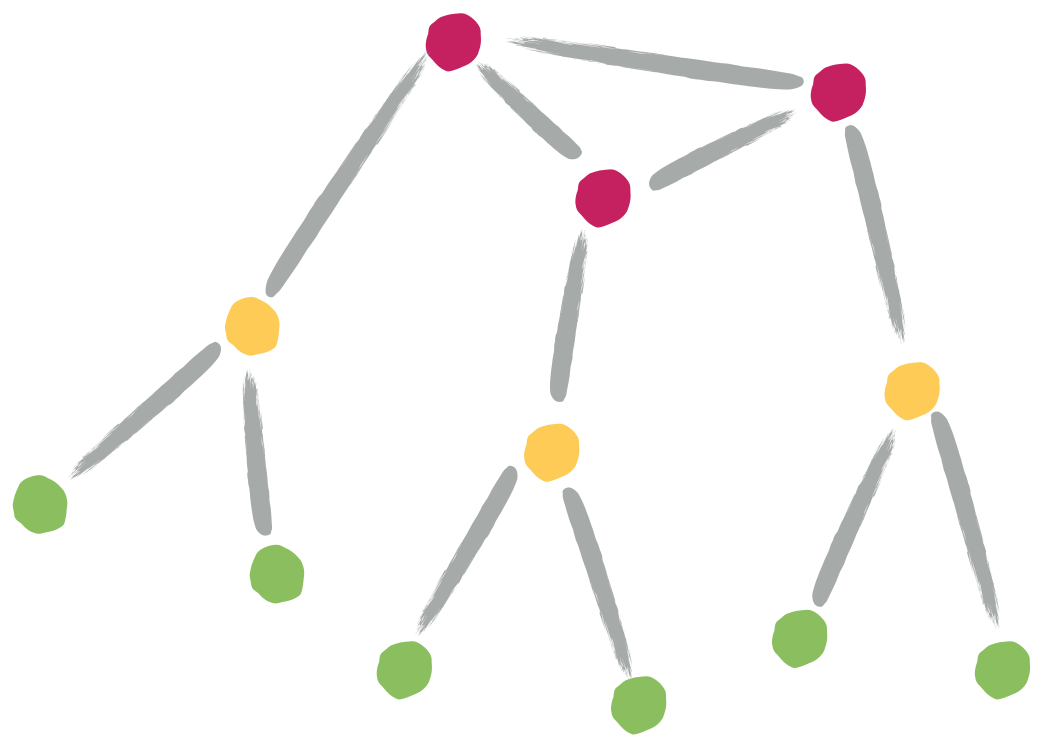
VOLCANOES AGAIN?

If $\mathscr{A}$ has maximal RM (locally at ℓ), and $\mathfrak{l}$ is a prime ideal of $\mathscr{O}_{K_0}$ above ℓ, is the graph of $\mathfrak{l}$-isogenies a volcano?

VOLCANOES AGAIN?

If $\mathscr{A}$ has maximal RM (locally at ℓ), and $\mathfrak{l}$ is a prime ideal of $\mathcal{O}_{K_0}$ above ℓ, is the graph of $\mathfrak{l}$-isogenies a volcano?

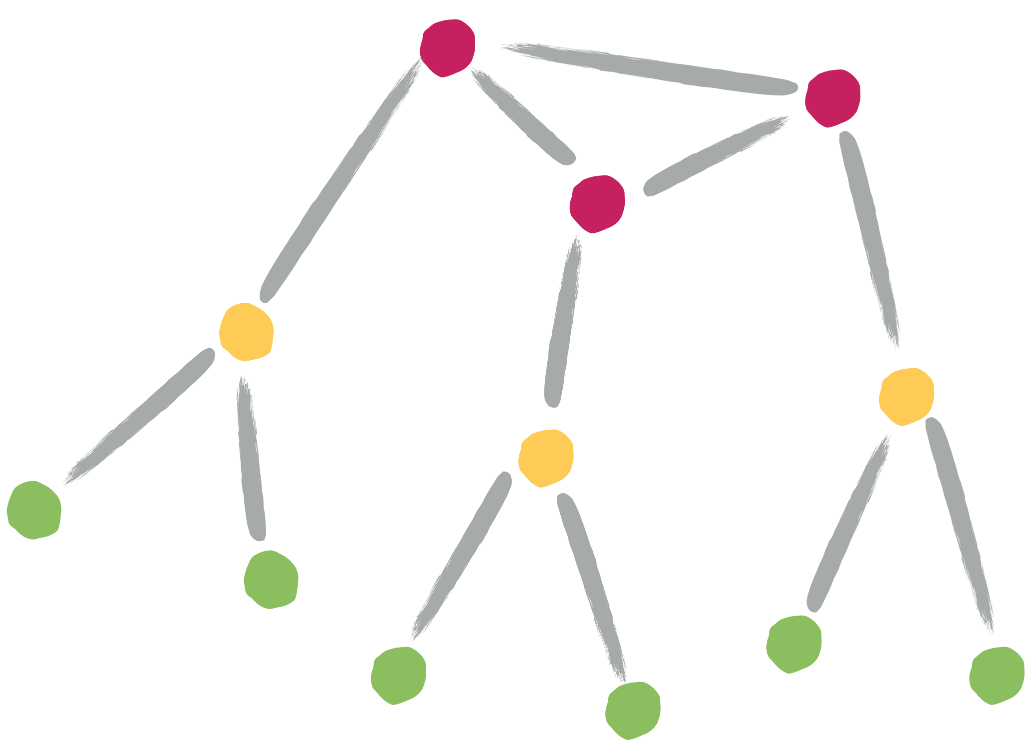
Theorem: yes!... at least when $\mathfrak{l}$ is principal, and all the units of $\mathcal{O}_K$ are totally real!



VOLCANOES AGAIN?

If $\mathscr{A}$ has maximal RM (locally at ℓ), and $\mathfrak{l}$ is a prime ideal of $\mathcal{O}_{K_0}$ above ℓ, is the graph of $\mathfrak{l}$-isogenies a volcano?

Theorem: yes!... at least when $\mathfrak{l}$ is principal, and all the units of $\mathcal{O}_K$ are totally real!



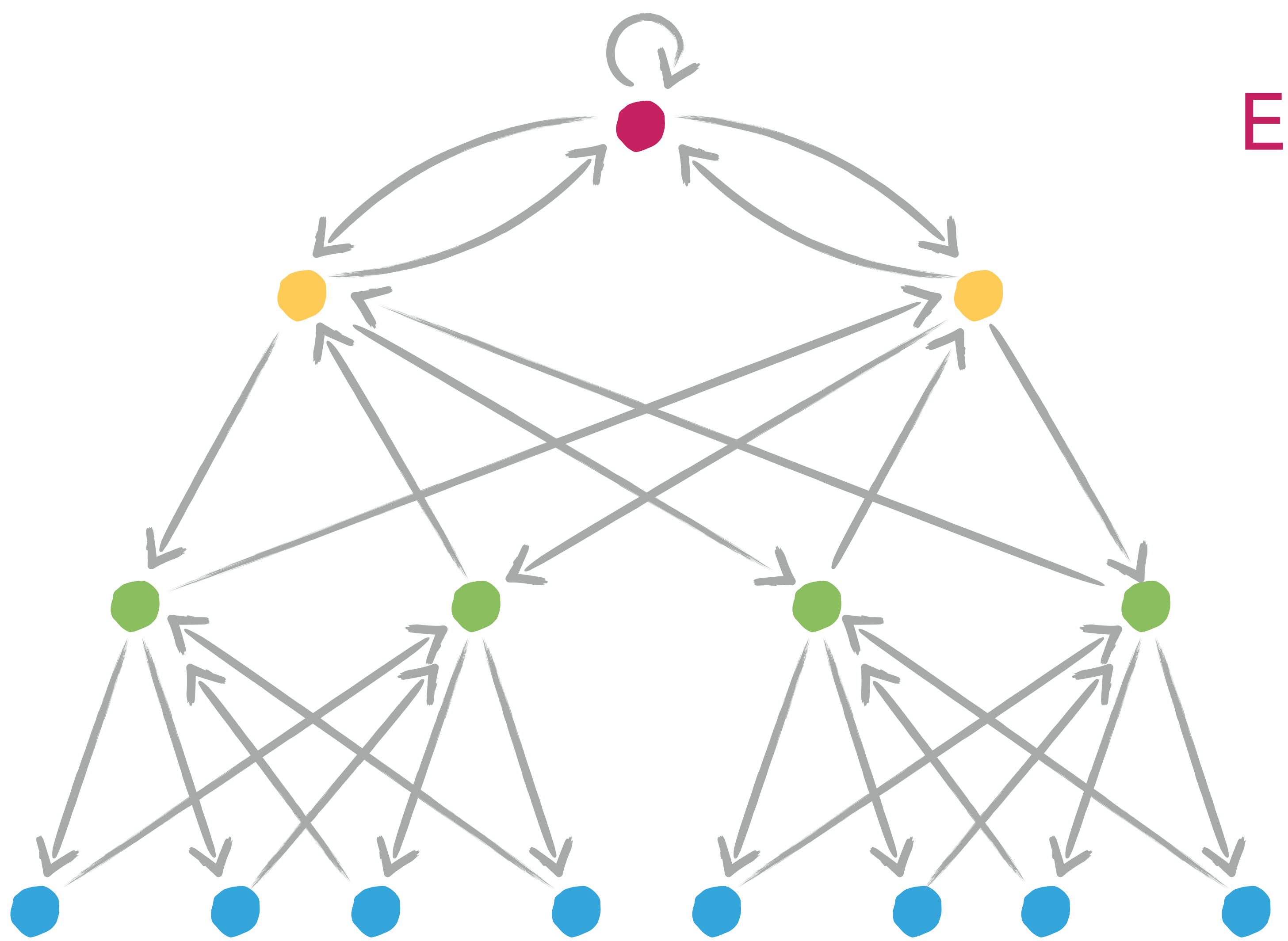
$\mathrm{End} \cong \mathcal{O}_{K_0} + \mathfrak{f}\mathcal{O}_K$

$\mathrm{End} \cong \mathcal{O}_{K_0} + \mathfrak{l}\mathfrak{f}\mathcal{O}_K$

$\mathrm{End} \cong \mathcal{O}_{K_0} + \mathfrak{l}^2\mathfrak{f}\mathcal{O}_K$

VOLCANOES AGAIN?

If $\mathfrak{l}$ is not principal? The graph is oriented!



$\mathrm{End} \cong \mathcal{O}_{K_0} + \mathfrak{f}\mathcal{O}_K$

$\mathrm{End} \cong \mathcal{O}_{K_0} + \mathfrak{l}\mathfrak{f}\mathcal{O}_K$

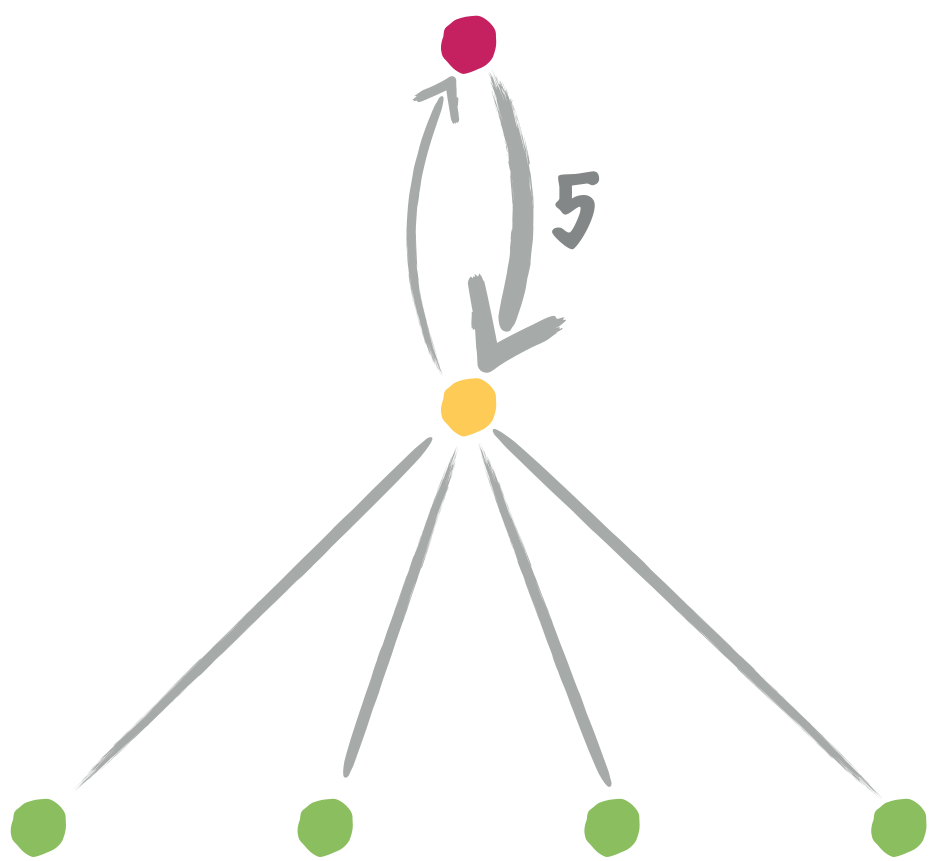
$\mathrm{End} \cong \mathcal{O}_{K_0} + \mathfrak{l}^2\mathfrak{f}\mathcal{O}_K$

$\mathrm{End} \cong \mathcal{O}_{K_0} + \mathfrak{l}^3\mathfrak{f}\mathcal{O}_K$

VOLCANOES AGAIN?

If $\mathcal{O}_K$ has complex units? Multiplicities appear

For instance, $K = \mathbb{Q}(\zeta_5)$, $K_0 = \mathbb{Q}\left(\zeta_5 + \zeta_5^{-1}\right)$, and $\mathfrak{l} = 2\mathcal{O}_{K_0}$.



End $\cong \mathcal{O}_{K_0} + \mathfrak{f}\mathcal{O}_K$

End $\cong \mathcal{O}_{K_0} + \mathfrak{l}\mathfrak{f}\mathcal{O}_K$

End $\cong \mathcal{O}_{K_0} + \mathfrak{l}^2\mathfrak{f}\mathcal{O}_K$

IN DIMENSION 2

(ℓ,ℓ)-ISOGENIES

(ℓ,ℓ)-ISOGENIES

- Let $\mathscr{A}$ be a principally polarised, ordinary abelian surface.
- An (ℓ,ℓ)-isogeny is an isogeny $\mathscr{A} \to \mathscr{B}$ whose kernel is a maximal isotropic subgroup of $\mathscr{A}[\ell]$ for the Weil pairing.
- (ℓ,ℓ)-isogenies are easier to compute! Much more efficient than $\mathfrak{l}$-isogenies…

(ℓ,ℓ)-ISOGENIES

We show that (ℓ,ℓ)-isogenies preserving the maximal RM are exactly:

(ℓ,ℓ)-ISOGENIES

We show that (ℓ,ℓ)-isogenies preserving the maximal RM are exactly:

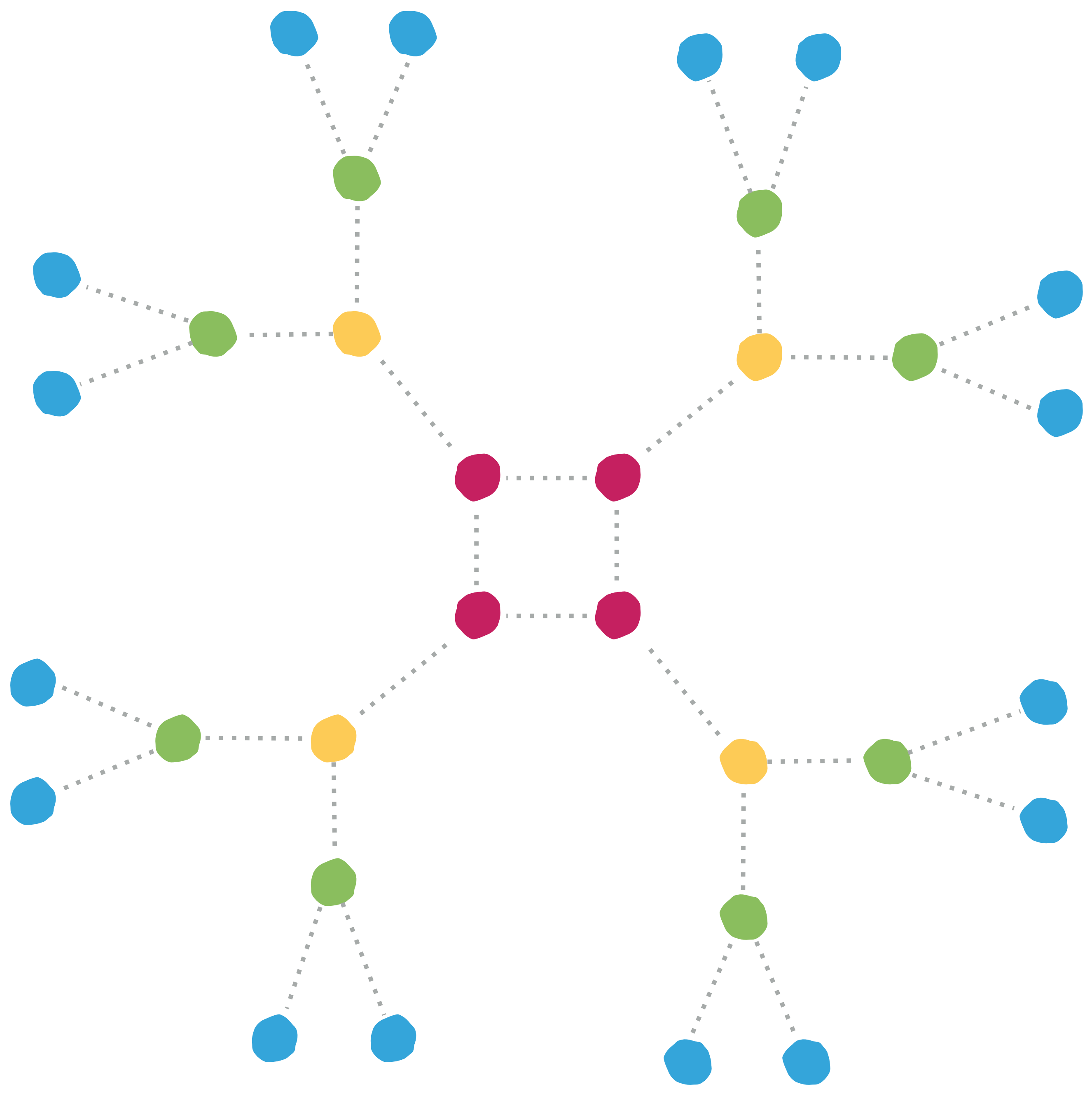
- The $\mathfrak{l}$-isogenies if ℓ is inert in K_0 (i.e., $\mathfrak{l} = \ell\mathcal{O}_{K_0}$)

(ℓ,ℓ)-ISOGENIES

We show that (ℓ,ℓ)-isogenies preserving the maximal RM are exactly:

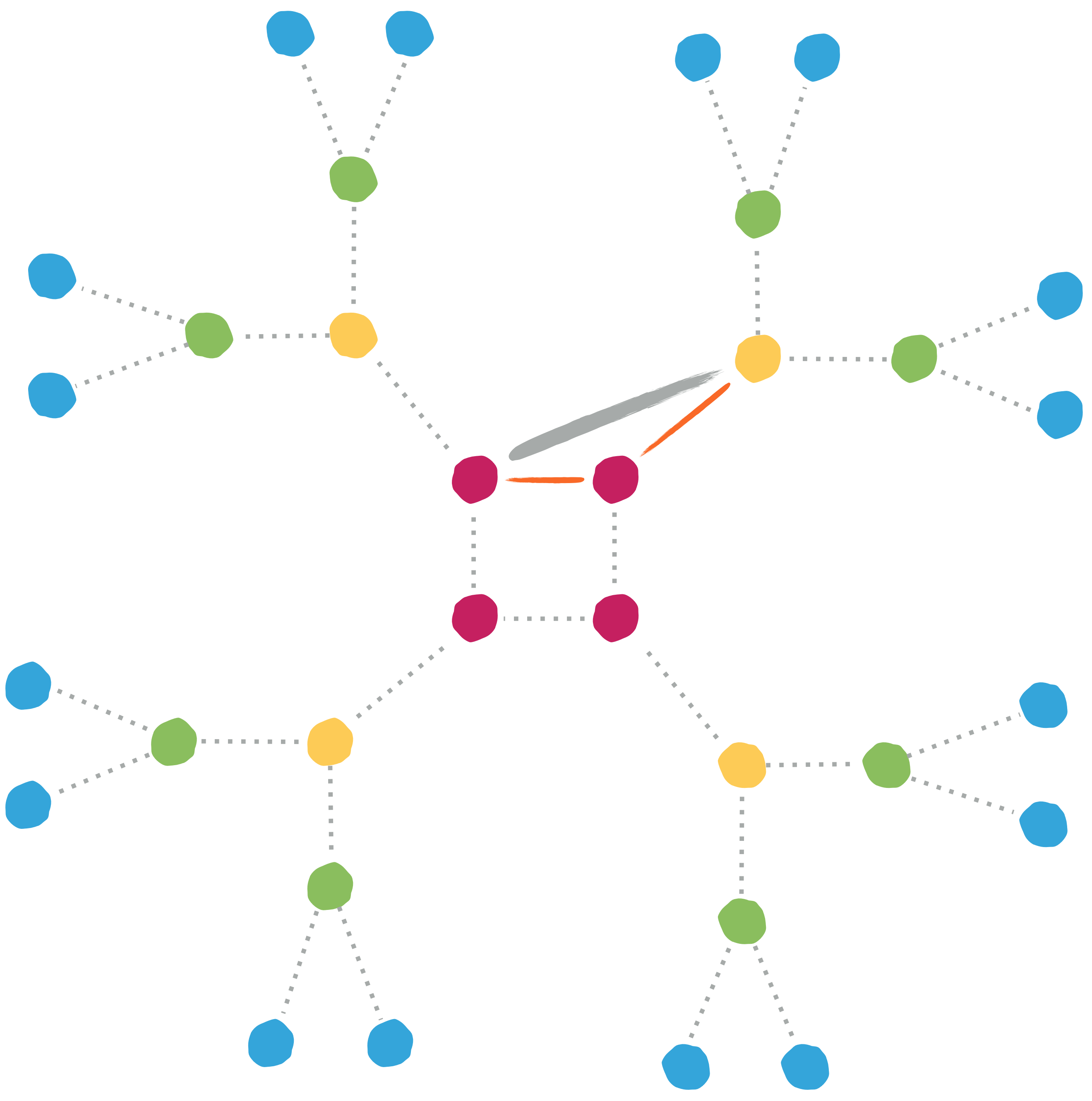
- The $\mathfrak{l}$-isogenies if ℓ is inert in K_0 (i.e., $\mathfrak{l} = \ell\mathcal{O}_{K_0}$)
- The compositions of an $\mathfrak{l}_1$-isogeny with an $\mathfrak{l}_2$-isogeny if ℓ splits or ramifies as $\ell\mathcal{O}_{K_0} = \mathfrak{l}_1\mathfrak{l}_2$.

GRAPHS OF (ℓ,ℓ)-ISOGENIES PRESERVING THE RM



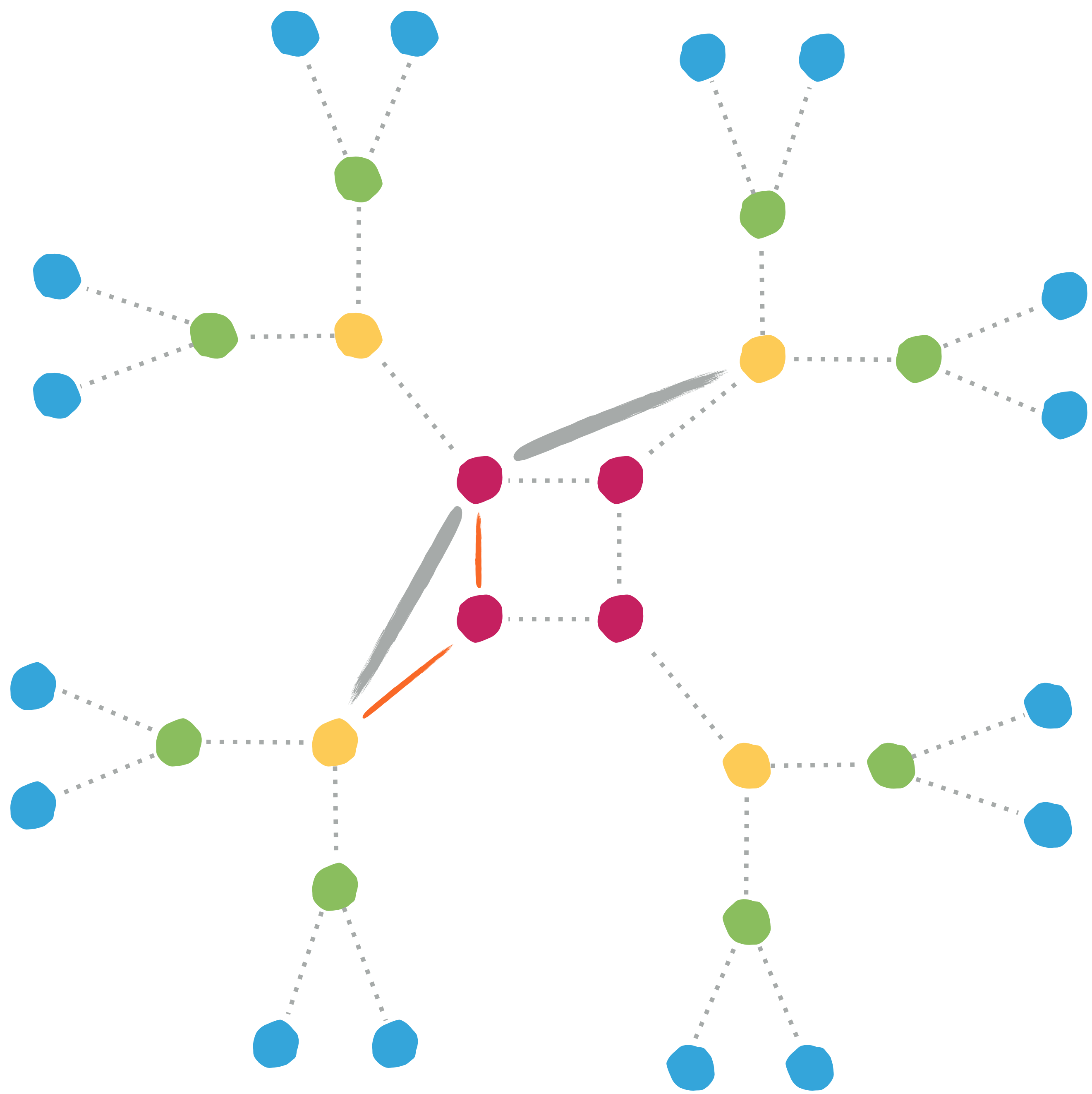
Assume $\ell\mathcal{O}_{K_0} = \mathfrak{l}^2$

GRAPHS OF (ℓ,ℓ)-ISOGENIES PRESERVING THE RM



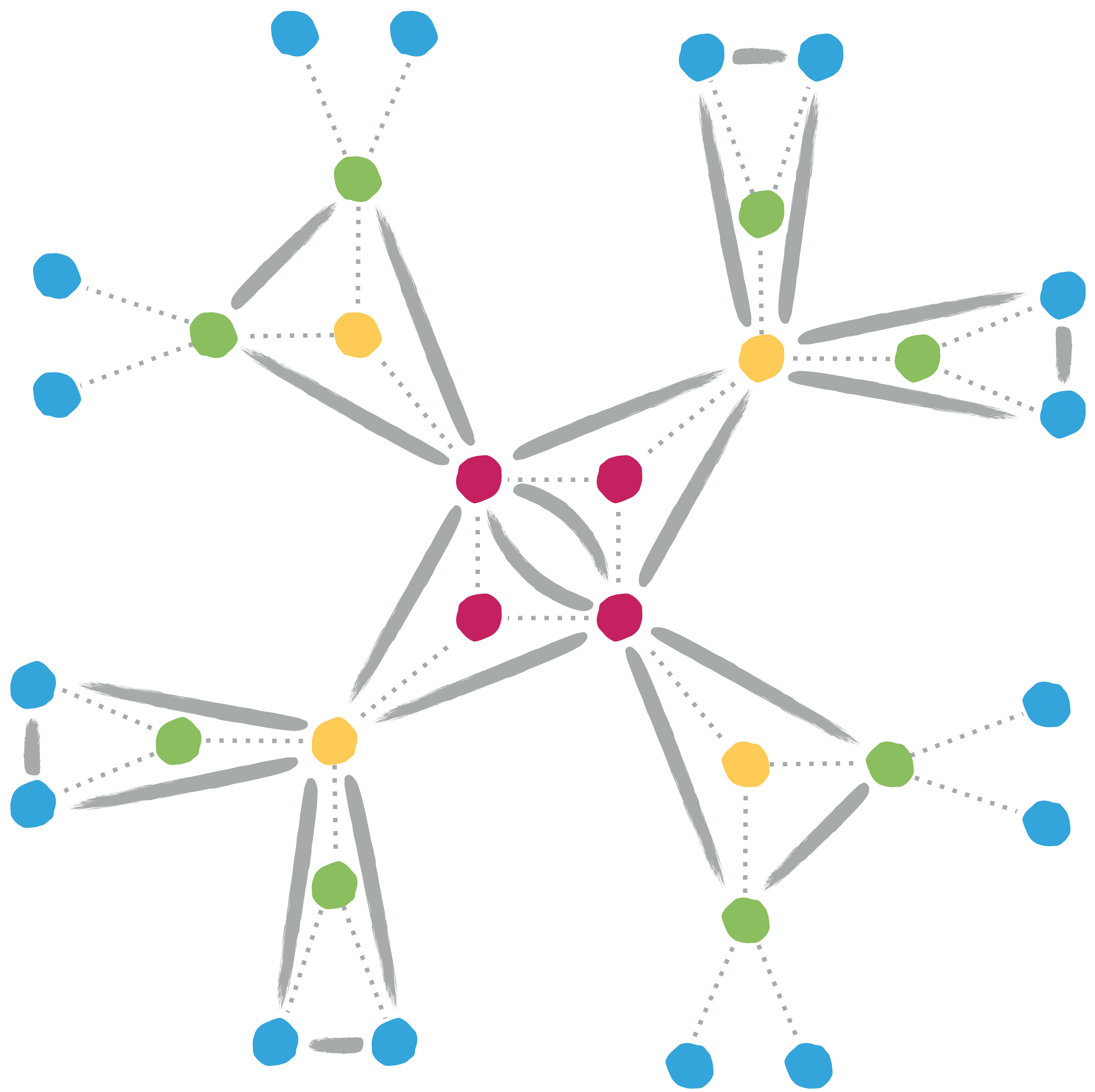
Assume $\ell\mathcal{O}_{K_0} = \mathfrak{l}^2$

GRAPHS OF (ℓ,ℓ)-ISOGENIES PRESERVING THE RM



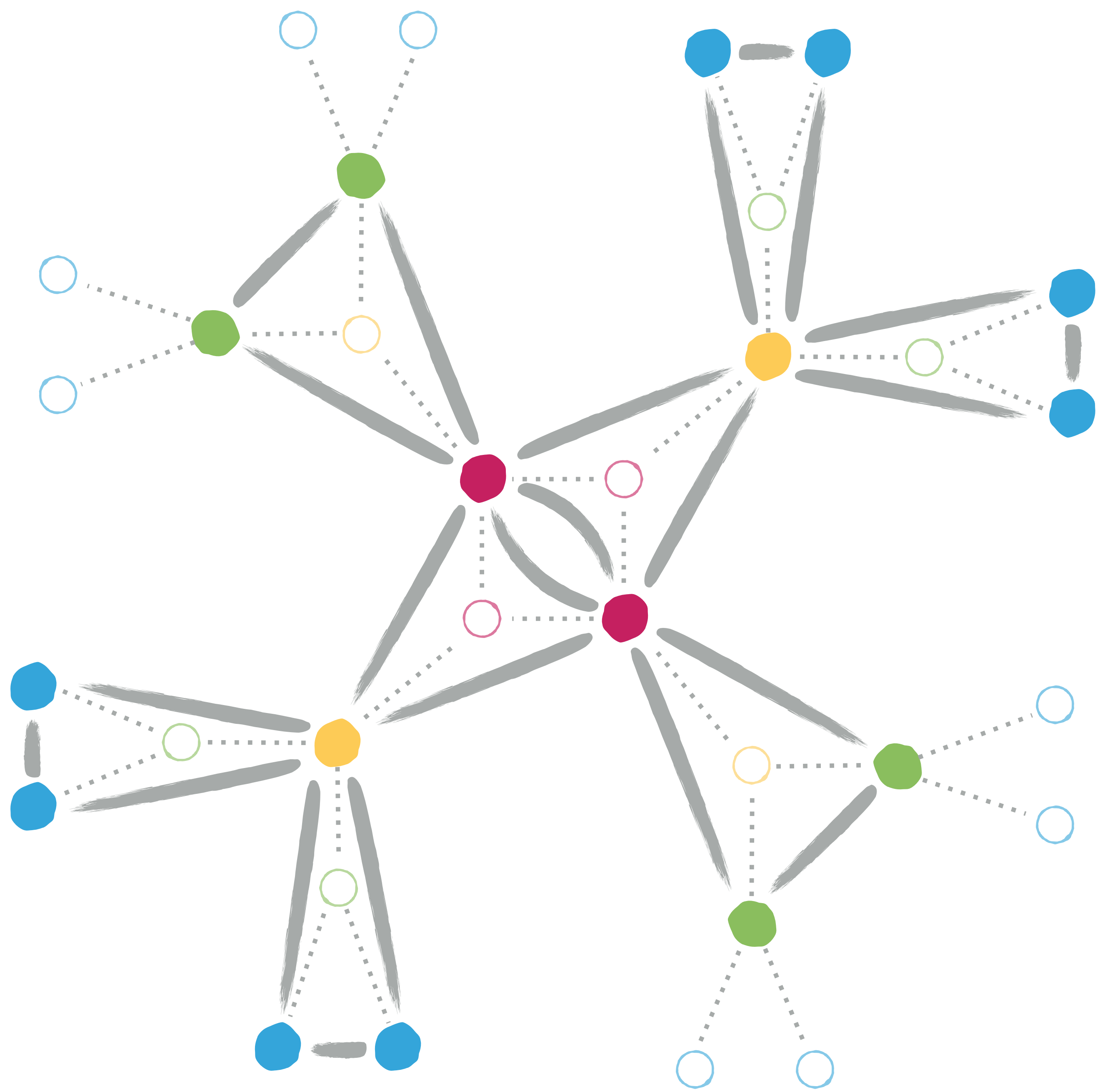
Assume $\ell \mathcal{O}_{K_0} = \mathfrak{l}^2$

GRAPHS OF (ℓ,ℓ)-ISOGENIES PRESERVING THE RM



Assume $\ell \mathcal{O}_{K_0} = \mathfrak{l}^2$

GRAPHS OF (ℓ,ℓ)-ISOGENIES PRESERVING THE RM



Assume $\ell \mathcal{O}_{K_0} = \mathfrak{l}^2$

WHERE TO GO FROM THERE?

- We described the structure of graphs of (ℓ,ℓ)-isogenies preserving the maximal RM.
- It is also interesting to look at (ℓ,ℓ)-isogenies changing the RM. We can describe this graph locally.
- In particular, if the RM is not maximal, we show that there is an (ℓ,ℓ)-isogeny increasing it.
- A first application: these results allow to describe an algorithm finding a path of (ℓ,ℓ)-isogenies to a variety with maximal endomorphism ring.

TECHNIQUES

ℓ-ADIC LATTICES AND COMPLEX MULTIPLICATION

THE TATE MODULE

- We have the following sequence of morphisms

$$0 \xleftarrow{\ell} \mathscr{A}[\ell] \xleftarrow{\ell} \mathscr{A}[\ell^2] \xleftarrow{\ell} \mathscr{A}[\ell^3] \xleftarrow{\ell} \mathscr{A}[\ell^4] \xleftarrow{\ell} \ldots$$

THE TATE MODULE

- We have the following sequence of morphisms

$$0 \xleftarrow{\ell} \mathscr{A}[\ell] \xleftarrow{\ell} \mathscr{A}[\ell^2] \xleftarrow{\ell} \mathscr{A}[\ell^3] \xleftarrow{\ell} \mathscr{A}[\ell^4] \xleftarrow{\ell} \ldots$$

- The Tate module is the inverse limit $T = T_\ell(\mathscr{A}) = \varprojlim \mathscr{A}[\ell^n]$.

THE TATE MODULE

- We have the following sequence of morphisms

$$0 \xleftarrow{\ell} \mathscr{A}[\ell] \xleftarrow{\ell} \mathscr{A}[\ell^2] \xleftarrow{\ell} \mathscr{A}[\ell^3] \xleftarrow{\ell} \mathscr{A}[\ell^4] \xleftarrow{\ell} \ldots$$

- The Tate module is the inverse limit $T = T_\ell(\mathscr{A}) = \varprojlim \mathscr{A}[\ell^n]$.
- T is a free $\mathbb{Z}_\ell$-module of rank $2g$.

THE TATE MODULE

- We have the following sequence of morphisms

$$0 \xleftarrow{\ell} \mathscr{A}[\ell] \xleftarrow{\ell} \mathscr{A}[\ell^2] \xleftarrow{\ell} \mathscr{A}[\ell^3] \xleftarrow{\ell} \mathscr{A}[\ell^4] \xleftarrow{\ell} \ldots$$

- The Tate module is the inverse limit $T = T_\ell(\mathscr{A}) = \varprojlim \mathscr{A}[\ell^n]$.
- T is a free $\mathbb{Z}_\ell$-module of rank $2g$.
- T is a full-rank lattice in the $\mathbb{Q}_\ell$-vector space $V = T \otimes \mathbb{Q}_\ell$.

THE TATE MODULE

- We have the following sequence of morphisms

$$0 \xleftarrow{\ell} \mathscr{A}[\ell] \xleftarrow{\ell} \mathscr{A}[\ell^2] \xleftarrow{\ell} \mathscr{A}[\ell^3] \xleftarrow{\ell} \mathscr{A}[\ell^4] \xleftarrow{\ell} \dots$$

- The Tate module is the inverse limit $T = T_\ell(\mathscr{A}) = \varprojlim \mathscr{A}[\ell^n]$.
- T is a free $\mathbb{Z}_\ell$-module of rank $2g$.
- T is a full-rank lattice in the $\mathbb{Q}_\ell$-vector space $V = T \otimes \mathbb{Q}_\ell$.
- There is a canonical one-to-one correspondence

$$\{\text{ lattices in } V \text{ containing } T\,\} \longleftrightarrow \{\text{ finite subgroups of } \mathscr{A}[\ell^\infty]\,\}$$

THE TATE MODULE

- We have the following sequence of morphisms

$$0 \xleftarrow{\ell} \mathscr{A}[\ell] \xleftarrow{\ell} \mathscr{A}[\ell^2] \xleftarrow{\ell} \mathscr{A}[\ell^3] \xleftarrow{\ell} \mathscr{A}[\ell^4] \xleftarrow{\ell} \dots$$

- The Tate module is the inverse limit $T = T_\ell(\mathscr{A}) = \varprojlim \mathscr{A}[\ell^n]$.
- T is a free $\mathbb{Z}_\ell$-module of rank $2g$.
- T is a full-rank lattice in the $\mathbb{Q}_\ell$-vector space $V = T \otimes \mathbb{Q}_\ell$.
- There is a canonical one-to-one correspondence

$$\{\text{ lattices in } V \text{ containing } T\,\} \longleftrightarrow \{\text{ finite subgroups of } \mathscr{A}[\ell^\infty]\,\}$$

Lattices in an ℓ-adic vector space $\longleftrightarrow$ Kernels of isogenies

THE TATE MODULE

Lattices in an ℓ-adic vector space $\longleftrightarrow$ Kernels of isogenies

$$\{\text{ lattices in } V \text{ containing } T\,\} \longleftrightarrow \{\text{ finite subgroups of } \mathscr{A}[\ell^\infty]\,\}$$

THE TATE MODULE

Lattices in an ℓ-adic vector space $\longleftrightarrow$ Kernels of isogenies

$$\{ \text{ lattices in } V \text{ containing } T \,\} \longleftrightarrow \{ \text{ finite subgroups of } \mathscr{A}[\ell^\infty] \,\}$$

- There is a natural isomorphism $f : V/T \cong \mathscr{A}[\ell^\infty]$.

THE TATE MODULE

Lattices in an ℓ-adic vector space $\longleftrightarrow$ Kernels of isogenies

$$\{\text{ lattices in } V \text{ containing } T\,\} \longleftrightarrow \{\text{ finite subgroups of } \mathscr{A}[\ell^\infty]\,\}$$

$$L \qquad\longmapsto\qquad f(L/T)$$

- There is a natural isomorphism $f : V/T \cong \mathscr{A}[\ell^\infty]$.

THE TATE MODULE

Lattices in an ℓ-adic vector space $\longleftrightarrow$ Kernels of isogenies

$$\{\text{ lattices in } V \text{ containing } T\} \longleftrightarrow \{\text{ finite subgroups of } \mathscr{A}[\ell^\infty]\}$$

$$\begin{array}{ccc} L & \longmapsto & f(L/T) \\ f^{-1}(G) + T & \longleftarrow\!\!\! \mid & G \end{array}$$

- There is a natural isomorphism $f : V/T \cong \mathscr{A}[\ell^\infty]$.

COMPLEX MULTIPLICATION ON THE TATE MODULE

- $T = T_\ell(\mathscr{A}) = \varprojlim \mathscr{A}[\ell^n]$ and $V = T \otimes \mathbb{Q}_\ell$.

COMPLEX MULTIPLICATION ON THE TATE MODULE

- $T = T_\ell(\mathscr{A}) = \varprojlim \mathscr{A}[\ell^n]$ and $V = T \otimes \mathbb{Q}_\ell$.
- $\mathrm{End}(\mathscr{A})$ acts on T. Actually, $\mathrm{End}(\mathscr{A}) \otimes \mathbb{Z}_\ell$ acts on T.

COMPLEX MULTIPLICATION ON THE TATE MODULE

- $T = T_\ell(\mathscr{A}) = \varprojlim \mathscr{A}[\ell^n]$ and $V = T \otimes \mathbb{Q}_\ell$.
- $\mathrm{End}(\mathscr{A})$ acts on T. Actually, $\mathrm{End}(\mathscr{A}) \otimes \mathbb{Z}_\ell$ acts on T.
- $K_\ell = \mathrm{End}(\mathscr{A}) \otimes \mathbb{Q}_\ell$ acts on V (we have $K_\ell = K \otimes \mathbb{Q}_\ell$ where K is the endomorphism algebra of $\mathscr{A}$, a CM-field)

COMPLEX MULTIPLICATION ON THE TATE MODULE

- $T = T_\ell(\mathscr{A}) = \varprojlim \mathscr{A}[\ell^n]$ and $V = T \otimes \mathbb{Q}_\ell$.
- $\mathrm{End}(\mathscr{A})$ acts on T. Actually, $\mathrm{End}(\mathscr{A}) \otimes \mathbb{Z}_\ell$ acts on T.
- $K_\ell = \mathrm{End}(\mathscr{A}) \otimes \mathbb{Q}_\ell$ acts on V (we have $K_\ell = K \otimes \mathbb{Q}_\ell$ where K is the endomorphism algebra of $\mathscr{A}$, a CM-field)
- Given a lattice L in V containing T, the set of elements of K_ℓ preserving L is an order in K_ℓ, denoted $\mathcal{O}(L)$.

COMPLEX MULTIPLICATION ON THE TATE MODULE

Lattices in an ℓ-adic vector space $\longleftrightarrow$ Kernels of isogenies

$$\{\text{ lattices in } V \text{ containing } T\,\} \longleftrightarrow \{\text{ finite subgroups of } \mathscr{A}[\ell^\infty]\,\}$$

COMPLEX MULTIPLICATION ON THE TATE MODULE

Lattices in an ℓ-adic vector space $\longleftrightarrow$ Kernels of isogenies

$$\{ \text{ lattices in } V \text{ containing } T \} \longleftrightarrow \{ \text{ finite subgroups of } \mathscr{A}[\ell^\infty] \}$$

$$L \longleftrightarrow G$$

COMPLEX MULTIPLICATION ON THE TATE MODULE

Lattices in an ℓ-adic vector space $\longleftrightarrow$ Kernels of isogenies

$$\{\text{ lattices in } V \text{ containing } T \} \longleftrightarrow \{\text{ finite subgroups of } \mathscr{A}[\ell^\infty] \}$$

$$L \longleftrightarrow G$$

isogeny $\mathscr{A} \to \mathscr{A}/G$

COMPLEX MULTIPLICATION ON THE TATE MODULE

Lattices in an ℓ-adic vector space $\longleftrightarrow$ Kernels of isogenies

$$\{\text{ lattices in } V \text{ containing } T\,\} \longleftrightarrow \{\text{ finite subgroups of } \mathscr{A}[\ell^\infty]\,\}$$

$$L \qquad \longleftrightarrow \qquad G$$

isogeny $\mathscr{A} \to \mathscr{A}/G$

$$\mathscr{O}(L) \qquad \cong \qquad \mathrm{End}(\mathscr{A}/G) \otimes \mathbb{Z}_\ell$$

COMPLEX MULTIPLICATION ON THE TATE MODULE

Lattices in an ℓ-adic vector space $\longleftrightarrow$ Kernels of isogenies

$$\{\text{ lattices in } V \text{ containing } T\,\} \longleftrightarrow \{\text{ finite subgroups of } \mathscr{A}[\ell^\infty]\,\}$$

$$L \qquad \longleftrightarrow \qquad G$$

isogeny $\mathscr{A} \to \mathscr{A}/G$

$$\mathscr{O}(L) \qquad \cong \qquad \mathrm{End}(\mathscr{A}/G) \otimes \mathbb{Z}_\ell$$

- We can study isogenies and their relation to endomorphism rings by looking at lattices in the ℓ-adic vector space V.

ℓ-ADIC LATTICES AND $\mathfrak{l}$-ISOGENIES

LATTICES AND ℓ-ISOGENIES

$$\{\text{ lattices in } V \text{ containing } T\} \longleftrightarrow \{\text{ finite subgroups of } \mathscr{A}[\ell^\infty]\}$$

LATTICES AND $\mathfrak{l}$-ISOGENIES

$$\{\text{ lattices in } V \text{ containing } T\,\} \longleftrightarrow \{\text{ finite subgroups of } \mathscr{A}[\ell^\infty]\,\}$$

$$\cup$$

$$\{\text{ kernels of } \mathfrak{l}\text{-isogenies }\}$$

LATTICES AND $\mathfrak{L}$-ISOGENIES

$$\begin{array}{ccc} \{\text{ lattices in } V \text{ containing } T\ \} & \longleftrightarrow & \{\text{ finite subgroups of } \mathscr{A}[\ell^\infty]\ \} \\ & & \cup \\ ? & \longleftrightarrow & \{\text{ kernels of } \mathfrak{L}\text{-isogenies }\} \end{array}$$

LATTICES AND $\mathfrak{l}$-ISOGENIES

$$\{\text{ lattices in } V \text{ containing } T\ \} \longleftrightarrow \{\text{ finite subgroups of } \mathscr{A}[\ell^\infty]\ \}$$

$$\cup$$

? $\longleftrightarrow$ $\{\text{ kernels of } \mathfrak{l}\text{-isogenies }\}$

$$=$$

$$\{\text{ cyclic sub-}\mathscr{O}_{K_0}\text{-modules of } \mathscr{A}[\mathfrak{l}]\ \}$$

LATTICES AND $\mathfrak{l}$-ISOGENIES

$$\{ \text{lattices in } V \text{ containing } T \} \longleftrightarrow \{ \text{finite subgroups of } \mathscr{A}[\ell^\infty] \}$$

$$\cup$$

$$? \qquad \longleftrightarrow \qquad \{ \text{kernels of } \mathfrak{l}\text{-isogenies} \}$$

$$=$$

$$\{ \text{cyclic sub-}\mathscr{O}_{K_0}\text{-modules of } \mathscr{A}[\mathfrak{l}] \}$$

$$=$$

$$\{ \text{cyclic sub-}\mathscr{O}_{K_0}/\mathfrak{l}\text{-modules of } \mathscr{A}[\mathfrak{l}] \}$$

LATTICES AND $\mathfrak{l}$-ISOGENIES

$$\{\text{ lattices in } V \text{ containing } T\ \} \longleftrightarrow \{\text{ finite subgroups of } \mathscr{A}[\ell^\infty]\ \}$$

$$\cup$$

$$? \qquad \longleftrightarrow \qquad \{\text{ kernels of } \mathfrak{l}\text{-isogenies }\}$$

$$=$$

$$\{\text{ cyclic sub-}\mathcal{O}_{K_0}\text{-modules of } \mathscr{A}[\mathfrak{l}]\ \}$$

$$=$$

$$\{\text{ cyclic sub-}\mathcal{O}_{K_0}/\mathfrak{l}\text{-modules of } \mathscr{A}[\mathfrak{l}]\ \}$$

$$=$$

$$\{\text{ rank 1 sub-}F\text{-vector spaces of } \mathscr{A}[\mathfrak{l}]\ \}$$

$F = \mathcal{O}_{K_0}/\mathfrak{l}$ is a finite field

LATTICES AND $\mathfrak{l}$-ISOGENIES

$$\{\text{ lattices in } V \text{ containing } T\} \longleftrightarrow \{\text{ finite subgroups of } \mathscr{A}[\ell^\infty]\}$$

$$\cup \qquad\qquad\qquad\qquad \cup$$

$$\left\{\begin{array}{c}\text{lattices } L \text{ such that } T \subset L \\ \text{and } L/T \text{ is a sub-}F\text{-vector} \\ \text{space of rank 1 of } \mathfrak{l}^{-1}T/T\end{array}\right\} \longleftrightarrow \{\text{ kernels of } \mathfrak{l}\text{-isogenies }\}$$

$$=$$

$$\{\text{ cyclic sub-}\mathscr{O}_{K_0}\text{-modules of } \mathscr{A}[\mathfrak{l}]\}$$

$$=$$

$$\{\text{ cyclic sub-}\mathscr{O}_{K_0}/\mathfrak{l}\text{-modules of } \mathscr{A}[\mathfrak{l}]\}$$

$$=$$

$$\{\text{ rank 1 sub-}F\text{-vector spaces of } \mathscr{A}[\mathfrak{l}]\}$$

$F = \mathscr{O}_{K_0}/\mathfrak{l}$ is a finite field

LATTICES AND $\mathfrak{l}$-ISOGENIES

$$\begin{array}{ccc}
\{\text{ lattices in } V \text{ containing } T \} & \longleftrightarrow & \{\text{ finite subgroups of } \mathscr{A}[\ell^\infty] \} \\
\cup & & \cup \\
\left\{\begin{array}{c}\text{lattices } L \text{ such that } T \subset L \\ \text{and } L/T \text{ is a sub-}F\text{-vector} \\ \text{space of rank 1 of } \mathfrak{l}^{-1}T/T\end{array}\right\} & \longleftrightarrow & \{\text{ kernels of } \mathfrak{l}\text{-isogenies } \} \\
\updownarrow & & = \\
\mathbb{P}^1(T/\mathfrak{l}T) & & \{\text{ cyclic sub-}\mathcal{O}_{K_0}\text{-modules of } \mathscr{A}[\mathfrak{l}] \} \\
 & & = \\
 & & \{\text{ cyclic sub-}\mathcal{O}_{K_0}/\mathfrak{l}\text{-modules of } \mathscr{A}[\mathfrak{l}] \} \\
 & & = \\
 & & \{\text{ rank 1 sub-}F\text{-vector spaces of } \mathscr{A}[\mathfrak{l}] \}
\end{array}$$

$F = \mathcal{O}_{K_0}/\mathfrak{l}$ is a finite field

FINDING FIXED POINTS

$$\mathbb{P}^1(T/\mathfrak{l}T) \qquad \longleftrightarrow \qquad \{ \text{ kernels of } \mathfrak{l}\text{-isogenies } \}$$

FINDING FIXED POINTS

$$\mathbb{P}^1(T/\mathfrak{l}T) \quad \longleftrightarrow \quad \{ \text{ kernels of } \mathfrak{l}\text{-isogenies } \}$$

- Suppose $\mathcal{O} = \mathcal{O}(T)$ has maximal RM (i.e., $\mathcal{O}_{K_0} \otimes \mathbb{Z}_\ell \subset \mathcal{O}$). It is Gorenstein so T is a rank 1 free $\mathcal{O}$-module.

FINDING FIXED POINTS

$$\begin{array}{ccc} \mathbb{P}^1(T/\mathfrak{l}T) & \longleftrightarrow & \{ \text{ kernels of } \mathfrak{l}\text{-isogenies } \} \\ \updownarrow & & \\ \mathbb{P}^1(\mathcal{O}/\mathfrak{l}\mathcal{O}) & & \end{array}$$

- Suppose $\mathcal{O} = \mathcal{O}(T)$ has maximal RM (i.e., $\mathcal{O}_{K_0} \otimes \mathbb{Z}_\ell \subset \mathcal{O}$). It is Gorenstein so T is a rank 1 free $\mathcal{O}$-module.

FINDING FIXED POINTS

$$\begin{array}{ccc} \mathbb{P}^1(T/\mathfrak{l}T) & \longleftrightarrow & \{\text{ kernels of } \mathfrak{l}\text{-isogenies }\} \\ \updownarrow & & \\ \mathbb{P}^1(\mathcal{O}/\mathfrak{l}\mathcal{O}) & & \end{array}$$

- Suppose $\mathcal{O} = \mathcal{O}(T)$ has maximal RM (i.e., $\mathcal{O}_{K_0} \otimes \mathbb{Z}_\ell \subset \mathcal{O}$). It is Gorenstein so T is a rank 1 free $\mathcal{O}$-module.
- $\mathcal{O}^\times = (\mathrm{End}(\mathscr{A}) \otimes \mathbb{Z}_\ell)^\times$ acts on $\mathbb{P}^1(\mathcal{O}/\mathfrak{l}\mathcal{O})$, and elements that are **not** fixed by this action are descending $\mathfrak{l}$-isogenies.

FINDING FIXED POINTS

$$\mathbb{P}^1(\mathcal{O}/\mathfrak{l}\mathcal{O}) \quad \longleftrightarrow \quad \{ \text{ kernels of } \mathfrak{l}\text{-isogenies } \}$$

FINDING FIXED POINTS

$$\mathbb{P}^1(\mathcal{O}/\mathfrak{l}\mathcal{O}) \quad \longleftrightarrow \quad \{ \text{ kernels of } \mathfrak{l}\text{-isogenies } \}$$

- Let $\mathfrak{f}$ be the conductor of $\mathcal{O}$. Then, $\mathcal{O} = \mathcal{O}_{K_0} \otimes \mathbb{Z}_\ell + \mathfrak{f}(\mathcal{O}_K \otimes \mathbb{Z}_\ell)$.

FINDING FIXED POINTS

$$\mathbb{P}^1(\mathscr{O}/\mathfrak{l}\mathscr{O}) \quad \longleftrightarrow \quad \{ \text{ kernels of } \mathfrak{l}\text{-isogenies } \}$$

- Let $\mathfrak{f}$ be the conductor of $\mathscr{O}$. Then, $\mathscr{O} = \mathscr{O}_{K_0} \otimes \mathbb{Z}_\ell + \mathfrak{f}(\mathscr{O}_K \otimes \mathbb{Z}_\ell)$.
- The action of $\mathscr{O}^\times$ on $\mathbb{P}^1(\mathscr{O}/\mathfrak{l}\mathscr{O})$ has the following fixed points:

FINDING FIXED POINTS

$$\mathbb{P}^1(\mathcal{O}/\mathfrak{l}\mathcal{O}) \quad \longleftrightarrow \quad \{ \text{ kernels of } \mathfrak{l}\text{-isogenies } \}$$

- Let $\mathfrak{f}$ be the conductor of $\mathcal{O}$. Then, $\mathcal{O} = \mathcal{O}_{K_0} \otimes \mathbb{Z}_\ell + \mathfrak{f}(\mathcal{O}_K \otimes \mathbb{Z}_\ell)$.
- The action of $\mathcal{O}^\times$ on $\mathbb{P}^1(\mathcal{O}/\mathfrak{l}\mathcal{O})$ has the following fixed points:
  - $\varnothing$ if $\mathfrak{l} \nmid \mathfrak{f}$ and $\mathfrak{l}$ is inert in $\mathcal{O}$,

FINDING FIXED POINTS

$$\mathbb{P}^1(\mathcal{O}/\mathfrak{l}\mathcal{O}) \quad \longleftrightarrow \quad \{\text{ kernels of } \mathfrak{l}\text{-isogenies }\}$$

- Let $\mathfrak{f}$ be the conductor of $\mathcal{O}$. Then, $\mathcal{O} = \mathcal{O}_{K_0} \otimes \mathbb{Z}_\ell + \mathfrak{f}(\mathcal{O}_K \otimes \mathbb{Z}_\ell)$.
- The action of $\mathcal{O}^\times$ on $\mathbb{P}^1(\mathcal{O}/\mathfrak{l}\mathcal{O})$ has the following fixed points:
  - $\emptyset$ if $\mathfrak{l} \nmid \mathfrak{f}$ and $\mathfrak{l}$ is inert in $\mathcal{O}$,
  - $\{\mathfrak{L}_1/\mathfrak{l}\mathcal{O}, \mathfrak{L}_2/\mathfrak{l}\mathcal{O}\}$ if $\mathfrak{l} \nmid \mathfrak{f}$ and $\mathfrak{l}$ splits/ramifies as $\mathfrak{l}\mathcal{O} = \mathfrak{L}_1\mathfrak{L}_2$,

FINDING FIXED POINTS

$$\mathbb{P}^1(\mathcal{O}/\mathfrak{l}\mathcal{O}) \quad \longleftrightarrow \quad \{\text{ kernels of } \mathfrak{l}\text{-isogenies }\}$$

- Let $\mathfrak{f}$ be the conductor of $\mathcal{O}$. Then, $\mathcal{O} = \mathcal{O}_{K_0} \otimes \mathbb{Z}_\ell + \mathfrak{f}(\mathcal{O}_K \otimes \mathbb{Z}_\ell)$.
- The action of $\mathcal{O}^\times$ on $\mathbb{P}^1(\mathcal{O}/\mathfrak{l}\mathcal{O})$ has the following fixed points:
  - $\varnothing$ if $\mathfrak{l} \nmid \mathfrak{f}$ and $\mathfrak{l}$ is inert in $\mathcal{O}$,
  - $\{\mathfrak{L}_1/\mathfrak{l}\mathcal{O}, \mathfrak{L}_2/\mathfrak{l}\mathcal{O}\}$ if $\mathfrak{l} \nmid \mathfrak{f}$ and $\mathfrak{l}$ splits/ramifies as $\mathfrak{l}\mathcal{O} = \mathfrak{L}_1\mathfrak{L}_2$,
  - $\{\mathfrak{l}\mathcal{O}'/\mathfrak{l}\mathcal{O}\}$ if $\mathfrak{l} \mid \mathfrak{f}$, with $\mathcal{O}'$ the order of conductor $\mathfrak{l}^{-1}\mathfrak{f}$.

FINDING FIXED POINTS

$$\mathbb{P}^1(\mathcal{O}/\mathfrak{l}\mathcal{O}) \quad \longleftrightarrow \quad \{\text{ kernels of } \mathfrak{l}\text{-isogenies }\}$$

- Let $\mathfrak{f}$ be the conductor of $\mathcal{O}$. Then, $\mathcal{O} = \mathcal{O}_{K_0} \otimes \mathbb{Z}_\ell + \mathfrak{f}(\mathcal{O}_K \otimes \mathbb{Z}_\ell)$.
- The action of $\mathcal{O}^\times$ on $\mathbb{P}^1(\mathcal{O}/\mathfrak{l}\mathcal{O})$ has the following fixed points:
  - $\varnothing$ if $\mathfrak{l} \nmid \mathfrak{f}$ and $\mathfrak{l}$ is inert in $\mathcal{O}$,
  - $\{\mathfrak{L}_1/\mathfrak{l}\mathcal{O}, \mathfrak{L}_2/\mathfrak{l}\mathcal{O}\}$ if $\mathfrak{l} \nmid \mathfrak{f}$ and $\mathfrak{l}$ splits/ramifies as $\mathfrak{l}\mathcal{O} = \mathfrak{L}_1\mathfrak{L}_2$,
  - $\{\mathfrak{l}\mathcal{O}'/\mathfrak{l}\mathcal{O}\}$ if $\mathfrak{l} \mid \mathfrak{f}$, with $\mathcal{O}'$ the order of conductor $\mathfrak{l}^{-1}\mathfrak{f}$.

All the other (non-fixed) elements give descending isogenies

FINDING FIXED POINTS

$$\mathbb{P}^1(\mathcal{O}/\mathfrak{l}\mathcal{O}) \quad \longleftrightarrow \quad \{\text{ kernels of } \mathfrak{l}\text{-isogenies }\}$$

- Let $\mathfrak{f}$ be the conductor of $\mathcal{O}$. Then, $\mathcal{O} = \mathcal{O}_{K_0} \otimes \mathbb{Z}_\ell + \mathfrak{f}(\mathcal{O}_K \otimes \mathbb{Z}_\ell)$.
- The action of $\mathcal{O}^\times$ on $\mathbb{P}^1(\mathcal{O}/\mathfrak{l}\mathcal{O})$ has the following fixed points:
  - $\varnothing$ if $\mathfrak{l} \nmid \mathfrak{f}$ and $\mathfrak{l}$ is inert in $\mathcal{O}$,
  - $\{\mathfrak{L}_1/\mathfrak{l}\mathcal{O}, \mathfrak{L}_2/\mathfrak{l}\mathcal{O}\}$ if $\mathfrak{l} \nmid \mathfrak{f}$ and $\mathfrak{l}$ splits/ramifies as $\mathfrak{l}\mathcal{O} = \mathfrak{L}_1\mathfrak{L}_2$,
  - $\{\mathfrak{l}\mathcal{O}'/\mathfrak{l}\mathcal{O}\}$ if $\mathfrak{l} \mid \mathfrak{f}$, with $\mathcal{O}'$ the order of conductor $\mathfrak{l}^{-1}\mathfrak{f}$.

the surface

All the other (non-fixed) elements give descending isogenies

FINDING FIXED POINTS

$$\mathbb{P}^1(\mathcal{O}/\mathfrak{l}\mathcal{O}) \quad \longleftrightarrow \quad \{\text{ kernels of } \mathfrak{l}\text{-isogenies }\}$$

- Let $\mathfrak{f}$ be the conductor of $\mathcal{O}$. Then, $\mathcal{O} = \mathcal{O}_{K_0} \otimes \mathbb{Z}_\ell + \mathfrak{f}(\mathcal{O}_K \otimes \mathbb{Z}_\ell)$.
- The action of $\mathcal{O}^\times$ on $\mathbb{P}^1(\mathcal{O}/\mathfrak{l}\mathcal{O})$ has the following fixed points:
  - $\varnothing$ if $\mathfrak{l} \nmid \mathfrak{f}$ and $\mathfrak{l}$ is inert in $\mathcal{O}$,
  - $\{\mathfrak{L}_1/\mathfrak{l}\mathcal{O}, \mathfrak{L}_2/\mathfrak{l}\mathcal{O}\}$ if $\mathfrak{l} \nmid \mathfrak{f}$ and $\mathfrak{l}$ splits/ramifies as $\mathfrak{l}\mathcal{O} = \mathfrak{L}_1\mathfrak{L}_2$,
  - $\{\mathfrak{l}\mathcal{O}'/\mathfrak{l}\mathcal{O}\}$ if $\mathfrak{l} \mid \mathfrak{f}$, with $\mathcal{O}'$ the order of conductor $\mathfrak{l}^{-1}\mathfrak{f}$.

the surface

Is this isogeny ascending?

All the other (non-fixed) elements give descending isogenies

FINDING FIXED POINTS

- The action of $\mathcal{O}^\times$ on $\mathbb{P}^1(\mathcal{O}/\mathfrak{l}\mathcal{O})$ has the following fixed points:
  - $\varnothing$ if $\mathfrak{l} \nmid \mathfrak{f}$ and $\mathfrak{l}$ is inert in $\mathcal{O}$,
  - $\{\mathfrak{L}_1/\mathfrak{l}\mathcal{O}, \mathfrak{L}_2/\mathfrak{l}\mathcal{O}\}$ if $\mathfrak{l} \nmid \mathfrak{f}$ and $\mathfrak{l}$ splits/ramifies as $\mathfrak{l}\mathcal{O} = \mathfrak{L}_1\mathfrak{L}_2$,
  - $\{\mathfrak{l}\mathcal{O}'/\mathfrak{l}\mathcal{O}\}$ if $\mathfrak{l} \mid \mathfrak{f}$, with $\mathcal{O}'$ the order of conductor $\mathfrak{l}^{-1}\mathfrak{f}$.

the surface

FINDING FIXED POINTS

- The action of $\mathcal{O}^\times$ on $\mathbb{P}^1(\mathcal{O}/\mathfrak{l}\mathcal{O})$ has the following fixed points:
  - $\varnothing$ if $\mathfrak{l} \nmid \mathfrak{f}$ and $\mathfrak{l}$ is inert in $\mathcal{O}$,
  - $\{\mathfrak{L}_1/\mathfrak{l}\mathcal{O}, \mathfrak{L}_2/\mathfrak{l}\mathcal{O}\}$ if $\mathfrak{l} \nmid \mathfrak{f}$ and $\mathfrak{l}$ splits/ramifies as $\mathfrak{l}\mathcal{O} = \mathfrak{L}_1\mathfrak{L}_2$,
  - $\{\mathfrak{l}\mathcal{O}'/\mathfrak{l}\mathcal{O}\}$ if $\mathfrak{l} \mid \mathfrak{f}$, with $\mathcal{O}'$ the order of conductor $\mathfrak{l}^{-1}\mathfrak{f}$.

the surface

$$\mathbb{P}^1(\mathcal{O}/\mathfrak{l}\mathcal{O}) \longleftrightarrow \left\{ \begin{array}{c} \text{lattices } L \text{ such that } T \subset L \\ \text{and } L/T \text{ is a sub-}F\text{-vector} \\ \text{space of rank 1 of } \mathfrak{l}^{-1}T/T \end{array} \right\}$$

FINDING FIXED POINTS

- The action of $\mathcal{O}^\times$ on $\mathbb{P}^1(\mathcal{O}/\mathfrak{l}\mathcal{O})$ has the following fixed points:
  - $\varnothing$ if $\mathfrak{l} \nmid \mathfrak{f}$ and $\mathfrak{l}$ is inert in $\mathcal{O}$,
  - $\{\mathfrak{L}_1/\mathfrak{l}\mathcal{O}, \mathfrak{L}_2/\mathfrak{l}\mathcal{O}\}$ if $\mathfrak{l} \nmid \mathfrak{f}$ and $\mathfrak{l}$ splits/ramifies as $\mathfrak{l}\mathcal{O} = \mathfrak{L}_1\mathfrak{L}_2$,
  - $\{\mathfrak{l}\mathcal{O}'/\mathfrak{l}\mathcal{O}\}$ if $\mathfrak{l} \mid \mathfrak{f}$, with $\mathcal{O}'$ the order of conductor $\mathfrak{l}^{-1}\mathfrak{f}$.

the surface

$$\mathbb{P}^1(\mathcal{O}/\mathfrak{l}\mathcal{O}) \longleftrightarrow \left\{ \begin{array}{c} \text{lattices } L \text{ such that } T \subset L \\ \text{and } L/T \text{ is a sub-}F\text{-vector} \\ \text{space of rank 1 of } \mathfrak{l}^{-1}T/T \end{array} \right\}$$

$\mathfrak{l}\mathcal{O}'/\mathfrak{l}\mathcal{O}$

FINDING FIXED POINTS

- The action of $\mathcal{O}^\times$ on $\mathbb{P}^1(\mathcal{O}/\mathfrak{l}\mathcal{O})$ has the following fixed points:
  - $\varnothing$ if $\mathfrak{l} \nmid \mathfrak{f}$ and $\mathfrak{l}$ is inert in $\mathcal{O}$,
  - $\{\mathfrak{L}_1/\mathfrak{l}\mathcal{O}, \mathfrak{L}_2/\mathfrak{l}\mathcal{O}\}$ if $\mathfrak{l} \nmid \mathfrak{f}$ and $\mathfrak{l}$ splits/ramifies as $\mathfrak{l}\mathcal{O} = \mathfrak{L}_1\mathfrak{L}_2$,
  - $\{\mathfrak{l}\mathcal{O}'/\mathfrak{l}\mathcal{O}\}$ if $\mathfrak{l} \mid \mathfrak{f}$, with $\mathcal{O}'$ the order of conductor $\mathfrak{l}^{-1}\mathfrak{f}$.

the surface

$$\mathbb{P}^1(\mathcal{O}/\mathfrak{l}\mathcal{O}) \longleftrightarrow \left\{ \begin{array}{c} \text{lattices } L \text{ such that } T \subset L \\ \text{and } L/T \text{ is a sub-}F\text{-vector} \\ \text{space of rank 1 of } \mathfrak{l}^{-1}T/T \end{array} \right\}$$

$$\mathfrak{l}\mathcal{O}'/\mathfrak{l}\mathcal{O} \longleftrightarrow \mathfrak{l}\mathcal{O}'T$$

FINDING FIXED POINTS

- The action of $\mathcal{O}^\times$ on $\mathbb{P}^1(\mathcal{O}/\mathfrak{l}\mathcal{O})$ has the following fixed points:
  - $\varnothing$ if $\mathfrak{l} \nmid \mathfrak{f}$ and $\mathfrak{l}$ is inert in $\mathcal{O}$,
  - $\{\mathfrak{L}_1/\mathfrak{l}\mathcal{O}, \mathfrak{L}_2/\mathfrak{l}\mathcal{O}\}$ if $\mathfrak{l} \nmid \mathfrak{f}$ and $\mathfrak{l}$ splits/ramifies as $\mathfrak{l}\mathcal{O} = \mathfrak{L}_1\mathfrak{L}_2$,
  - $\{\mathfrak{l}\mathcal{O}'/\mathfrak{l}\mathcal{O}\}$ if $\mathfrak{l} \mid \mathfrak{f}$, with $\mathcal{O}'$ the order of conductor $\mathfrak{l}^{-1}\mathfrak{f}$.

the surface

$$\mathbb{P}^1(\mathcal{O}/\mathfrak{l}\mathcal{O}) \longleftrightarrow \left\{ \begin{array}{c} \text{lattices } L \text{ such that } T \subset L \\ \text{and } L/T \text{ is a sub-}F\text{-vector} \\ \text{space of rank 1 of } \mathfrak{l}^{-1}T/T \end{array} \right\}$$

$$\mathfrak{l}\mathcal{O}'/\mathfrak{l}\mathcal{O} \longleftrightarrow \mathfrak{l}\mathcal{O}'T$$

$$\mathcal{O}(\mathfrak{l}\mathcal{O}'T) = \mathcal{O}'$$

FINDING FIXED POINTS

- The action of $\mathcal{O}^\times$ on $\mathbb{P}^1(\mathcal{O}/\mathfrak{l}\mathcal{O})$ has the following fixed points:
  - $\emptyset$ if $\mathfrak{l} \nmid \mathfrak{f}$ and $\mathfrak{l}$ is inert in $\mathcal{O}$,
  - $\{\mathfrak{L}_1/\mathfrak{l}\mathcal{O}, \mathfrak{L}_2/\mathfrak{l}\mathcal{O}\}$ if $\mathfrak{l} \nmid \mathfrak{f}$ and $\mathfrak{l}$ splits/ramifies as $\mathfrak{l}\mathcal{O} = \mathfrak{L}_1\mathfrak{L}_2$,

    the surface
  - $\{\mathfrak{l}\mathcal{O}'/\mathfrak{l}\mathcal{O}\}$ if $\mathfrak{l} \mid \mathfrak{f}$, with $\mathcal{O}'$ the order of conductor $\mathfrak{l}^{-1}\mathfrak{f}$.

$$\mathbb{P}^1(\mathcal{O}/\mathfrak{l}\mathcal{O}) \longleftrightarrow \left\{\begin{array}{c}\text{lattices } L \text{ such that } T \subset L \\ \text{and } L/T \text{ is a sub-}F\text{-vector} \\ \text{space of rank 1 of } \mathfrak{l}^{-1}T/T\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{kernels of} \\ \mathfrak{l}\text{-isogenies}\end{array}\right\}$$

$$\mathfrak{l}\mathcal{O}'/\mathfrak{l}\mathcal{O} \longleftrightarrow \mathfrak{l}\mathcal{O}'T$$

$$\mathcal{O}(\mathfrak{l}\mathcal{O}'T) = \mathcal{O}'$$

FINDING FIXED POINTS

- The action of $\mathcal{O}^\times$ on $\mathbb{P}^1(\mathcal{O}/\mathfrak{l}\mathcal{O})$ has the following fixed points:
  - $\varnothing$ if $\mathfrak{l} \nmid \mathfrak{f}$ and $\mathfrak{l}$ is inert in $\mathcal{O}$,
  - $\{\mathfrak{L}_1/\mathfrak{l}\mathcal{O}, \mathfrak{L}_2/\mathfrak{l}\mathcal{O}\}$ if $\mathfrak{l} \nmid \mathfrak{f}$ and $\mathfrak{l}$ splits/ramifies as $\mathfrak{l}\mathcal{O} = \mathfrak{L}_1\mathfrak{L}_2$,

    the surface
  - $\{\mathfrak{l}\mathcal{O}'/\mathfrak{l}\mathcal{O}\}$ if $\mathfrak{l} \mid \mathfrak{f}$, with $\mathcal{O}'$ the order of conductor $\mathfrak{l}^{-1}\mathfrak{f}$.

$$\mathbb{P}^1(\mathcal{O}/\mathfrak{l}\mathcal{O}) \longleftrightarrow \left\{\begin{array}{c}\text{lattices } L \text{ such that } T \subset L \\ \text{and } L/T \text{ is a sub-}F\text{-vector} \\ \text{space of rank 1 of } \mathfrak{l}^{-1}T/T\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{kernels of} \\ \mathfrak{l}\text{-isogenies}\end{array}\right\}$$

$$\mathfrak{l}\mathcal{O}'/\mathfrak{l}\mathcal{O} \longleftrightarrow \mathfrak{l}\mathcal{O}'T \longleftrightarrow G$$

$$\mathcal{O}(\mathfrak{l}\mathcal{O}'T) = \mathcal{O}'$$

FINDING FIXED POINTS

- The action of $\mathcal{O}^\times$ on $\mathbb{P}^1(\mathcal{O}/\mathfrak{l}\mathcal{O})$ has the following fixed points:
  - $\varnothing$ if $\mathfrak{l} \nmid \mathfrak{f}$ and $\mathfrak{l}$ is inert in $\mathcal{O}$,
  - $\{\mathfrak{L}_1/\mathfrak{l}\mathcal{O}, \mathfrak{L}_2/\mathfrak{l}\mathcal{O}\}$ if $\mathfrak{l} \nmid \mathfrak{f}$ and $\mathfrak{l}$ splits/ramifies as $\mathfrak{l}\mathcal{O} = \mathfrak{L}_1\mathfrak{L}_2$,

  the surface

  - $\{\mathfrak{l}\mathcal{O}'/\mathfrak{l}\mathcal{O}\}$ if $\mathfrak{l} \mid \mathfrak{f}$, with $\mathcal{O}'$ the order of conductor $\mathfrak{l}^{-1}\mathfrak{f}$.

$$\mathbb{P}^1(\mathcal{O}/\mathfrak{l}\mathcal{O}) \longleftrightarrow \left\{\begin{array}{c}\text{lattices } L \text{ such that } T \subset L \\ \text{and } L/T \text{ is a sub-}F\text{-vector} \\ \text{space of rank 1 of } \mathfrak{l}^{-1}T/T\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{kernels of} \\ \mathfrak{l}\text{-isogenies}\end{array}\right\}$$

$$\mathfrak{l}\mathcal{O}'/\mathfrak{l}\mathcal{O} \longleftrightarrow \mathfrak{l}\mathcal{O}'T \longleftrightarrow G$$

$$\mathcal{O}(\mathfrak{l}\mathcal{O}'T) = \mathcal{O}' \implies \mathrm{End}(\mathscr{A}/G) \otimes \mathbb{Z}_\ell \cong \mathcal{O}'$$

FINDING FIXED POINTS

- The action of $\mathcal{O}^\times$ on $\mathbb{P}^1(\mathcal{O}/\mathfrak{l}\mathcal{O})$ has the following fixed points:
  - $\varnothing$ if $\mathfrak{l} \nmid \mathfrak{f}$ and $\mathfrak{l}$ is inert in $\mathcal{O}$,
  - $\{\mathfrak{L}_1/\mathfrak{l}\mathcal{O}, \mathfrak{L}_2/\mathfrak{l}\mathcal{O}\}$ if $\mathfrak{l} \nmid \mathfrak{f}$ and $\mathfrak{l}$ splits/ramifies as $\mathfrak{l}\mathcal{O} = \mathfrak{L}_1\mathfrak{L}_2$,

    the surface
  - $\{\mathfrak{l}\mathcal{O}'/\mathfrak{l}\mathcal{O}\}$ if $\mathfrak{l} \mid \mathfrak{f}$, with $\mathcal{O}'$ the order of conductor $\mathfrak{l}^{-1}\mathfrak{f}$.

$$\mathbb{P}^1(\mathcal{O}/\mathfrak{l}\mathcal{O}) \longleftrightarrow \left\{\begin{matrix}\text{lattices } L \text{ such that } T \subset L \\ \text{and } L/T \text{ is a sub-}F\text{-vector} \\ \text{space of rank 1 of } \mathfrak{l}^{-1}T/T\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\text{kernels of} \\ \mathfrak{l}\text{-isogenies}\end{matrix}\right\}$$

$$\mathfrak{l}\mathcal{O}'/\mathfrak{l}\mathcal{O} \longleftrightarrow \mathfrak{l}\mathcal{O}'T \longleftrightarrow G$$

$$\mathcal{O}(\mathfrak{l}\mathcal{O}'T) = \mathcal{O}' \quad\Longrightarrow\quad \mathrm{End}(\mathscr{A}/G) \otimes \mathbb{Z}_\ell \cong \mathcal{O}'$$

the corresponding isogeny is ascending

VOLCANOES ALREADY?

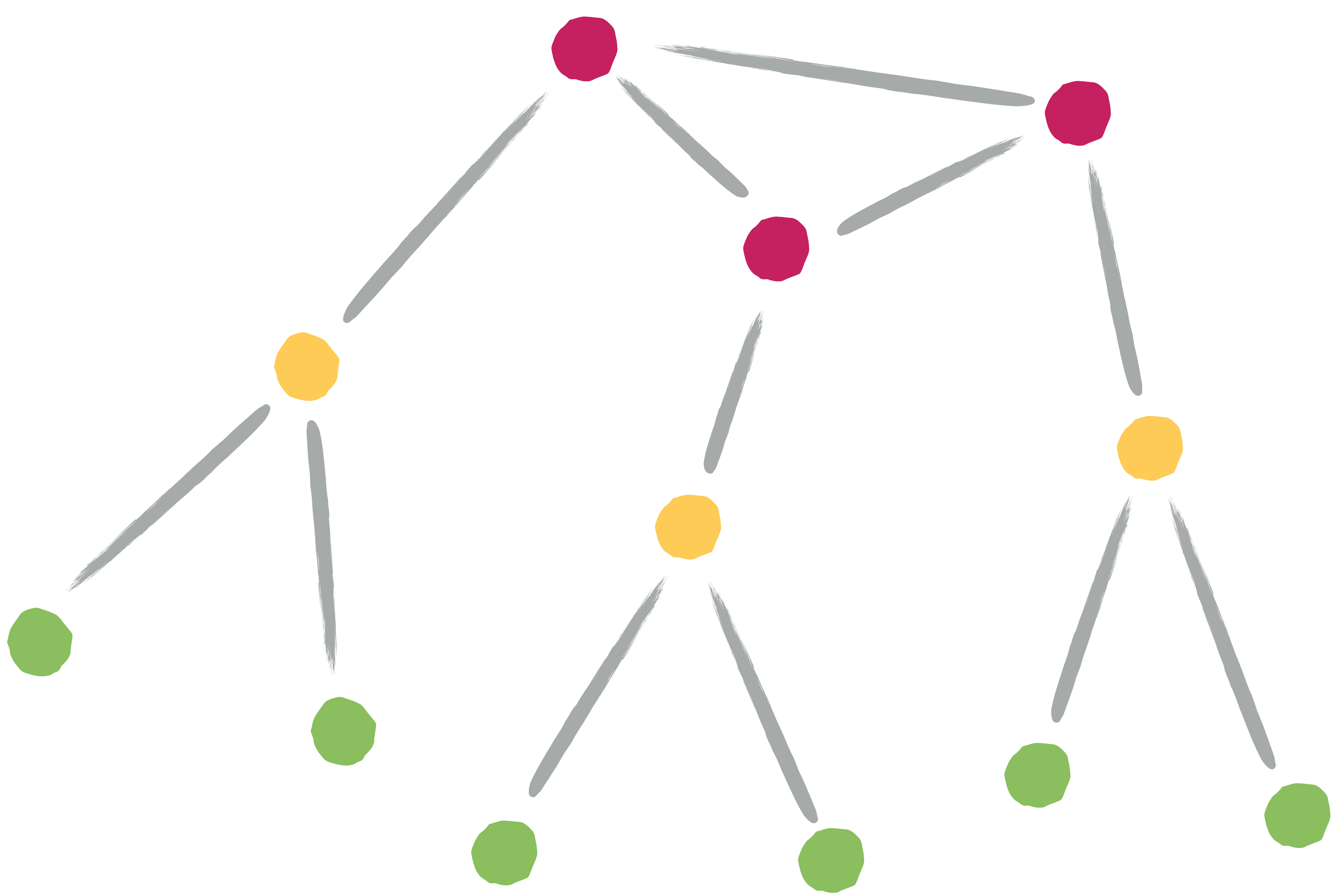
Is this enough?

For any vertex, we know how many outgoing edges are ascending, descending or horizontal… But this does not imply “volcano”

VOLCANOES ALREADY?

Is this enough?

For any vertex, we know how many outgoing edges are ascending, descending or horizontal… But this does not imply "volcano"



$\mathrm{End} \cong \mathcal{O}_{K_0} + \mathfrak{f}\mathcal{O}_K$

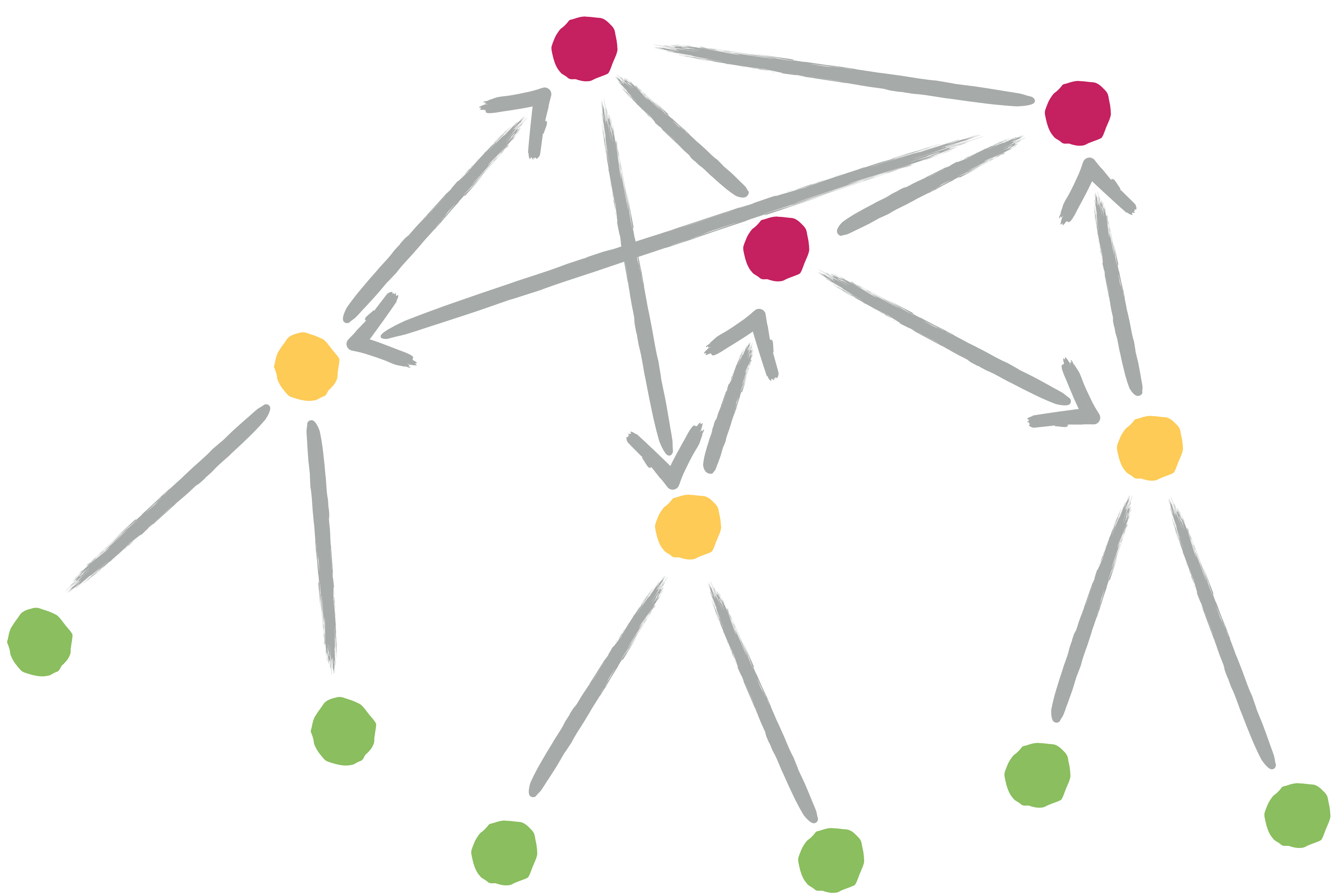
$\mathrm{End} \cong \mathcal{O}_{K_0} + \mathfrak{l}\mathfrak{f}\mathcal{O}_K$

$\mathrm{End} \cong \mathcal{O}_{K_0} + \mathfrak{l}^2\mathfrak{f}\mathcal{O}_K$

VOLCANOES ALREADY?

Is this enough?

For any vertex, we know how many outgoing edges are ascending, descending or horizontal... But this does not imply "volcano"

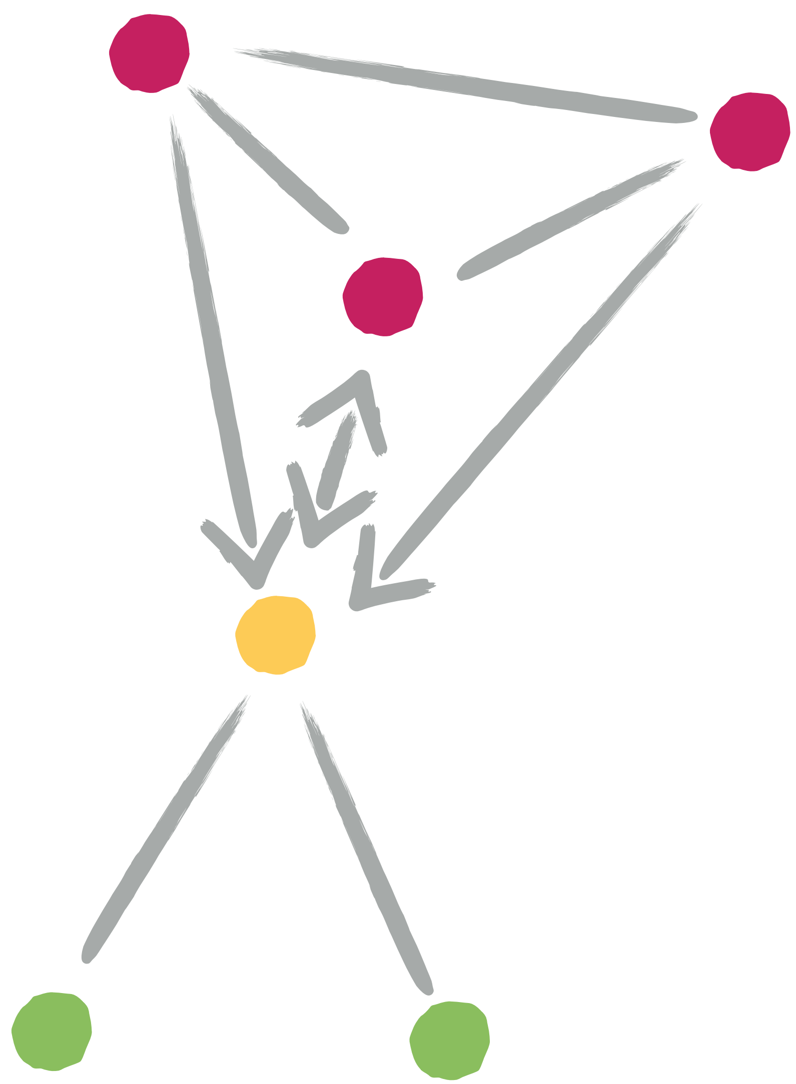


Why not this?

VOLCANOES ALREADY?

Is this enough?

For any vertex, we know how many outgoing edges are ascending, descending or horizontal... But this does not imply "volcano"

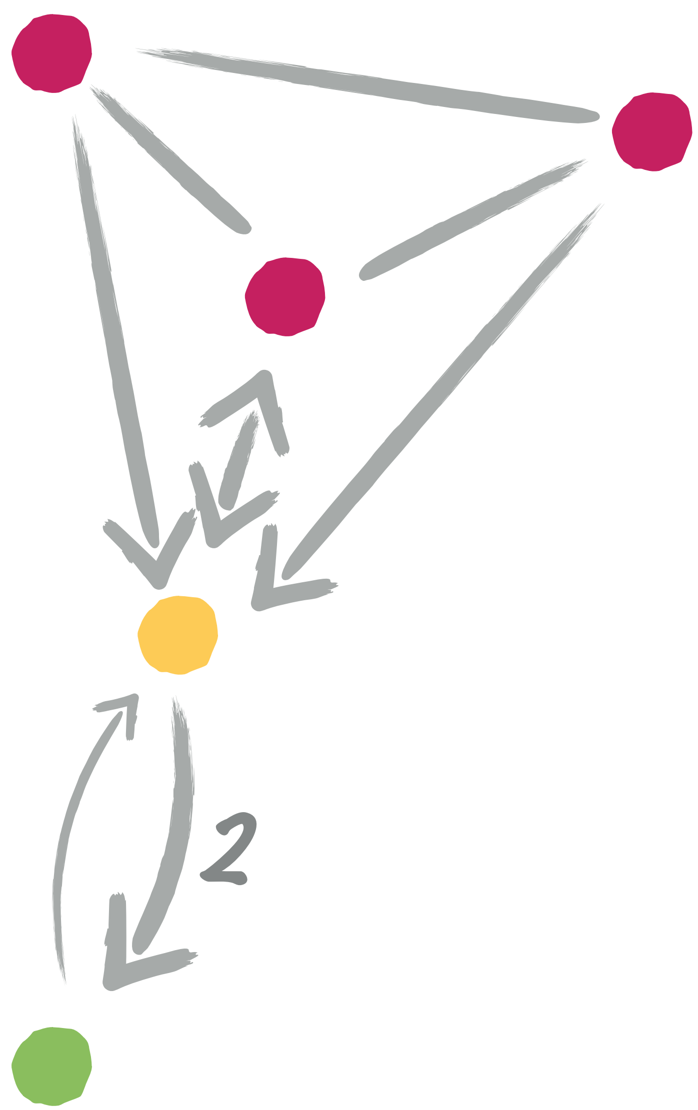


Or this?

VOLCANOES ALREADY?

Is this enough?

For any vertex, we know how many outgoing edges are ascending, descending or horizontal... But this does not imply "volcano"



What about this?

DESCENDING, THEN ASCENDING

- If $\mathscr{A} \longrightarrow \mathscr{B}$ is a descending $\mathfrak{l}$-isogeny, where does the **unique** ascending isogeny from $\mathscr{B}$ go?

DESCENDING, THEN ASCENDING

- If $\mathscr{A} \longrightarrow \mathscr{B}$ is a descending $\mathfrak{l}$-isogeny, where does the **unique** ascending isogeny from $\mathscr{B}$ go?

$$\begin{tikzcd}
\mathscr{A} \arrow[dr] & \\
& \mathscr{B}
\end{tikzcd}$$

DESCENDING, THEN ASCENDING

- If $\mathscr{A} \longrightarrow \mathscr{B}$ is a descending $\mathfrak{l}$-isogeny, where does the **unique** ascending isogeny from $\mathscr{B}$ go?

$$\begin{tikzcd}
\mathscr{A} \arrow[dr] & & \mathscr{C} \\
& \mathscr{B} \arrow[ur] &
\end{tikzcd}$$

DESCENDING, THEN ASCENDING

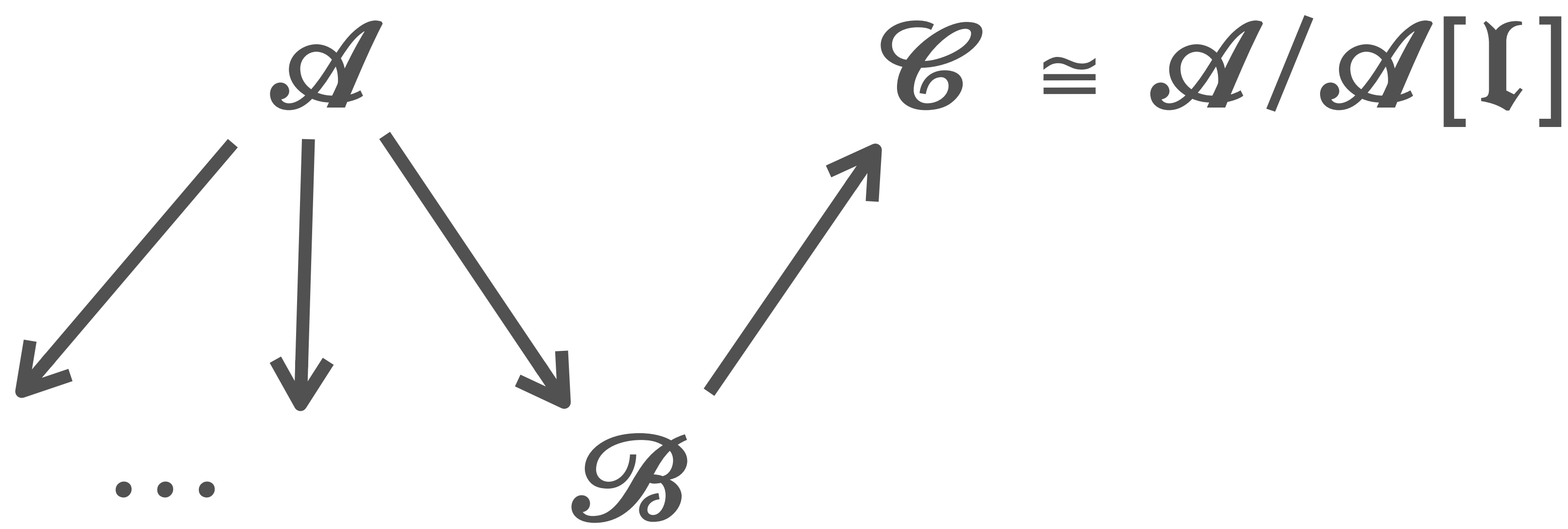
- If $\mathscr{A} \longrightarrow \mathscr{B}$ is a descending $\mathfrak{l}$-isogeny, where does the **unique** ascending isogeny from $\mathscr{B}$ go?

$$\begin{tikzcd}
\mathscr{A} \arrow[dr] & & \mathscr{C} \cong \mathscr{A}/\mathscr{A}[\mathfrak{l}] \\
& \mathscr{B} \arrow[ur] &
\end{tikzcd}$$

- It goes to $\mathscr{C} \cong \mathscr{A}/\mathscr{A}[\mathfrak{l}]$.

DESCENDING, THEN ASCENDING

- If $\mathscr{A} \longrightarrow \mathscr{B}$ is a descending $\mathfrak{l}$-isogeny, where does the **unique** ascending isogeny from $\mathscr{B}$ go?



- It goes to $\mathscr{C} \cong \mathscr{A}/\mathscr{A}[\mathfrak{l}]$.

DESCENDING, THEN ASCENDING

- If $\mathscr{A} \longrightarrow \mathscr{B}$ is a descending $\mathfrak{l}$-isogeny, where does the **unique** ascending isogeny from $\mathscr{B}$ go?

$$
\begin{tikzcd}
& \mathscr{A} \arrow[dl] \arrow[d] \arrow[dr] & & \mathscr{C} \cong \mathscr{A}/\mathscr{A}[\mathfrak{l}] \\
\mathscr{B}_3 & \mathscr{B}_2 & \mathscr{B}_1 \arrow[ur] &
\end{tikzcd}
$$

- It goes to $\mathscr{C} \cong \mathscr{A}/\mathscr{A}[\mathfrak{l}]$.

DESCENDING, THEN ASCENDING

- If $\mathscr{A} \longrightarrow \mathscr{B}$ is a descending $\mathfrak{l}$-isogeny, where does the **unique** ascending isogeny from $\mathscr{B}$ go?

$$
\begin{tikzcd}
 & & \mathscr{A} \arrow[dll] \arrow[d] \arrow[drr] & & & \mathscr{C} \cong \mathscr{A}/\mathscr{A}[\mathfrak{l}] \\
\mathscr{B}_3 \arrow[urrrrr] & & \mathscr{B}_2 \arrow[urrr] & & \mathscr{B}_1 \arrow[ur] &
\end{tikzcd}
$$

- It goes to $\mathscr{C} \cong \mathscr{A}/\mathscr{A}[\mathfrak{l}]$.

DESCENDING, THEN ASCENDING

- If $\mathscr{A} \longrightarrow \mathscr{B}$ is a descending $\mathfrak{l}$-isogeny, where does the **unique** ascending isogeny from $\mathscr{B}$ go?

$$\begin{tikzcd}
 & \mathscr{A} \arrow[dl] \arrow[d] \arrow[dr] & & \mathscr{C} \cong \mathscr{A}/\mathscr{A}[\mathfrak{l}] \\
\mathscr{B}_3 \arrow[urrr] & \mathscr{B}_2 \arrow[urr] & \mathscr{B}_1 \arrow[ur] &
\end{tikzcd}$$

- It goes to $\mathscr{C} \cong \mathscr{A}/\mathscr{A}[\mathfrak{l}]$.

- If $\mathfrak{l} = (\alpha)$ is principal, then the endomorphism α induces an isomorphism $\mathscr{A} \cong \mathscr{A}/\mathscr{A}[\mathfrak{l}]$.

DESCENDING, THEN ASCENDING

- If $\mathscr{A} \longrightarrow \mathscr{B}$ is a descending $\mathfrak{l}$-isogeny, where does the **unique** ascending isogeny from $\mathscr{B}$ go?

$$\begin{tikzcd} & \mathscr{A} \cong \mathscr{A}/\mathscr{A}[\mathfrak{l}] \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\ \mathscr{B}_3 & \mathscr{B}_2 & \mathscr{B}_1 \end{tikzcd}$$

- It goes to $\mathscr{C} \cong \mathscr{A}/\mathscr{A}[\mathfrak{l}]$.

- If $\mathfrak{l} = (\alpha)$ is principal, then the endomorphism α induces an isomorphism $\mathscr{A} \cong \mathscr{A}/\mathscr{A}[\mathfrak{l}]$.

MULTIPLICITIES

- Suppose there is a descending $\mathfrak{l}$-isogeny $\mathscr{A} \longrightarrow \mathscr{B}$.

MULTIPLICITIES

- Suppose there is a descending $\mathfrak{l}$-isogeny $\mathscr{A} \longrightarrow \mathscr{B}$.
- Then, there are $[\mathrm{End}(\mathscr{A})^\times : \mathrm{End}(\mathscr{B})^\times]$ distinct kernels of $\mathfrak{l}$-isogeny $\mathscr{A} \longrightarrow \mathscr{B}$.

MULTIPLICITIES

- Suppose there is a descending $\mathfrak{l}$-isogeny $\mathscr{A} \longrightarrow \mathscr{B}$.
- Then, there are $[\mathrm{End}(\mathscr{A})^\times : \mathrm{End}(\mathscr{B})^\times]$ distinct kernels of $\mathfrak{l}$-isogeny $\mathscr{A} \longrightarrow \mathscr{B}$.

$$\begin{tikzcd}
\mathscr{A} \arrow[dr, "{[\mathrm{End}(\mathscr{A})^\times : \mathrm{End}(\mathscr{B})^\times]}"'] & \\
& \mathscr{B}
\end{tikzcd}$$

MULTIPLICITIES

- Suppose there is a descending $\mathfrak{l}$-isogeny $\mathscr{A} \longrightarrow \mathscr{B}$.
- Then, there are $[\mathrm{End}(\mathscr{A})^\times : \mathrm{End}(\mathscr{B})^\times]$ distinct kernels of $\mathfrak{l}$-isogeny $\mathscr{A} \longrightarrow \mathscr{B}$.

$$\begin{tikzcd} \mathscr{A} \arrow[dr, "{[\mathrm{End}(\mathscr{A})^\times : \mathrm{End}(\mathscr{B})^\times]}"'] & & \mathscr{A}/\mathscr{A}[\mathfrak{l}] \\ & \mathscr{B} \arrow[ur, "1"'] & \end{tikzcd}$$

MULTIPLICITIES

- Suppose there is a descending $\mathfrak{l}$-isogeny $\mathscr{A} \longrightarrow \mathscr{B}$.
- Then, there are $[\mathrm{End}(\mathscr{A})^\times : \mathrm{End}(\mathscr{B})^\times]$ distinct kernels of $\mathfrak{l}$-isogeny $\mathscr{A} \longrightarrow \mathscr{B}$.

$$\begin{tikzcd}
\mathscr{A} \arrow[dr, "{[\mathrm{End}(\mathscr{A})^\times : \mathrm{End}(\mathscr{B})^\times]}"'] & & \mathscr{A}/\mathscr{A}[\mathfrak{l}] \\
& \mathscr{B} \arrow[ur, "1"'] &
\end{tikzcd}$$

- The index $[\mathrm{End}(\mathscr{A})^\times : \mathrm{End}(\mathscr{B})^\times]$ is always 1 if all the units of K are totally real (it is the case of any quartic $K \neq \mathbb{Q}(\zeta_5)$)

COUNTING VERTICES AND CONCLUDING

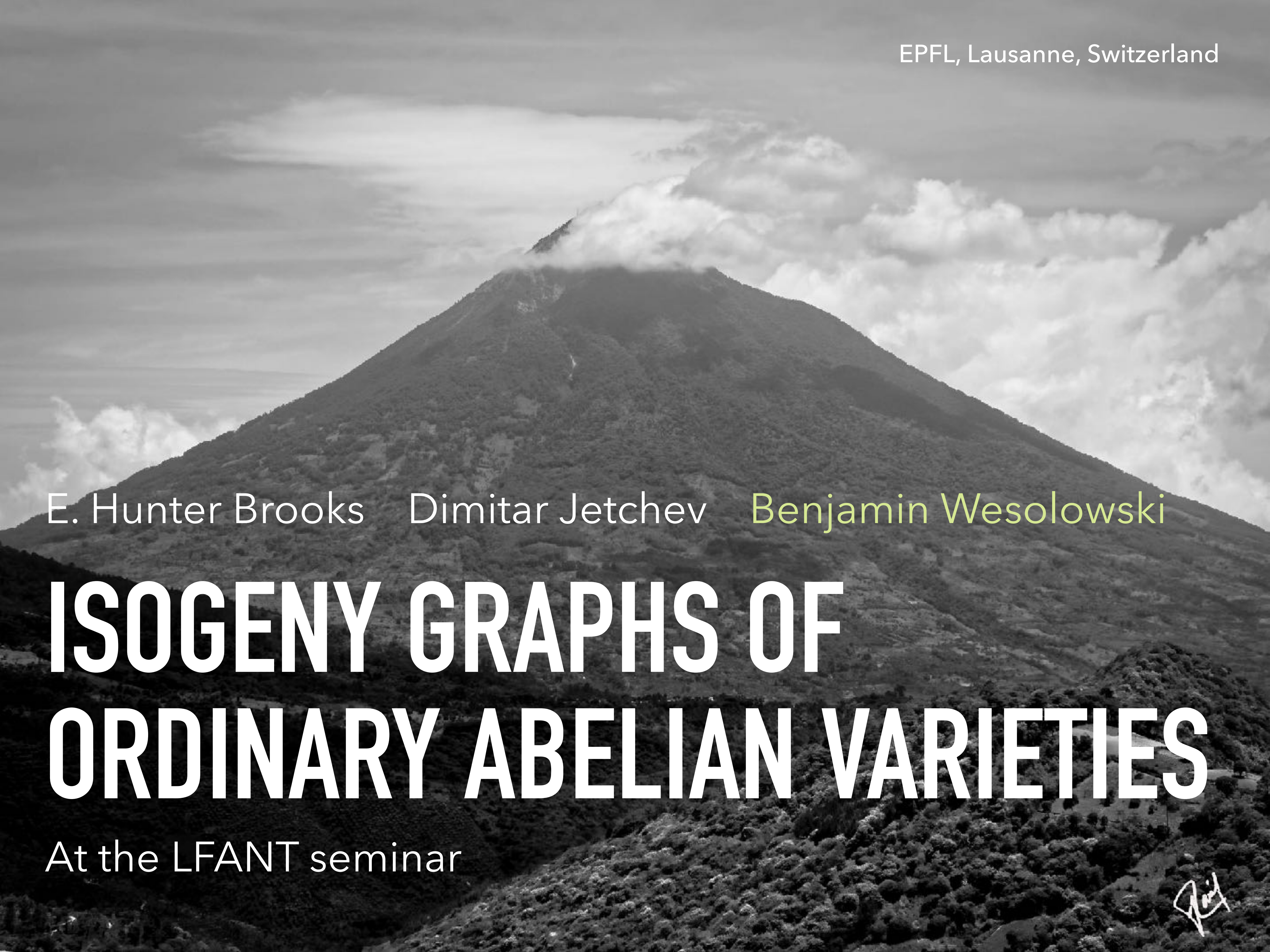
- Last ingredient: we can count the number of vertices on each level using the class number formula.

COUNTING VERTICES AND CONCLUDING

- Last ingredient: we can count the number of vertices on each level using the class number formula.
- Putting all this together, we obtain a precise description of the isogeny graphs.

COUNTING VERTICES AND CONCLUDING

- Last ingredient: we can count the number of vertices on each level using the class number formula.
- Putting all this together, we obtain a precise description of the isogeny graphs.
- They are volcanoes exactly when K has no complex units (no multiplicities on the edges) and $\mathfrak{l}$ is principal (the edges are undirected).



EPFL, Lausanne, Switzerland

E. Hunter Brooks Dimitar Jetchev Benjamin Wesolowski

ISOGENY GRAPHS OF ORDINARY ABELIAN VARIETIES

At the LFANT seminar