ERNEST HUNTER BROOKS

DIMITAR JETCHEV

BENJAMIN WESOLOWSKI

ISOGENY GRAPHS OF ORDINARY ABELIAN VARIETIES

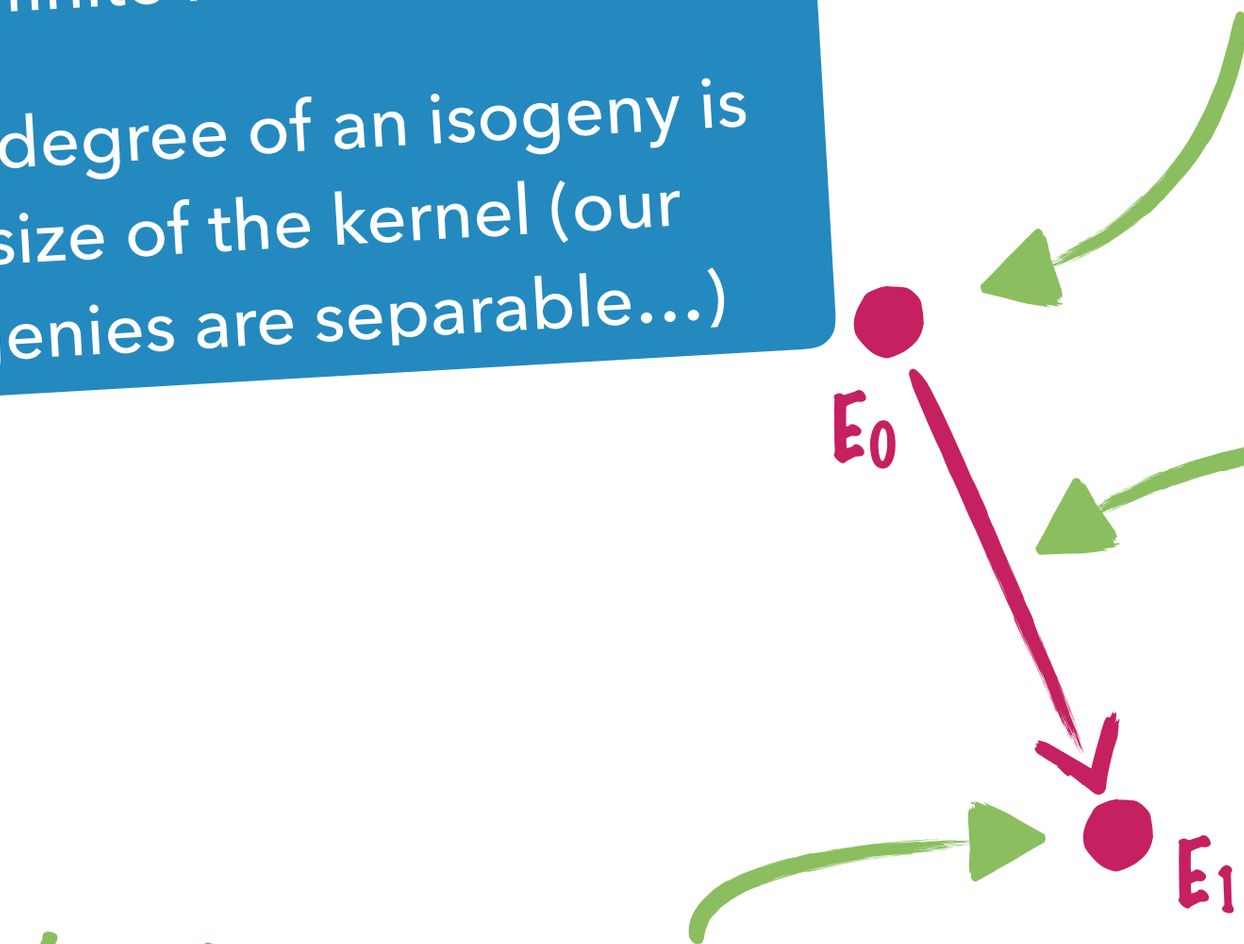
PRESENTED AT ECC 2017, NIJMEGEN, THE NETHERLANDS BY BENJAMIN WESOLOWSKI FROM EPFL, SWITZERLAND

AN INTRODUCTION TO ISOGENY GRAPHS

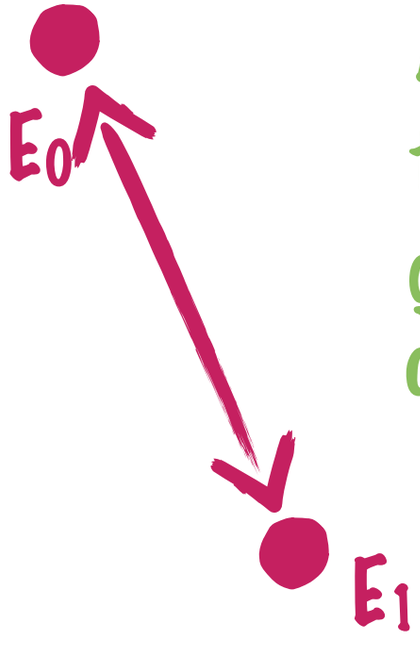
ISOGENY GRAPHS OF ORDINARY ELLIPTIC CURVES

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

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

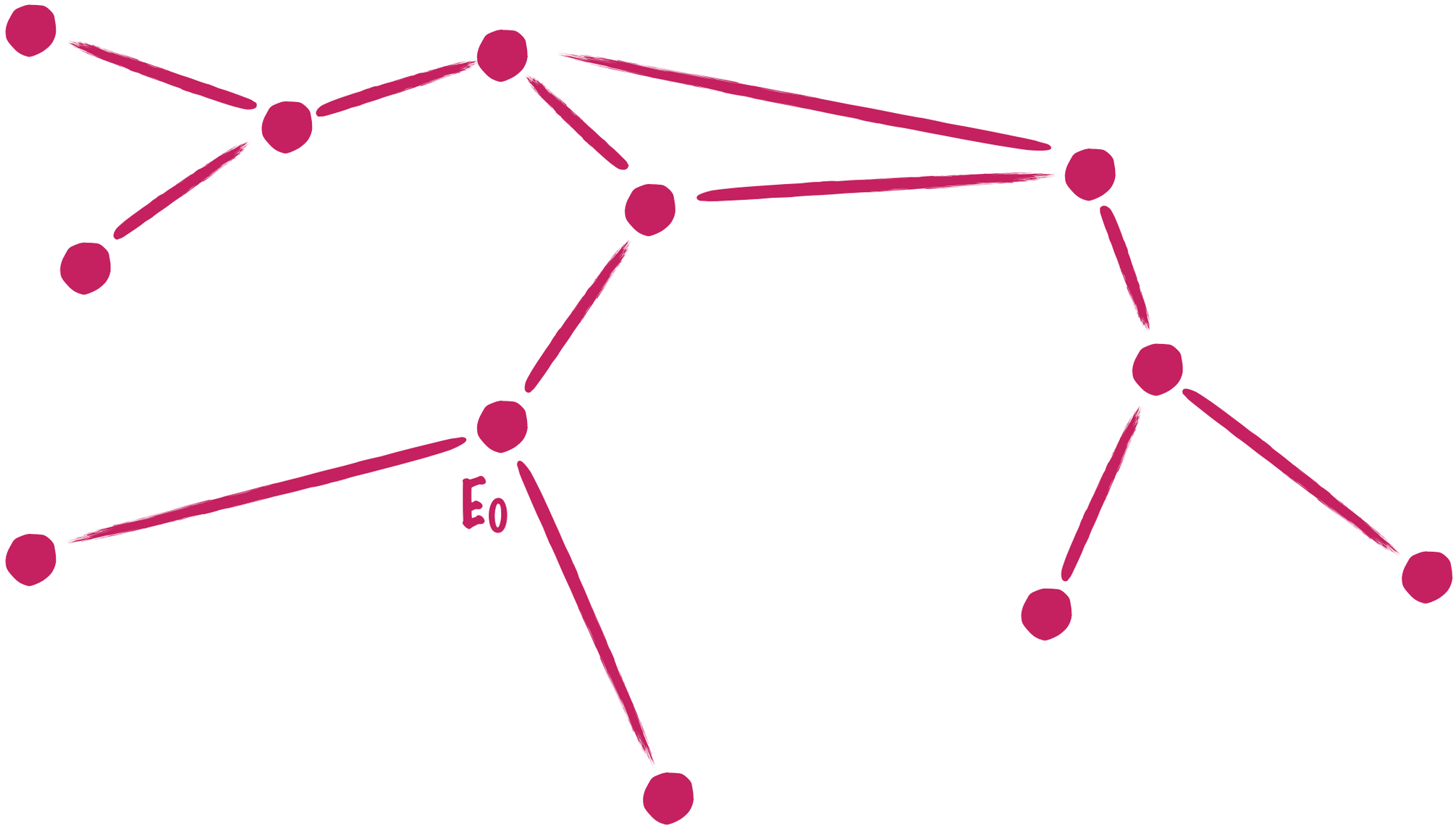
From E_0, there are other isogenies of degree ℓ, going to other curves

Neighbours of E_0 have more neighbours

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

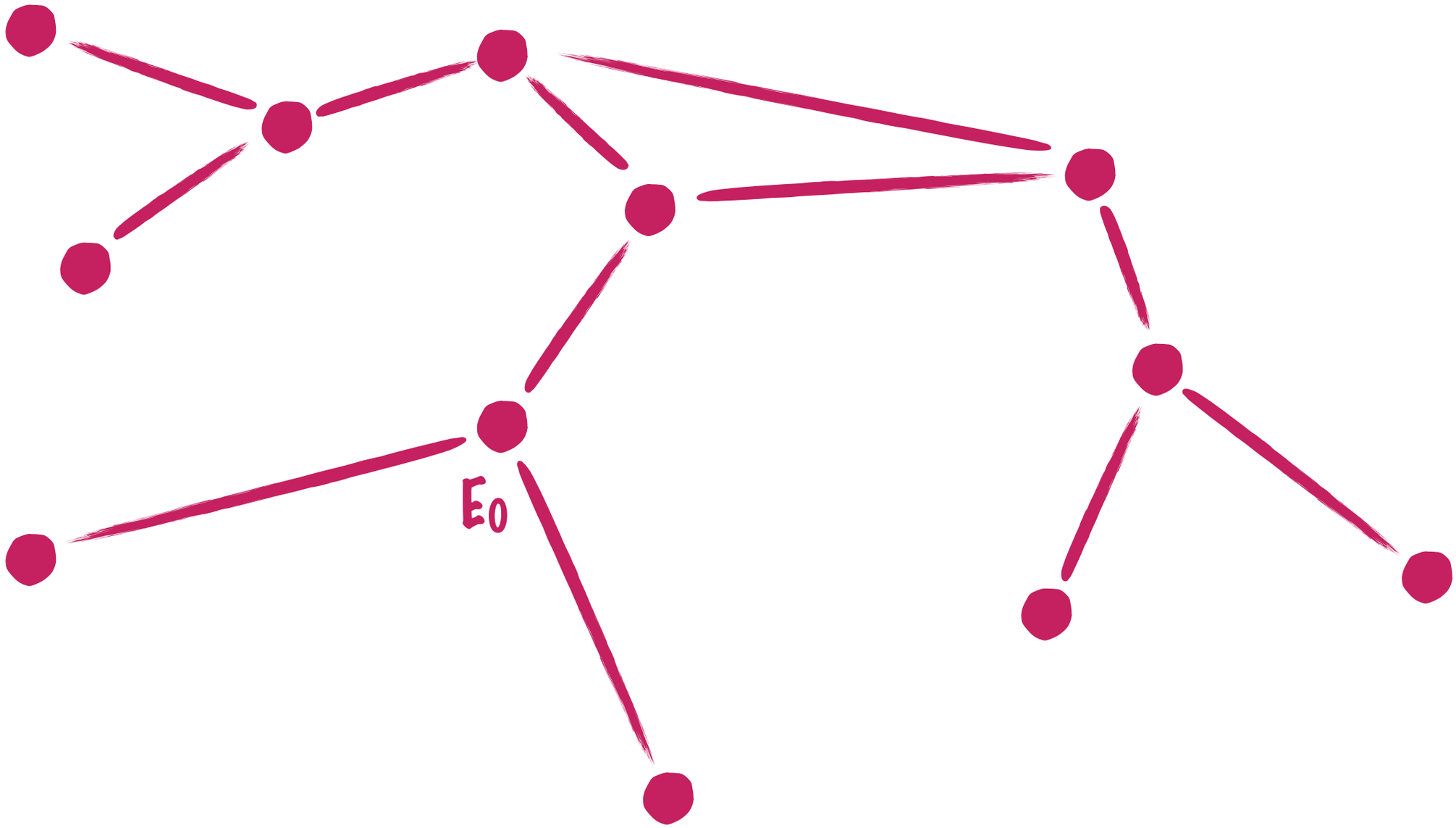
So we represent it by an undirected edge

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

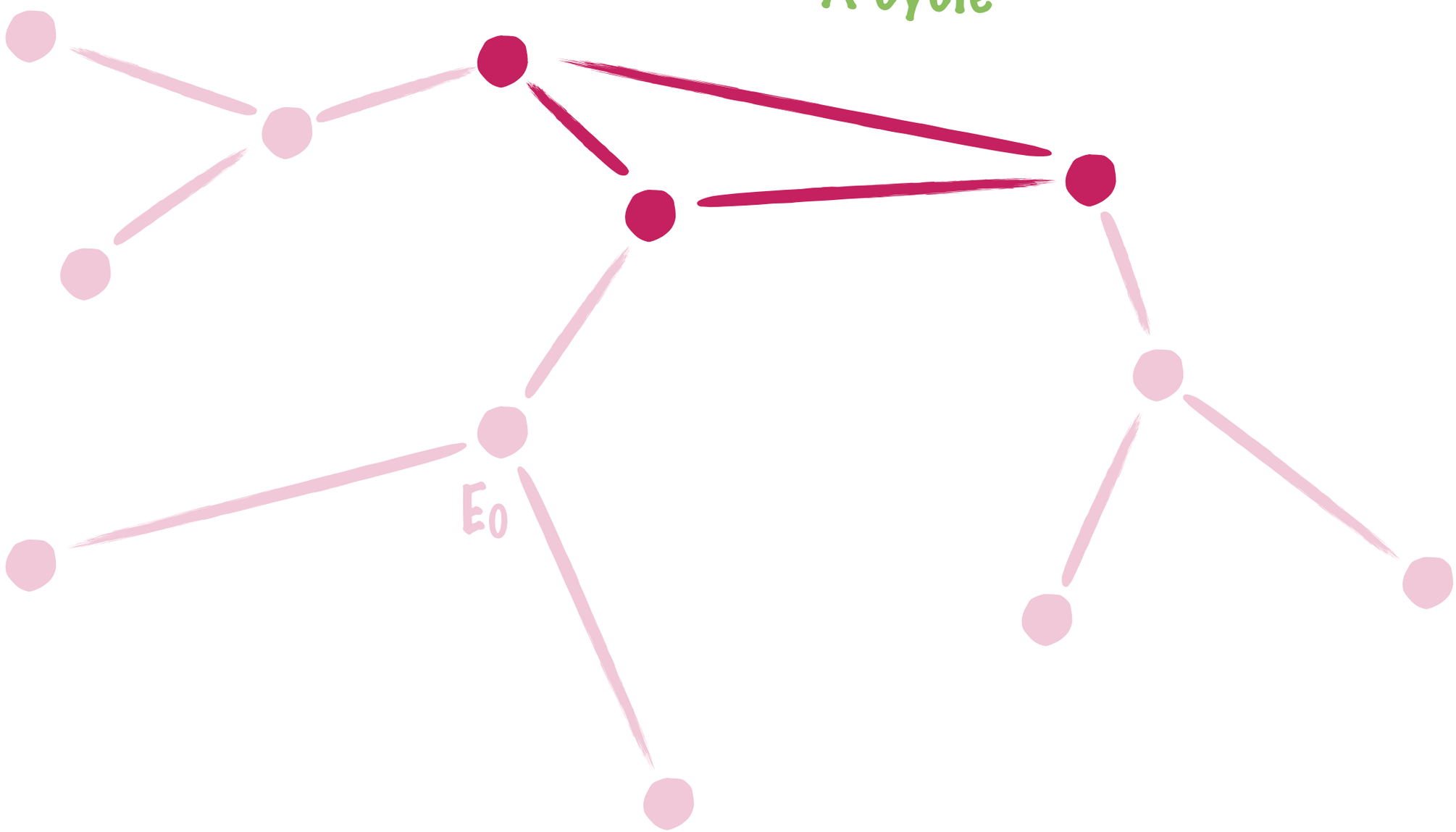
ISOGENY GRAPHS OF ORDINARY ELLIPTIC CURVES



This one is a typical example!

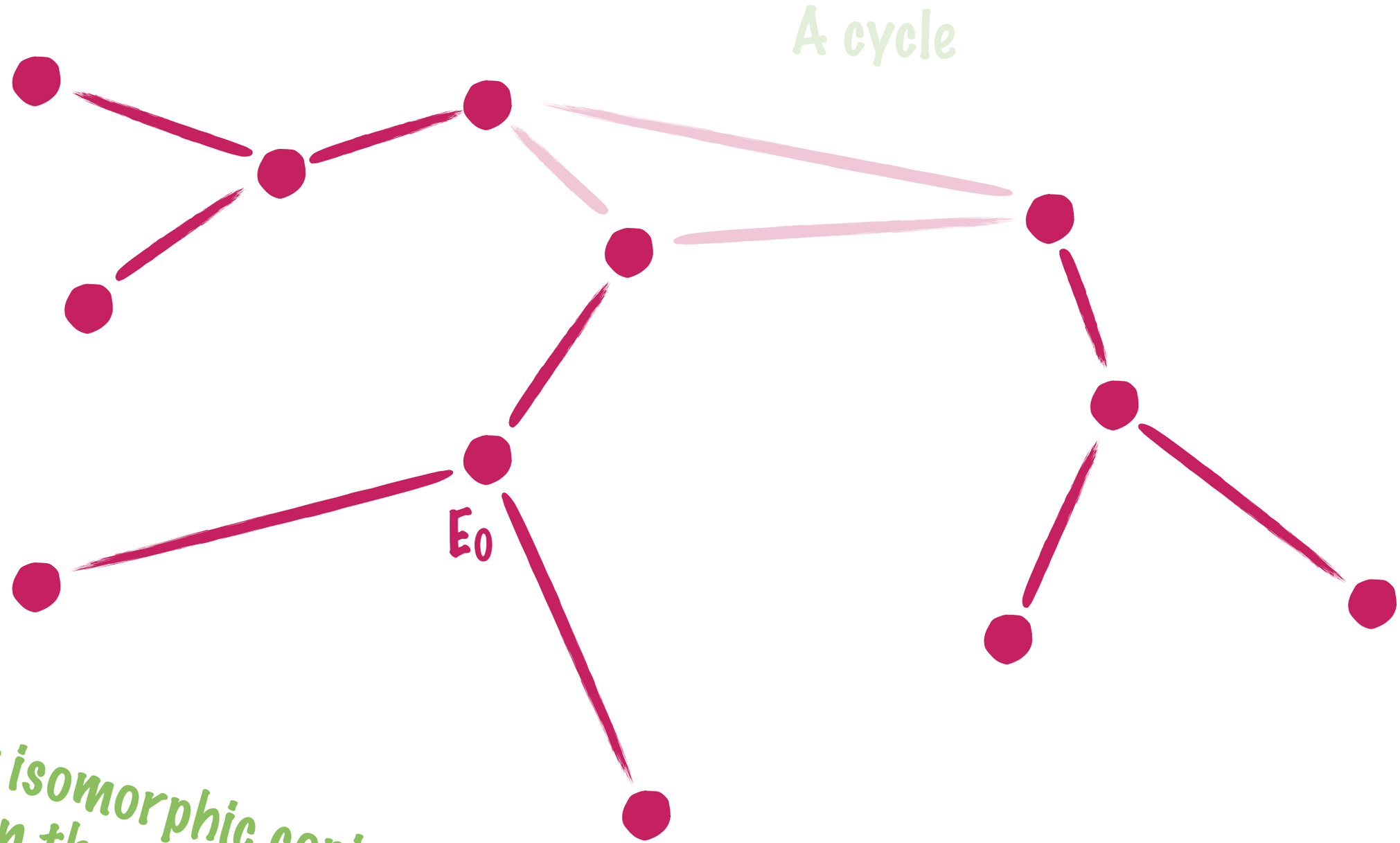
ISOGENY GRAPHS OF ORDINARY ELLIPTIC CURVES

A cycle



This one is a typical example!

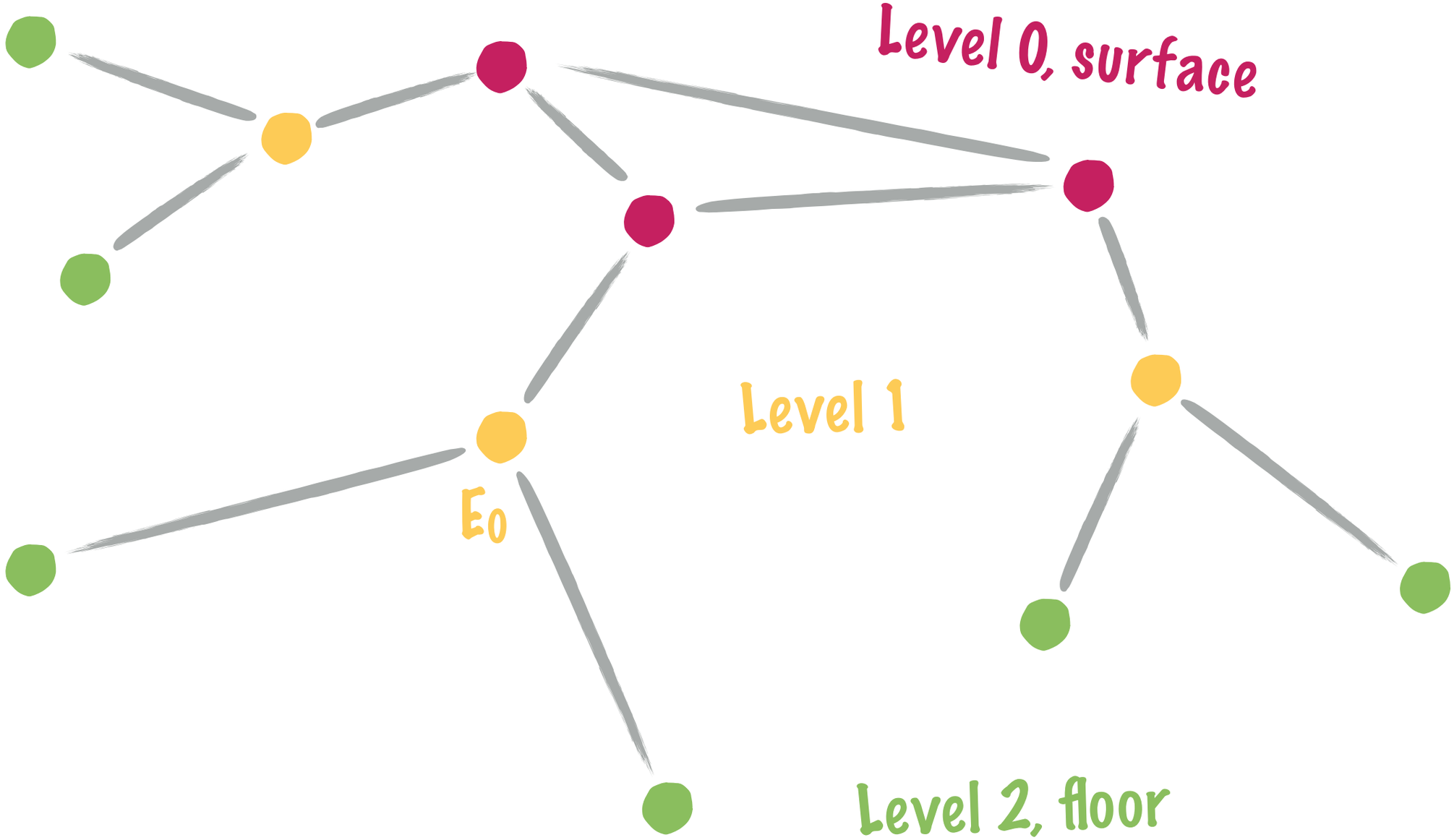
ISOGENY GRAPHS OF ORDINARY ELLIPTIC CURVES

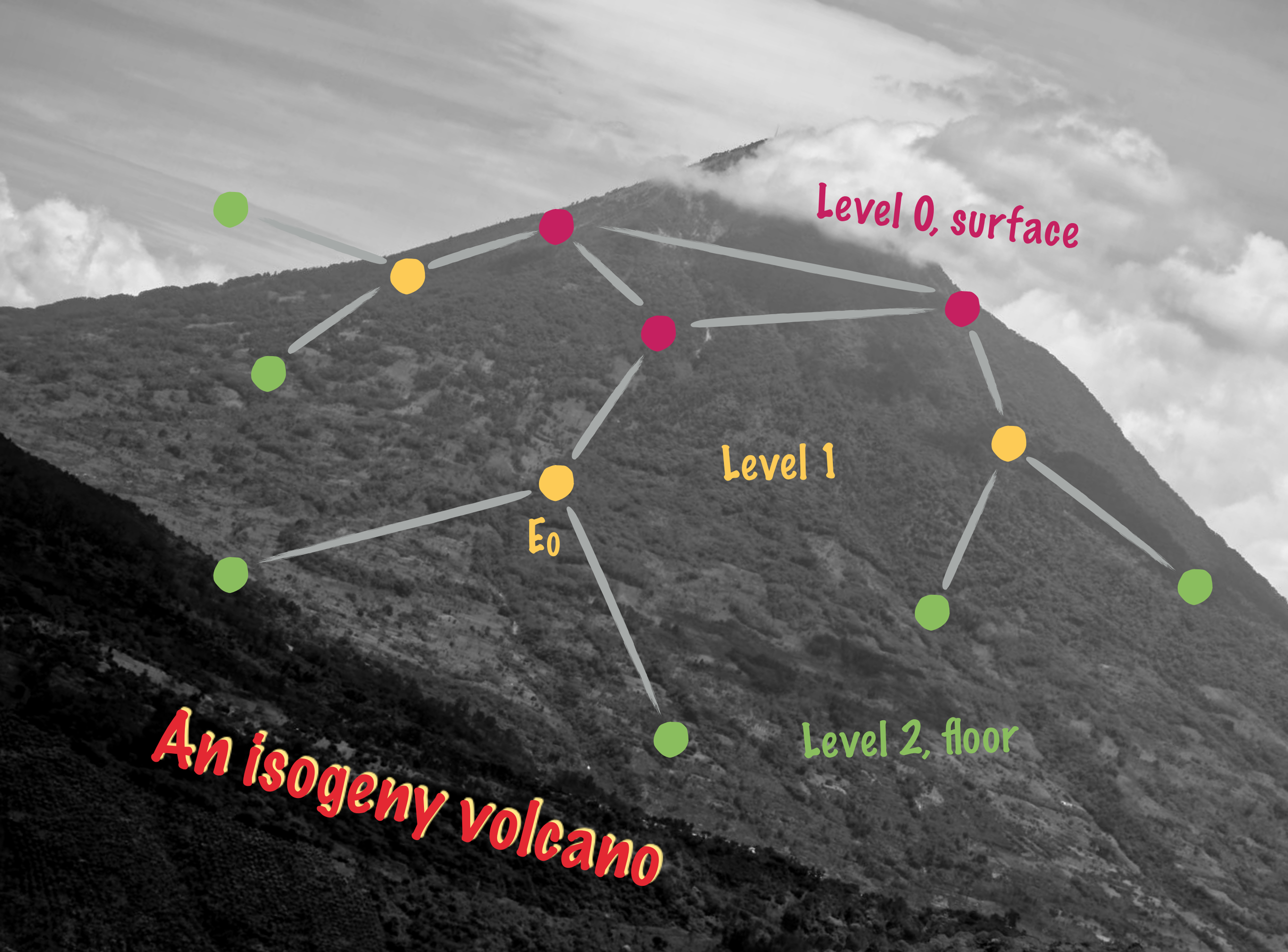


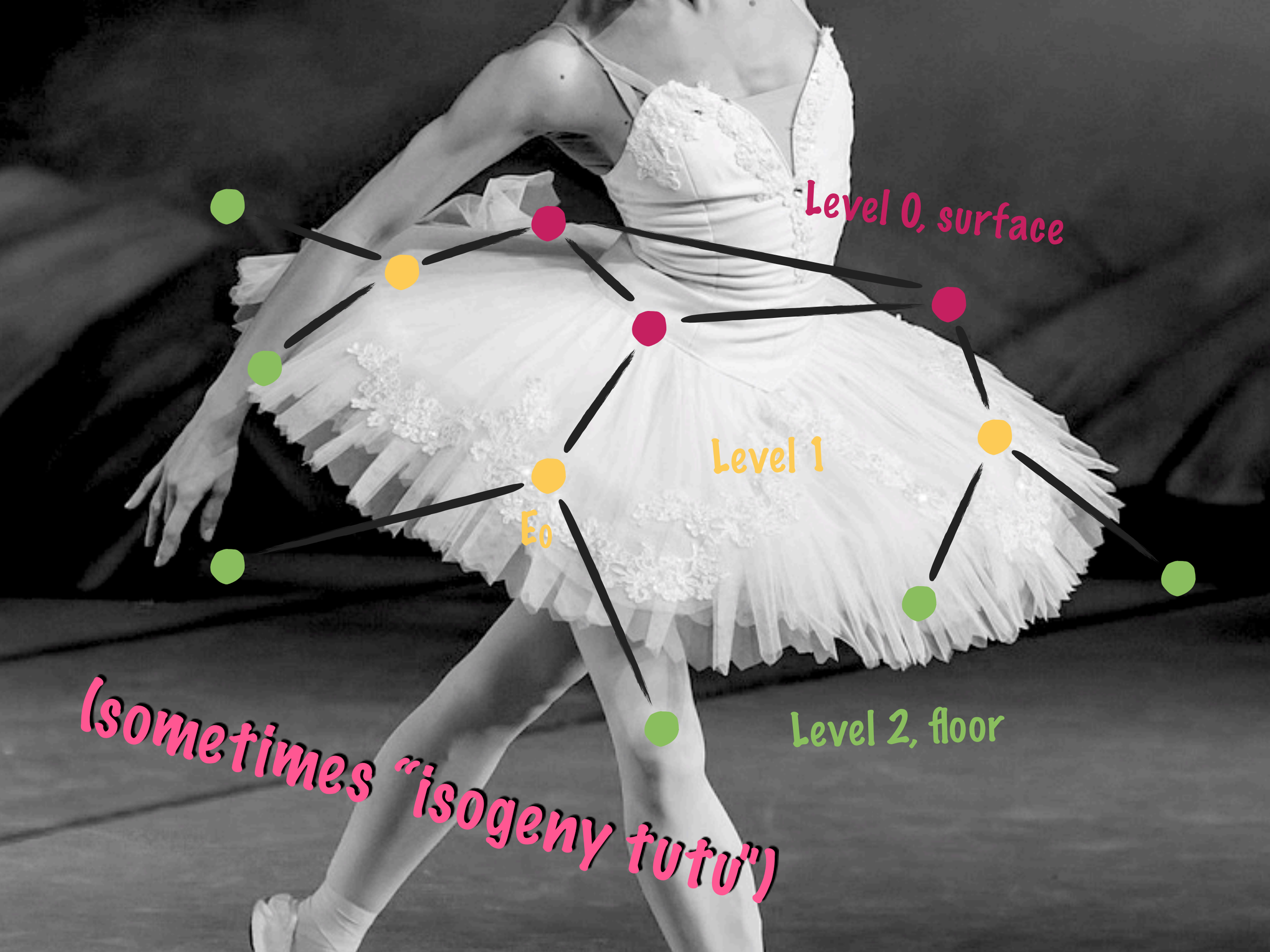
Disjoint isomorphic copies of a tree rooted on the cycle

This one is a typical example!

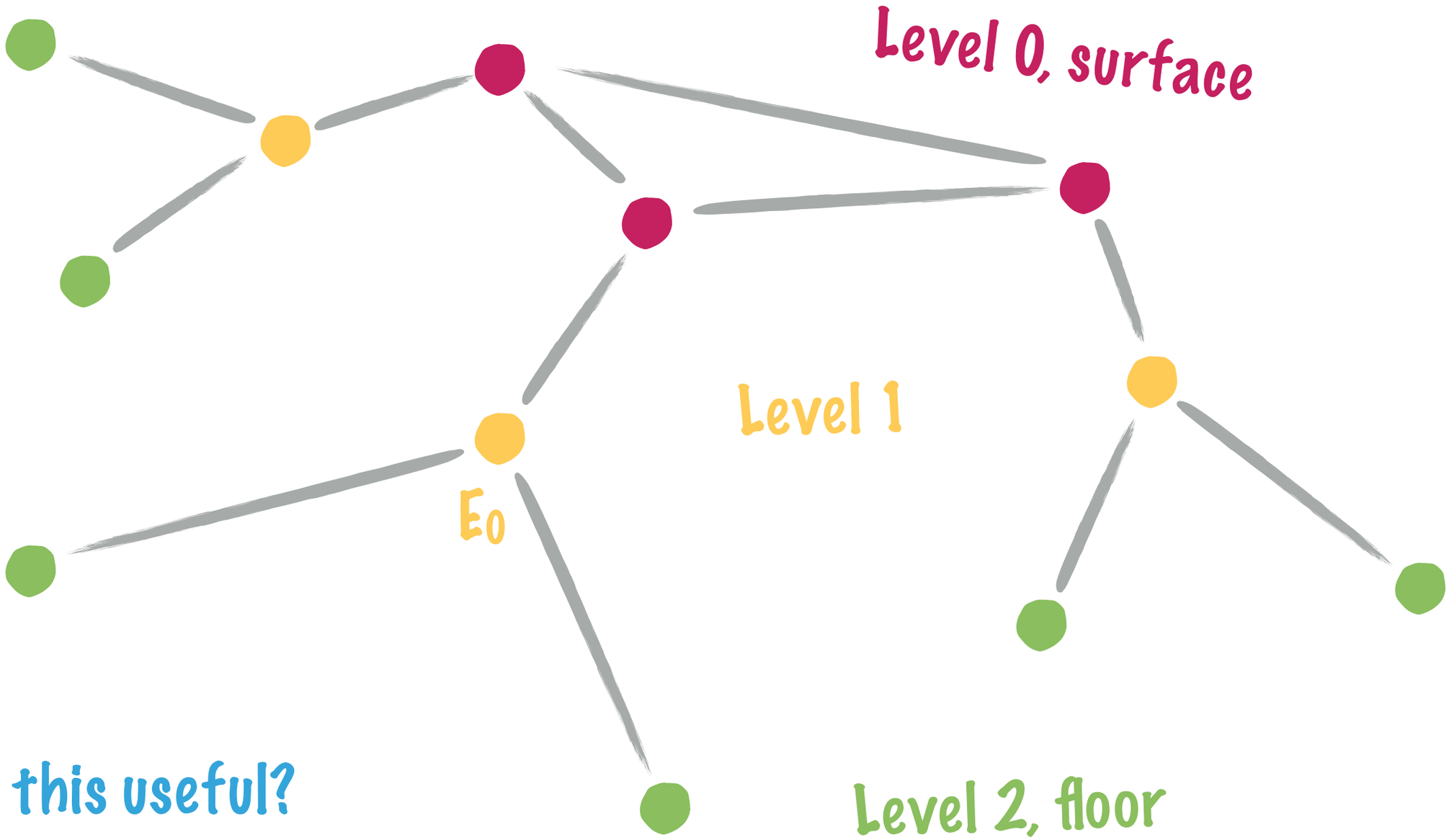
ISOGENY GRAPHS OF ORDINARY ELLIPTIC CURVES




Level 0, surface
Level 1
E0
Level 2, floor
An isogeny volcano


Level 0, surface
Level 1
Eo
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" at 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 and 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…

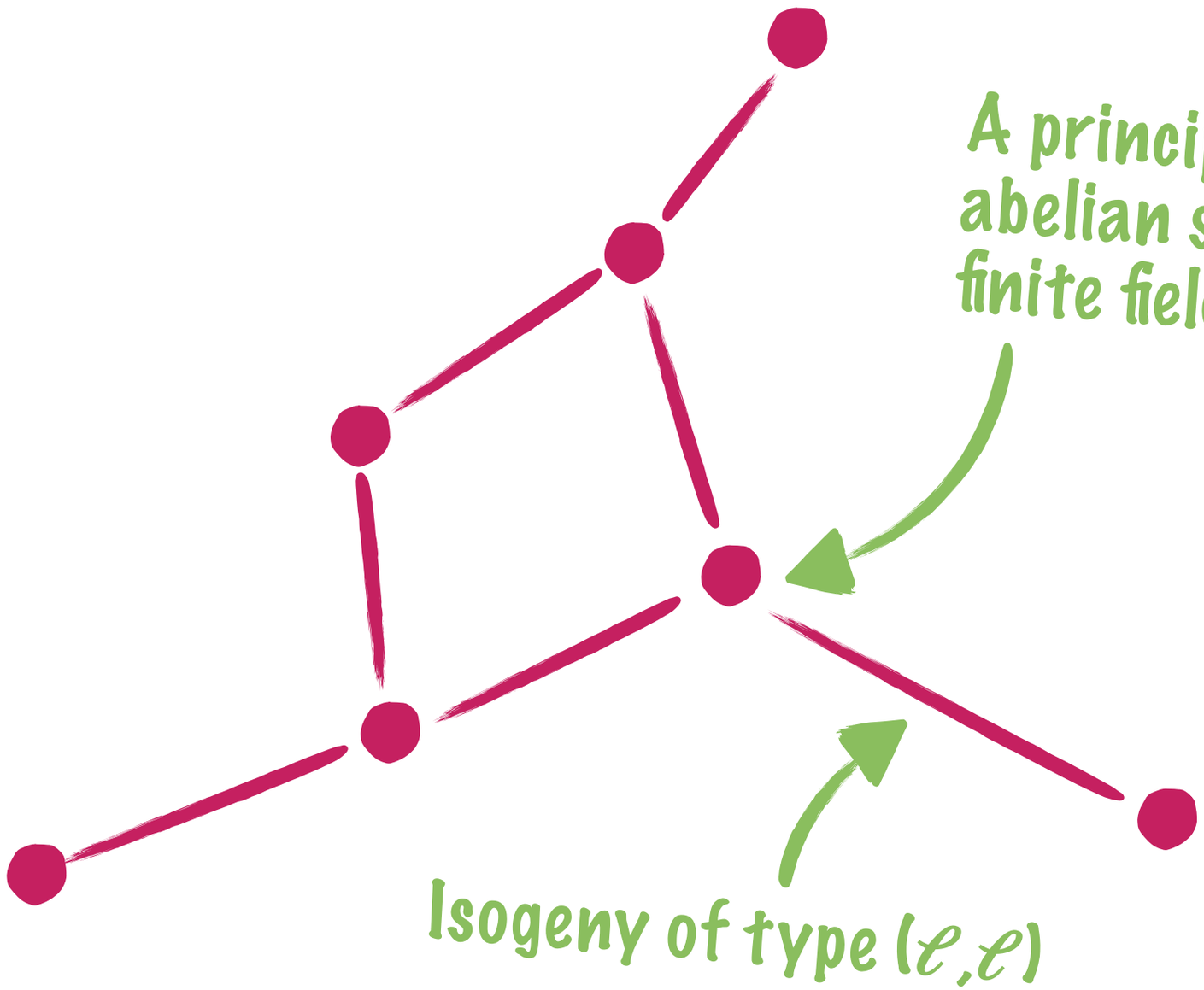
- These applications motivate the search for a generalisation to other abelian varieties…

An abelian variety is a geometric object (curve, surface…) which is also an abelian group (there is an addition law on the points).

Elliptic curves = abelian varieties of dimension 1.

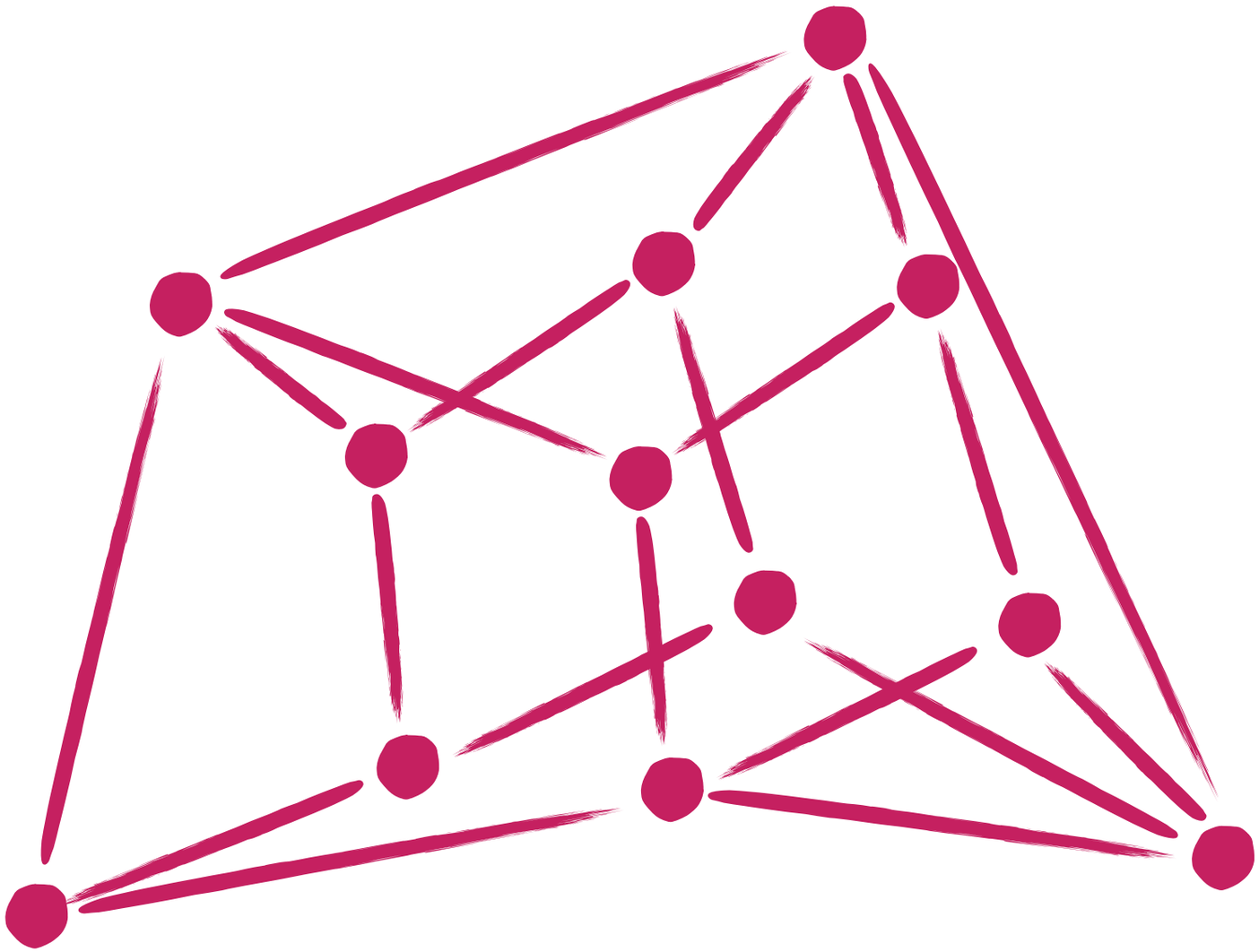
GENERALISING TO ORDINARY ABELIAN VARIETIES…

- 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...

How to study (ℓ,ℓ)-isogeny graphs?

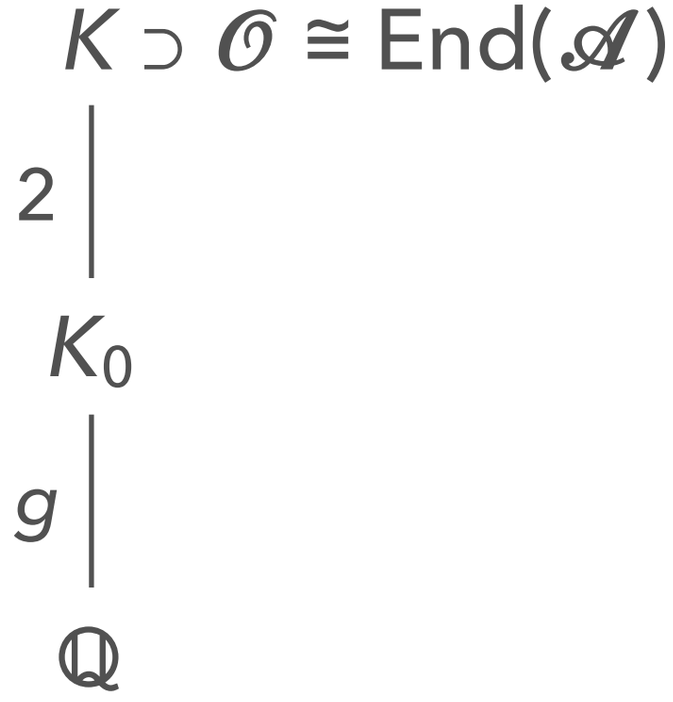
➡ Focus on interesting subgraphs

➡ Decompose (ℓ,ℓ)-isogenies into simpler ones

ENDOMORPHISM RINGS

ENDOMORPHISM RING AND ALGEBRA

- Let $\mathscr{A}$ be an ordinary abelian variety of dimension g over a finite field $F = \mathbb{F}_q$.
- 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 $\mathcal{O}$ of K (i.e., a lattice of dimension $2g$ in K, that is also a subring).



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**.

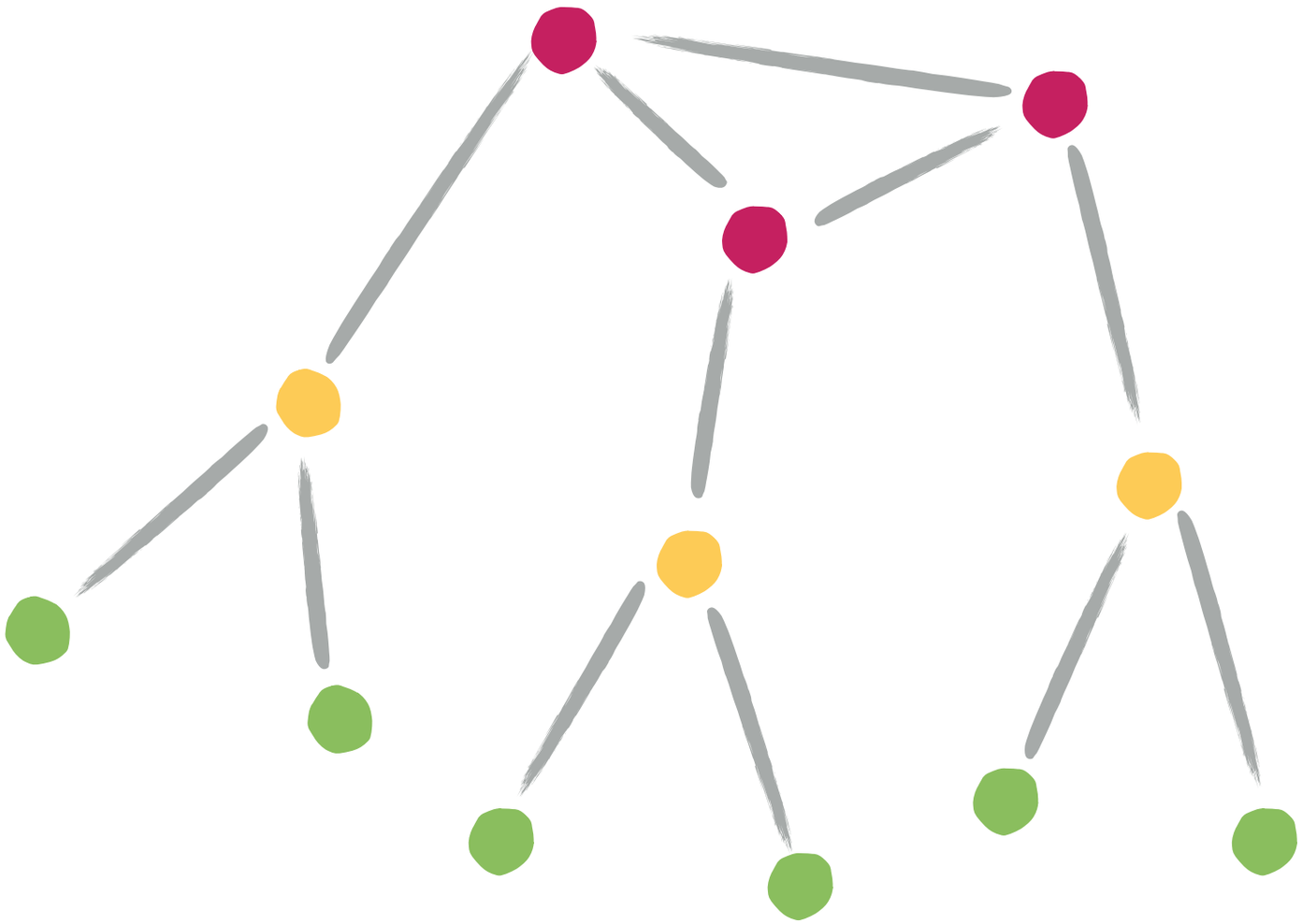
$$K \supset \mathcal{O} \cong \mathrm{End}(E)$$

$$2 \Big|$$

$$K_0 = \mathbb{Q}$$

THE CASE OF ELLIPTIC CURVES

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



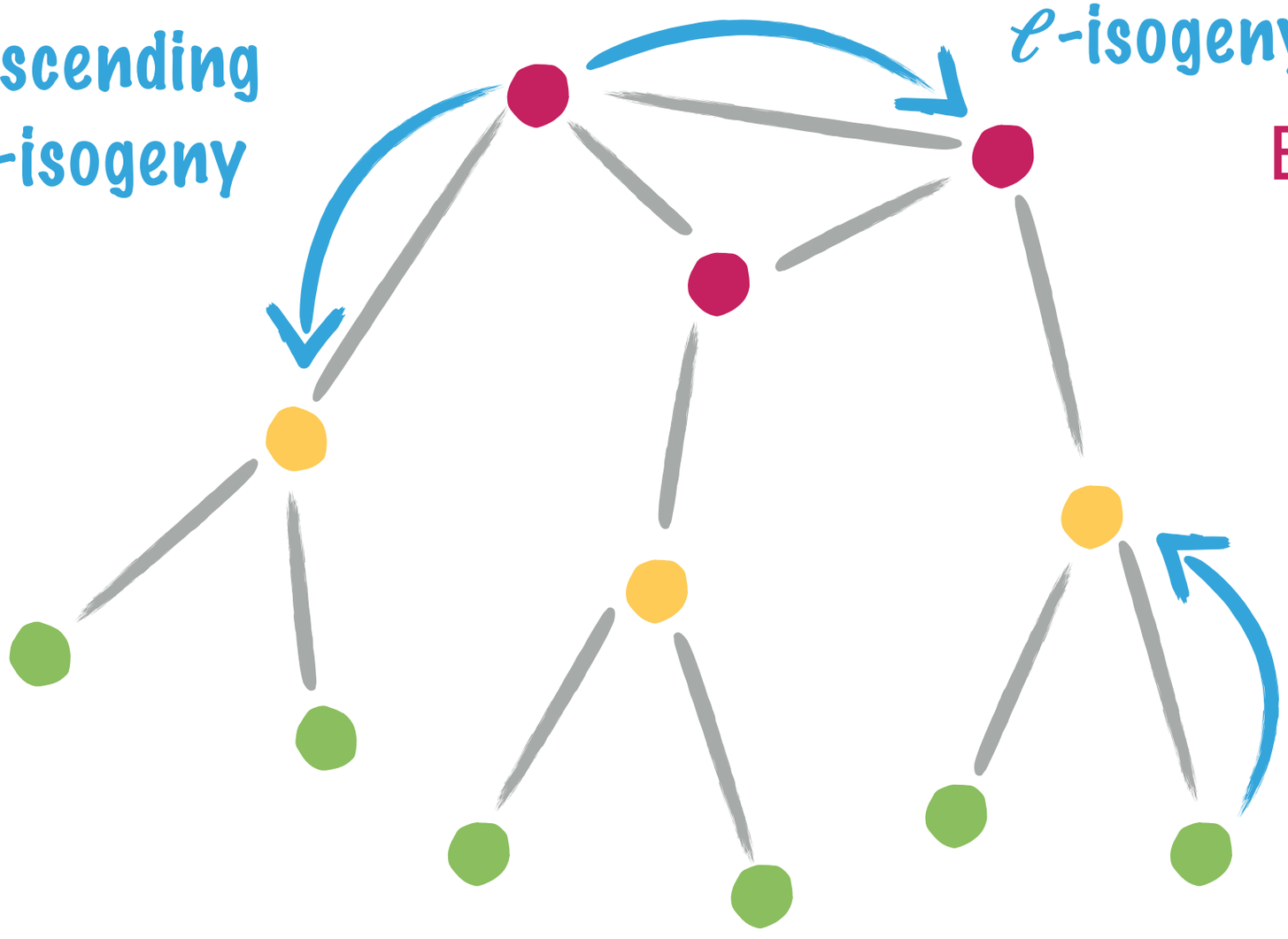
$\mathrm{End} \cong \mathbb{Z} + f\mathcal{O}_K$

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

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

THE CASE OF ELLIPTIC CURVES

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



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

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

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

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 number 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

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?

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

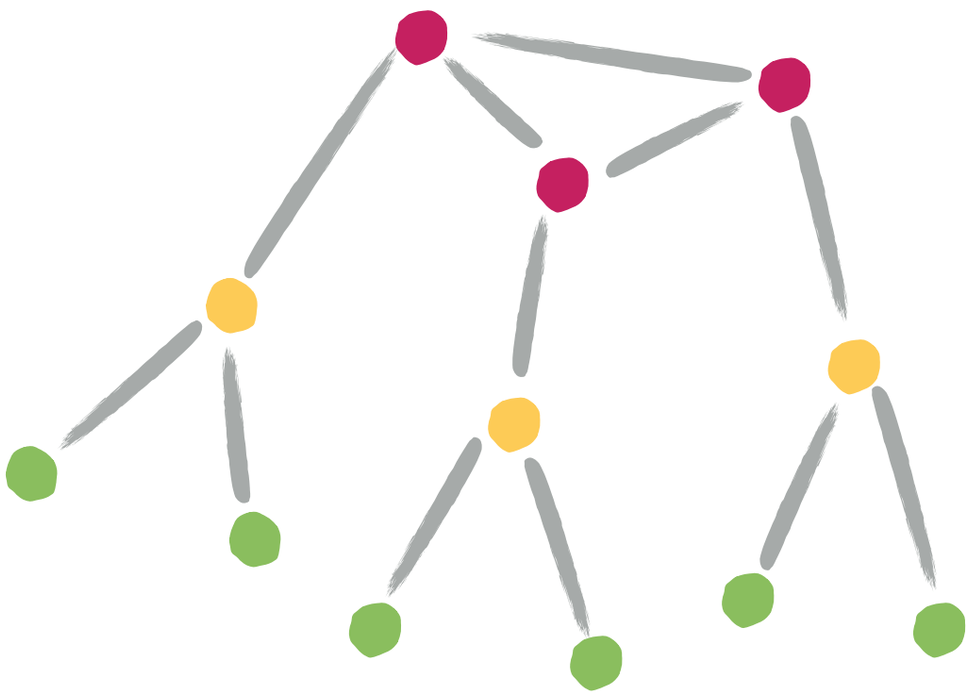
> An $\mathfrak{I}$-isogeny from $\mathcal{A}$ is an isogeny whose kernel is a proper, $\mathcal{O}_{K_0}$-stable subgroup of $\mathcal{A}[\mathfrak{I}]$.

- Coincides with the "$\mathfrak{I}$-isogenies" defined in [Ionica and Thomé, 2014] when g = 2

VOLCANOES AGAIN?

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

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

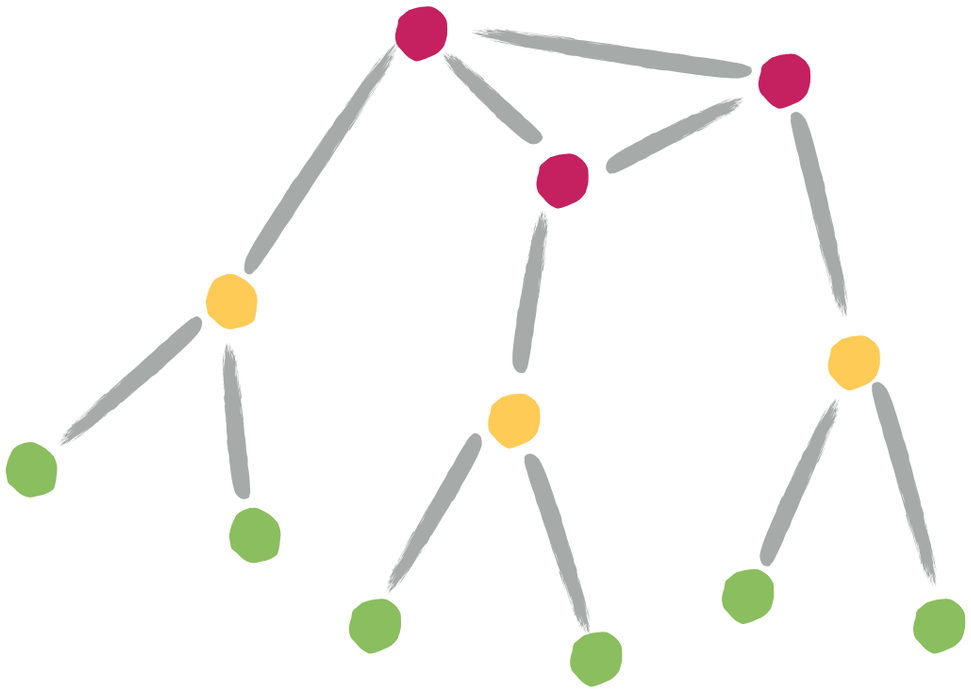


- First observed in some particular case in [Ionica and Thomé, 2014]
- When $\mathfrak{I}$ is generated by a totally positive unit, independently proven in [Martindale, 2017]

VOLCANOES AGAIN?

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

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



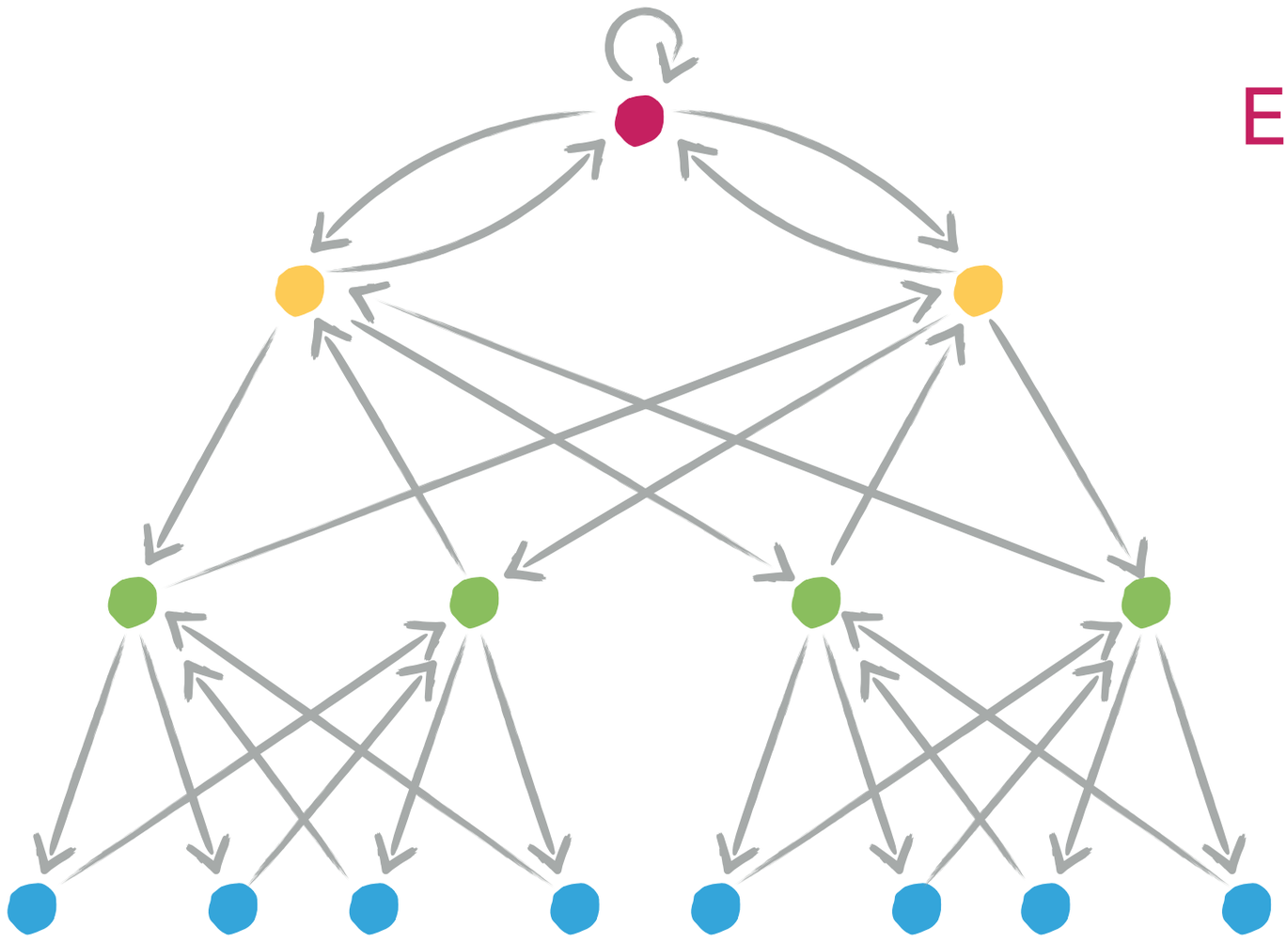
End $\cong \mathcal{O}_{K_0} + \mathfrak{f}\mathcal{O}_K$

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

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

VOLCANOES AGAIN?

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



$$\mathrm{End} \cong \mathcal{O}_{K0} + \mathfrak{f}\mathcal{O}_K$$

$$\mathrm{End} \cong \mathcal{O}_{K0} + \mathfrak{I}\mathfrak{f}\mathcal{O}_K$$

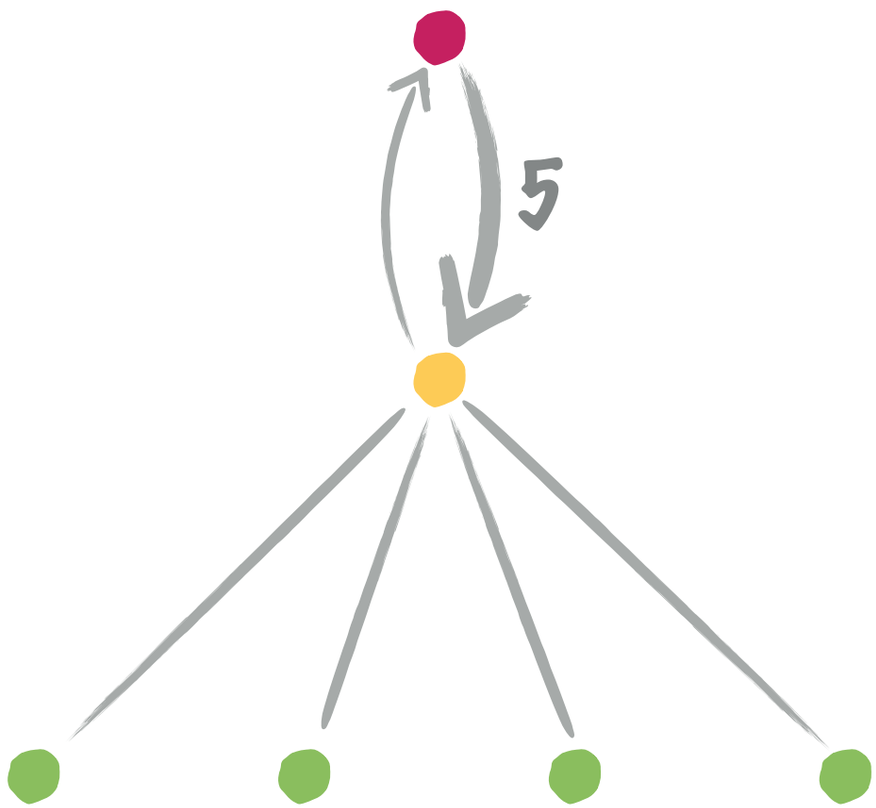
$$\mathrm{End} \cong \mathcal{O}_{K0} + \mathfrak{I}^2\mathfrak{f}\mathcal{O}_K$$

$$\mathrm{End} \cong \mathcal{O}_{K0} + \mathfrak{I}^3\mathfrak{f}\mathcal{O}_K$$

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 $\mathfrak{I} = 2\mathcal{O}_{K_0}$.



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

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

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

MAIN STEPS OF THE

PROOF

COUNTING VERTICES AT EACH LEVEL

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

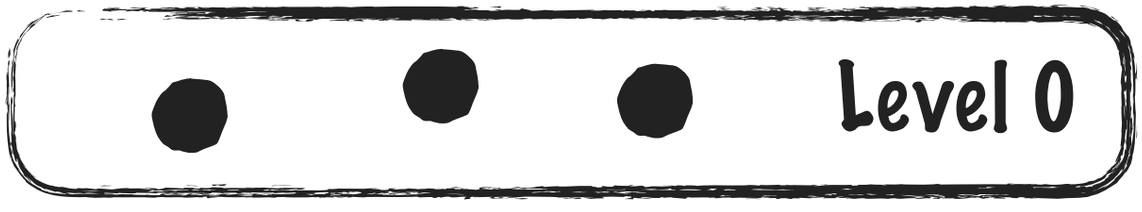
Level 0 — $\mathrm{End} \cong \mathcal{O}_{K0} + \mathfrak{f}\mathcal{O}_K$

Level 1 — $\mathrm{End} \cong \mathcal{O}_{K0} + \mathfrak{l}\mathfrak{f}\mathcal{O}_K$

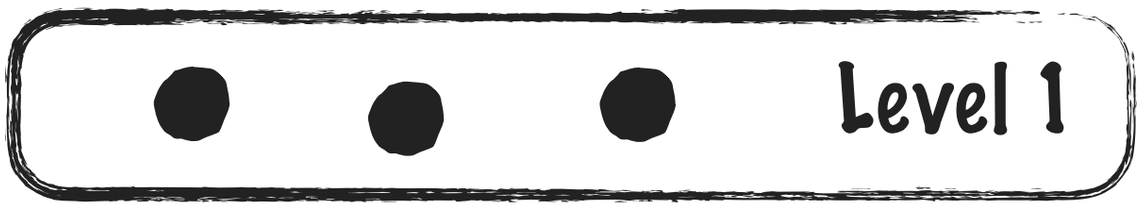
Level 2 — $\mathrm{End} \cong \mathcal{O}_{K0} + \mathfrak{l}^2\mathfrak{f}\mathcal{O}_K$

COUNTING VERTICES AT EACH LEVEL

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



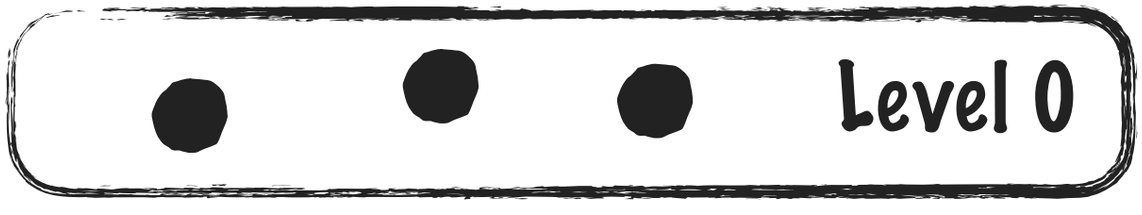
$$\#(\text{level } 0) = \#\mathrm{Cl}(\overbrace{\mathcal{O}_{K_0} + \mathfrak{f}\mathcal{O}_K}^{\text{End}})$$



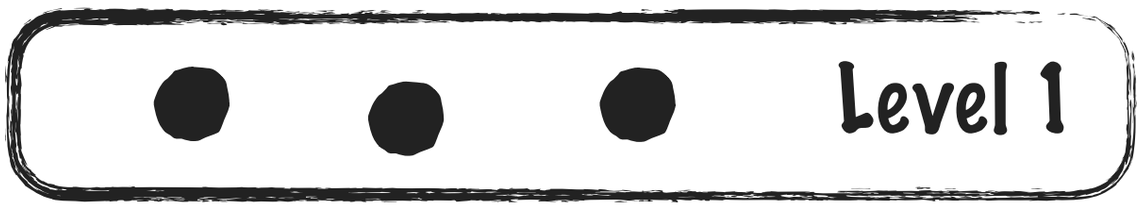
#(level 1) = ? $\#\mathrm{Cl}(\mathcal{O}_{K_0} + \mathfrak{f}\mathcal{O}_K)$

COUNTING VERTICES AT EACH LEVEL

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



$$\#(\text{level } 0) = \#\mathrm{Cl}(\overbrace{\mathcal{O}_{K_0} + \mathfrak{f}\mathcal{O}_K}^{\text{End}})$$

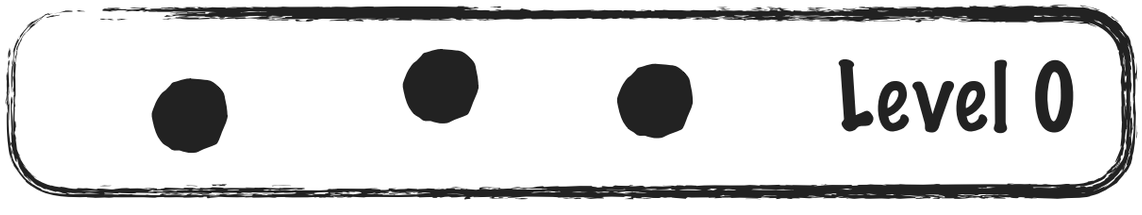


$\#(\text{level } 1) = ?$

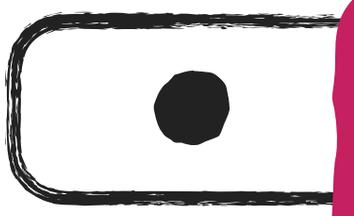
- $\#(\text{level } 1) = (N(\mathfrak{l}) - 1) \cdot \#(\text{level } 0)$ if $\mathfrak{l}$ splits in K
- $\#(\text{level } 1) = N(\mathfrak{l}) \cdot \#(\text{level } 0)$ if $\mathfrak{l}$ ramifies in K
- $\#(\text{level } 1) = (N(\mathfrak{l}) + 1) \cdot \#(\text{level } 0)$ if $\mathfrak{l}$ is inert in K

COUNTING VERTICES AT EACH LEVEL

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



$$\#(\text{level } 0) = \#\mathrm{Cl}(\overbrace{\mathcal{O}_{K_0} + \mathfrak{f}\mathcal{O}_K}^{\text{End}})$$

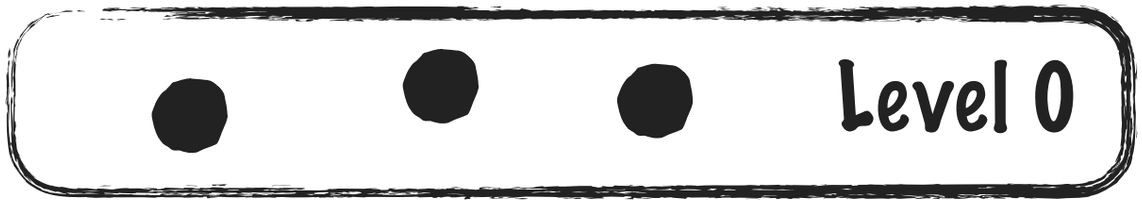


Warning: these are simplified formulas (need extra assumptions on the units of $\mathcal{O}_K$)

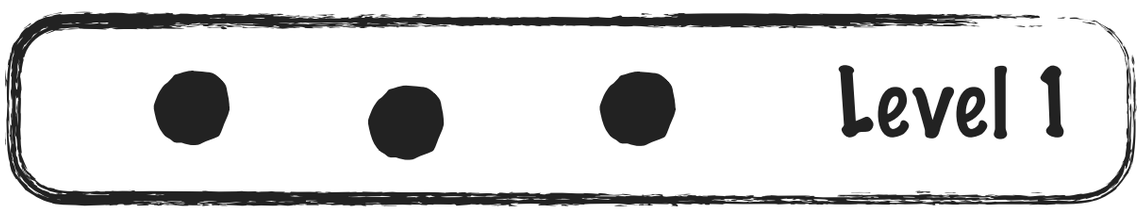
- $\#(\text{level } 1) = (\mathrm{N}(\mathfrak{I}) - 1) \cdot \#(\text{level } 0)$ if $\mathfrak{I}$ splits in K
- $\#(\text{level } 1) = \mathrm{N}(\mathfrak{I}) \cdot \#(\text{level } 0)$ if $\mathfrak{I}$ ramifies in K
- $\#(\text{level } 1) = (\mathrm{N}(\mathfrak{I}) + 1) \cdot \#(\text{level } 0)$ if $\mathfrak{I}$ is inert in K

COUNTING VERTICES AT EACH LEVEL

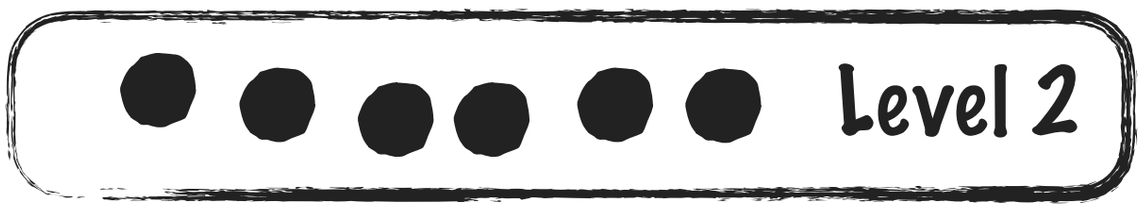
- First ingredient: we can count the number of vertices on each level using the class number formula.



$$\#(\text{level } 0) = \#\mathrm{Cl}(\mathcal{O}_{K_0} + \mathfrak{f}\mathcal{O}_K)$$



$$\#(\text{level } 1) = \begin{cases} (N(\mathfrak{l}) - 1) \cdot \#(\text{level } 0) \\ N(\mathfrak{l}) \cdot \#(\text{level } 0) \\ (N(\mathfrak{l}) + 1) \cdot \#(\text{level } 0) \end{cases}$$

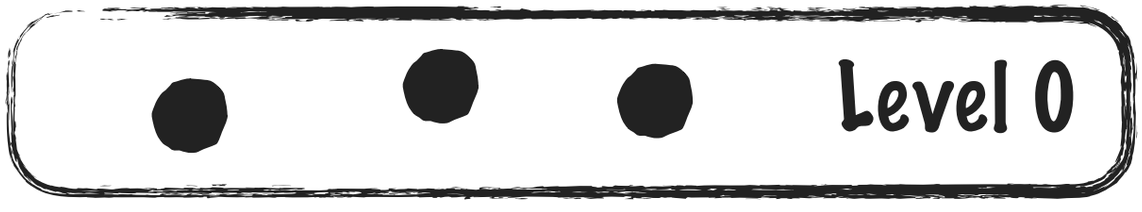


$$\#(\text{level } 2) = N(\mathfrak{l}) \cdot \#(\text{level } 1)$$

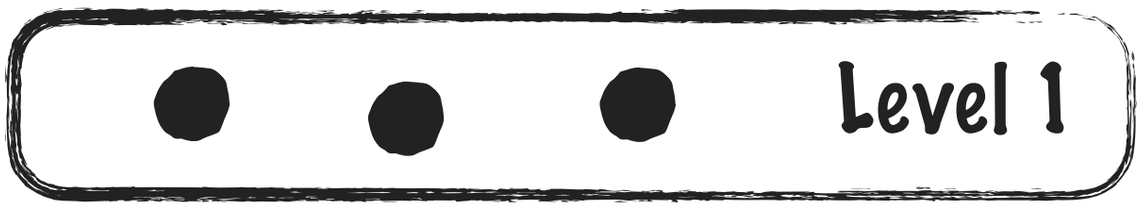
$$\#(\text{level } i + 1) = N(\mathfrak{l}) \cdot \#(\text{level } i) \quad \text{for } i \geq 1$$

COUNTING VERTICES AT EACH LEVEL

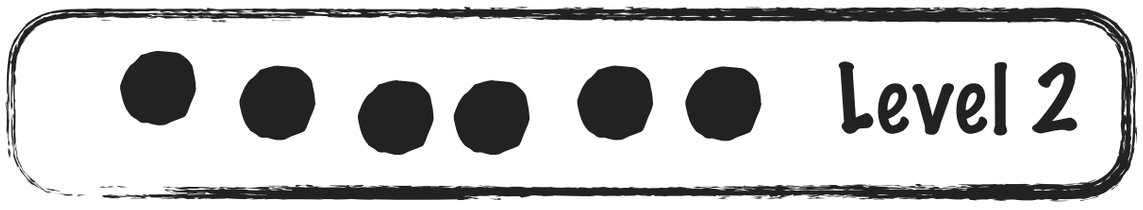
- First ingredient: we can count the number of vertices on each level using the class number formula.



#(level 0) = 3



#(level 2) = N(I) · #(level 1) = 6

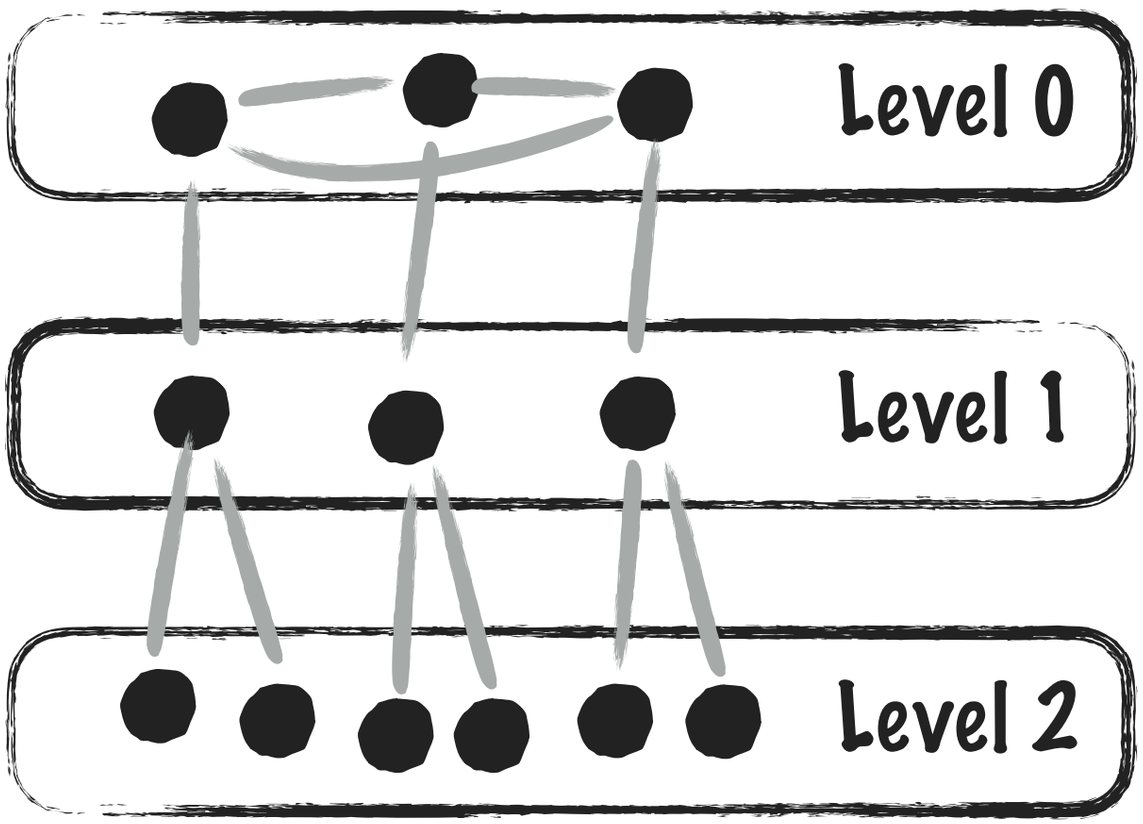


#(level 1) = (N(I) - 1) · #(level 0) = 3

in this example, #(level 0) = 3, I splits, and N(I) = 2

COUNTING VERTICES AT EACH LEVEL

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

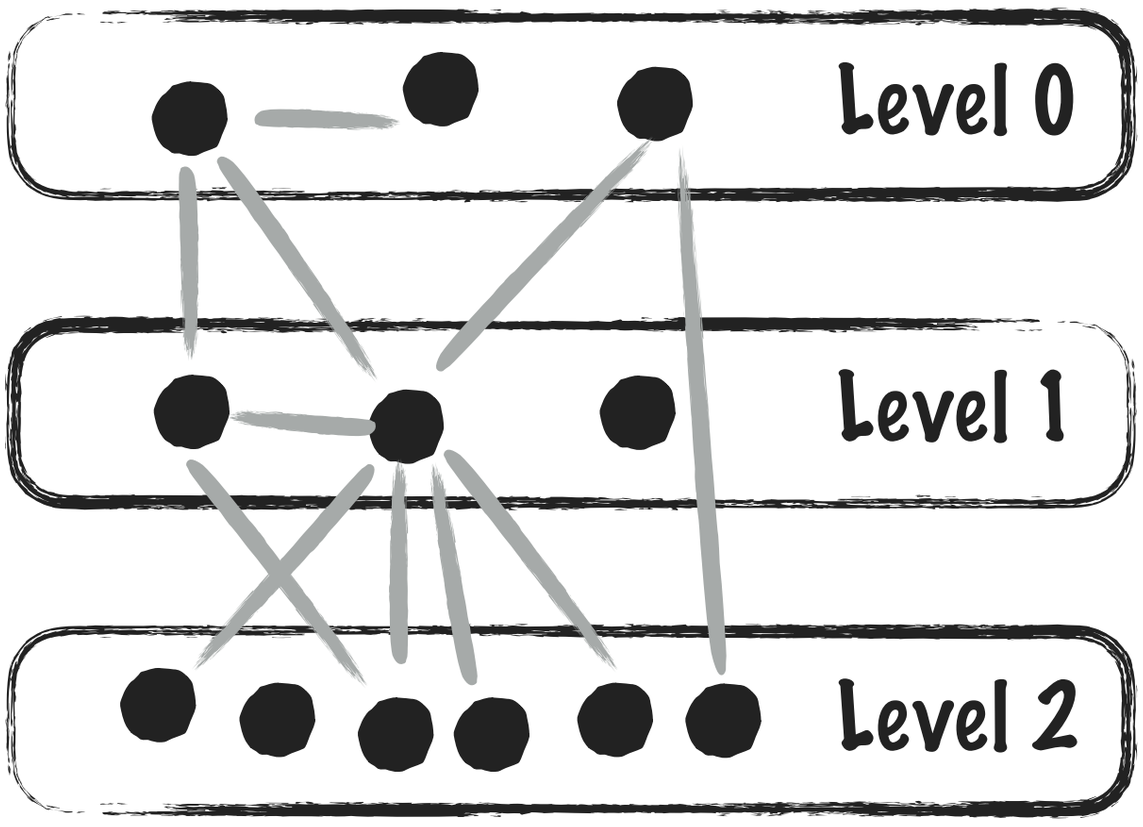


It could lead to a volcano...

in this example, #(level 0) = 3, I splits, and N(I) = 2

COUNTING VERTICES AT EACH LEVEL

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



It could lead to a volcano...

or to all sorts of ugly graphs...

We need to look at the edge structure

in this example, #(level 0) = 3, I splits, and N(I) = 2

COUNTING OUTGOING EDGES

- A simple fact: let $\mathcal{A}$ be a variety on the $\mathfrak{l}$-isogeny graph. There is a total of N($\mathfrak{l}$)+1 outgoing $\mathfrak{l}$-isogenies from $\mathcal{A}$.
- Why ? Recall the definition:

> An $\mathfrak{l}$-isogeny from $\mathcal{A}$ is an isogeny whose kernel is a proper, $\mathcal{O}_{K_0}$-stable subgroup of $\mathcal{A}[\mathfrak{l}]$.

- $\mathcal{A}[\mathfrak{l}]$ is an $\mathcal{O}_{K_0}/\mathfrak{l}$-vector space of dimension 2.
- It has N($\mathfrak{l}$)+1 many vector subspaces of dimension 1.
- So there are N($\mathfrak{l}$)+1 proper $\mathcal{O}_{K_0}$-stable subgroups of $\mathcal{A}[\mathfrak{l}]$.

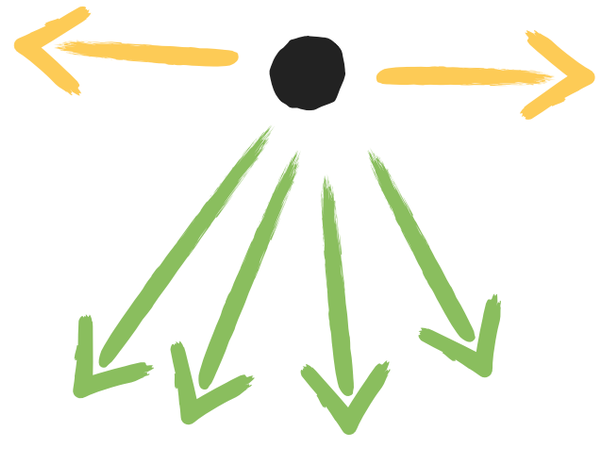
COUNTING OUTGOING EDGES

- Among the N($\mathfrak{l}$)+1 outgoing $\mathfrak{l}$-isogenies from $\mathscr{A}$, how many are horizontal? ascending? descending?
- This is the core of the proof. The idea is to build a correspondence between
  - $\mathfrak{l}$-isogenies from $\mathscr{A}$, and
  - certain sub-lattices of the Tate module of $\mathscr{A}$

  and use the action of the field K on these lattices.
- No details in this presentation, just the results:

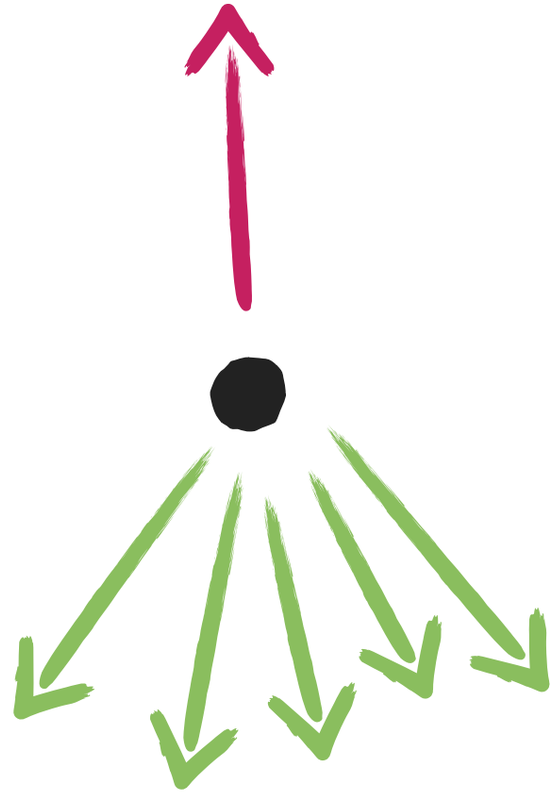
COUNTING OUTGOING EDGES

- Among the N($\mathfrak{l}$)+1 outgoing $\mathfrak{l}$-isogenies from $\mathscr{A}$, how many are horizontal? ascending? descending?
- If $\mathscr{A}$ is at the surface (level 0):
  - No ascending $\mathfrak{l}$-isogeny (obviously),
  - No horizontal $\mathfrak{l}$-isogeny *if* $\mathfrak{l}$ *is inert in* $\mathcal{O}$ = End($\mathscr{A}$),
  - One horizontal $\mathfrak{l}$-isogeny *if* $\mathfrak{l}$ *ramifies*,
  - Two horizontal $\mathfrak{l}$-isogenies *if* $\mathfrak{l}$ *splits*,
  - The other ones are descending



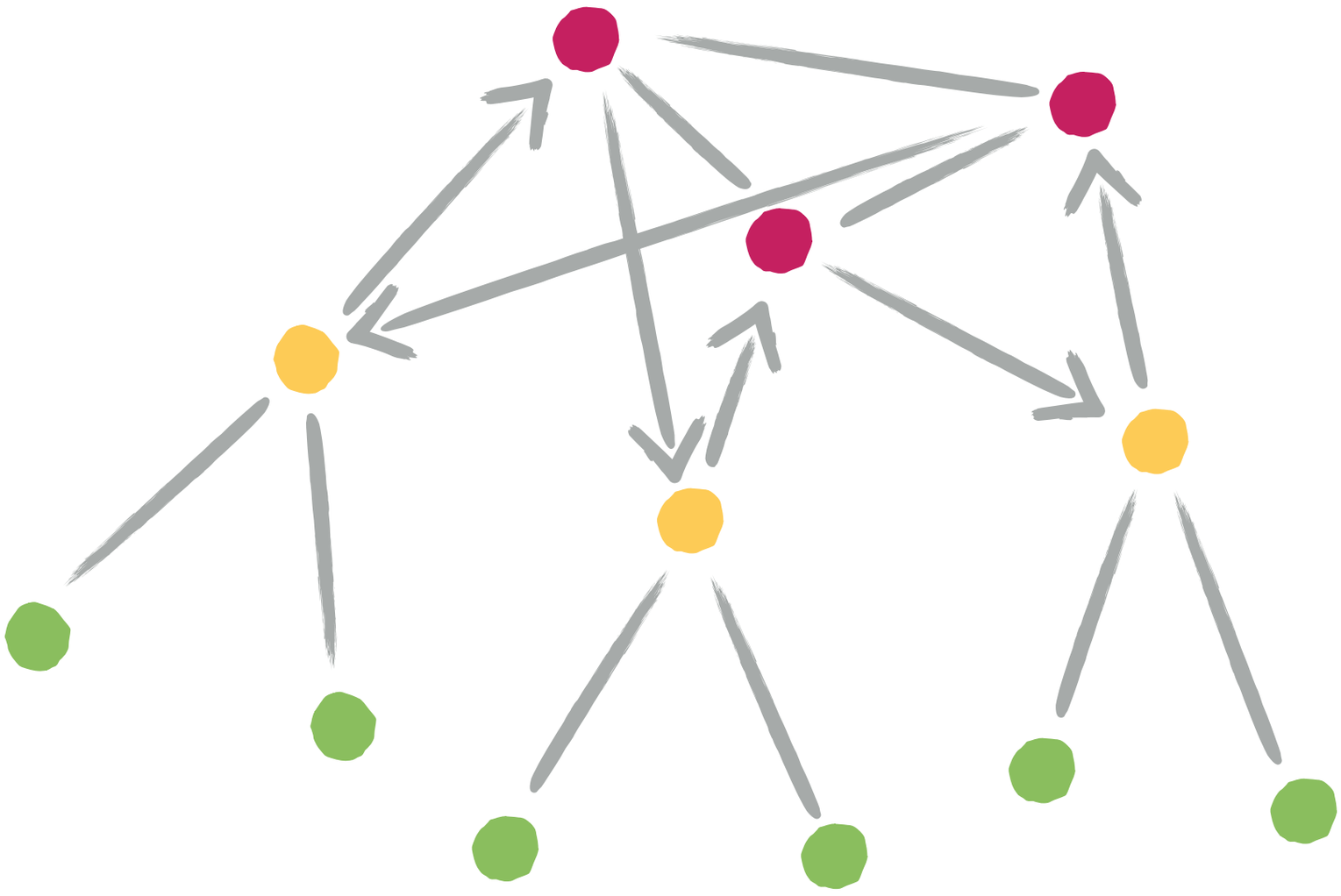
COUNTING OUTGOING EDGES

- Among the N($\mathfrak{l}$)+1 outgoing $\mathfrak{l}$-isogenies from $\mathscr{A}$, how many are horizontal? ascending? descending?
- If $\mathscr{A}$ is **not** at the surface:
  - One ascending $\mathfrak{l}$-isogeny,
  - No horizontal $\mathfrak{l}$-isogeny,
  - The other are descending (N($\mathfrak{l}$) many).



VOLCANOES ALREADY?

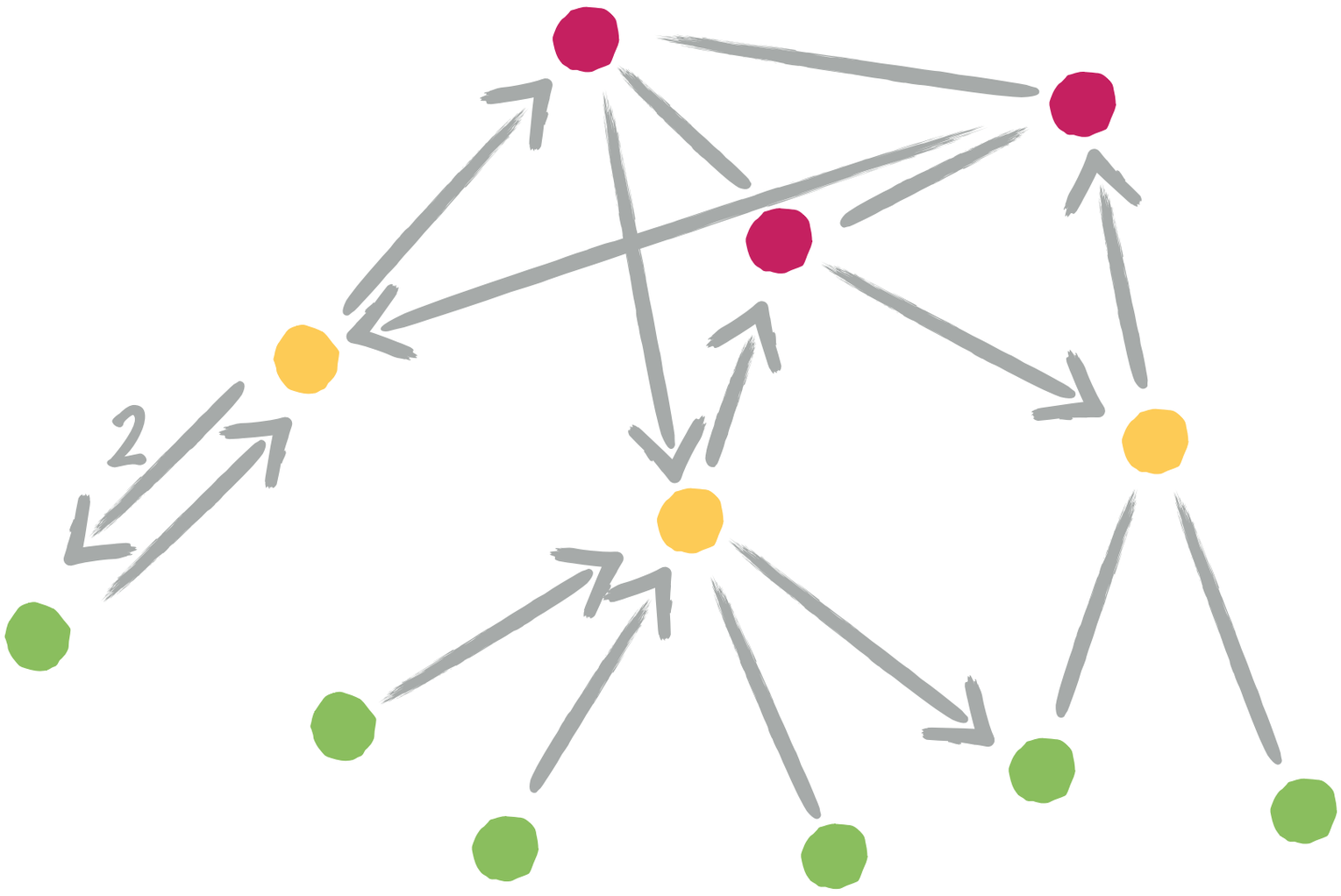
- With the number of vertices per level, and what we have seen about outgoing edges, do we have volcanoes?



Not yet...

VOLCANOES ALREADY?

- With the number of vertices per level, and what we have seen about outgoing edges, do we have volcanoes?

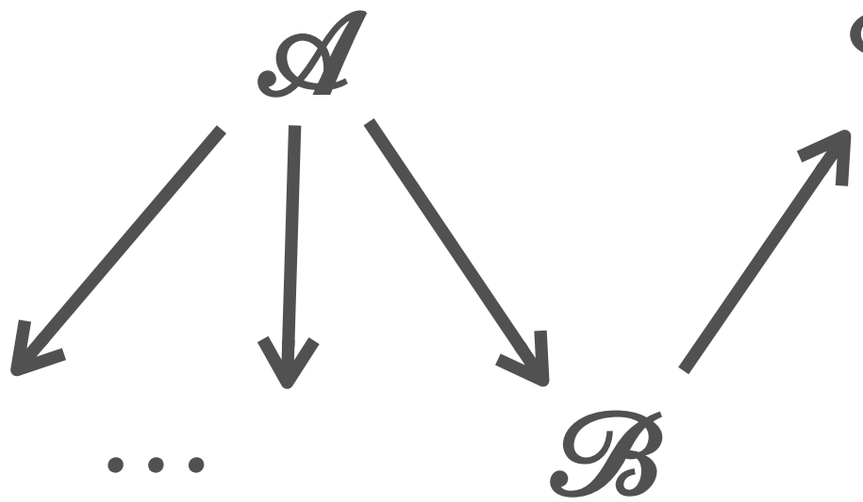


Not yet...

Not at all...

DESCENDING, THEN ASCENDING

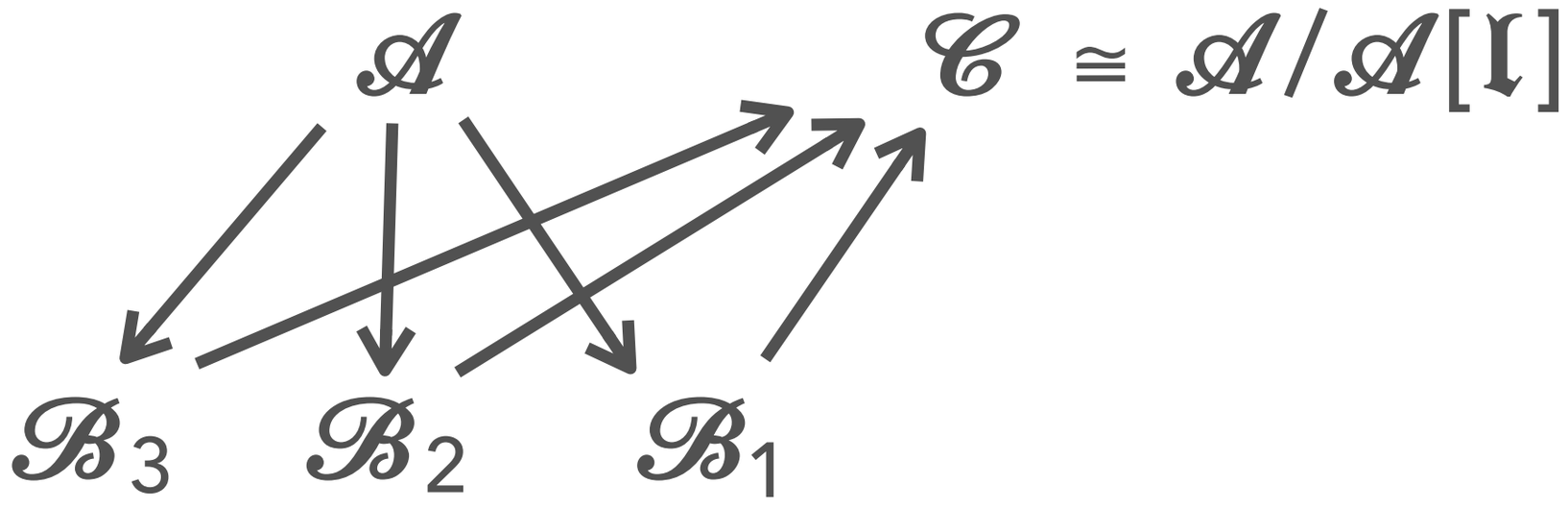
- If $\mathscr{A} \longrightarrow \mathscr{B}$ is a descending $\mathfrak{l}$-isogeny, where does the **unique** ascending isogeny from $\mathscr{B}$ go?



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

DESCENDING, THEN ASCENDING

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

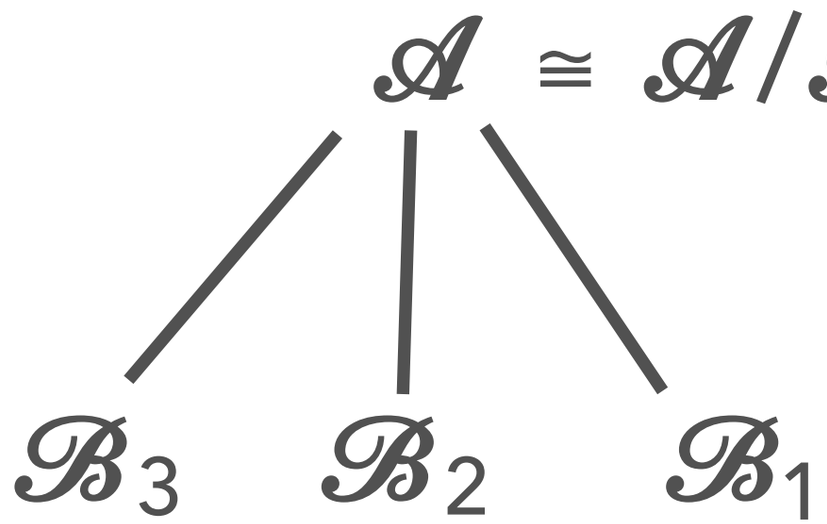


- It goes to $\mathscr{C} \cong \mathscr{A}/\mathscr{A}[\mathfrak{I}]$.

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

DESCENDING, THEN ASCENDING

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

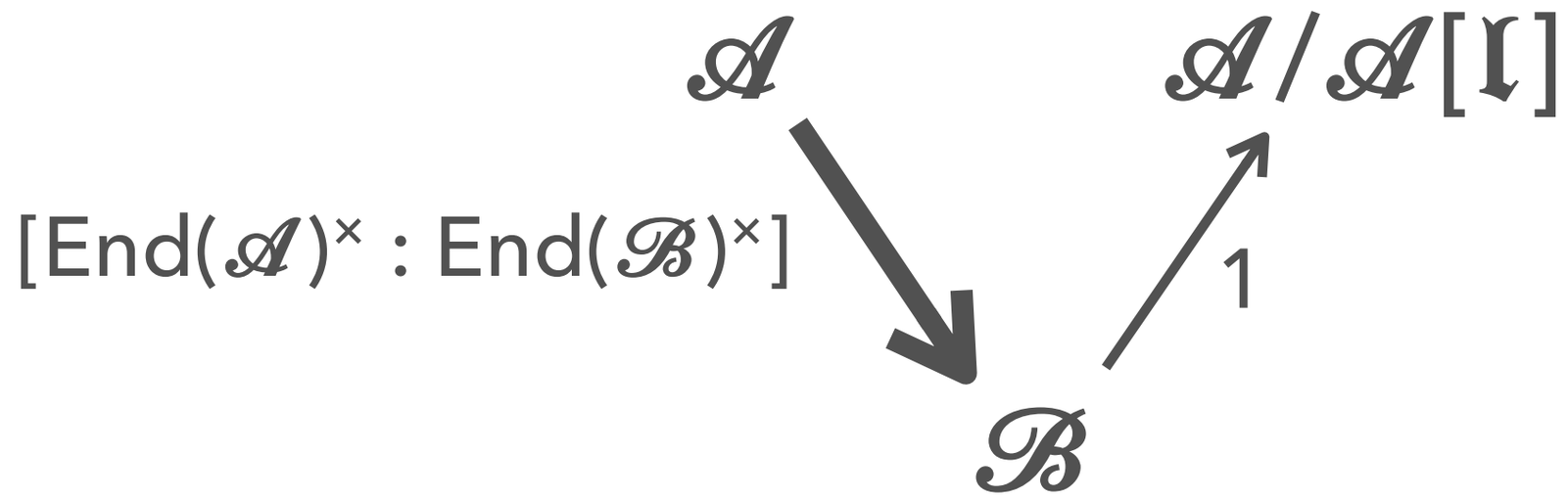


- It goes to $\mathscr{C} \cong \mathscr{A}/\mathscr{A}[\mathfrak{I}]$.

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

A LAST DETAIL: 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 $\mathscr{A} \longrightarrow \mathscr{B}$.



- 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 $K \neq \mathbb{Q}(\zeta_5)$)

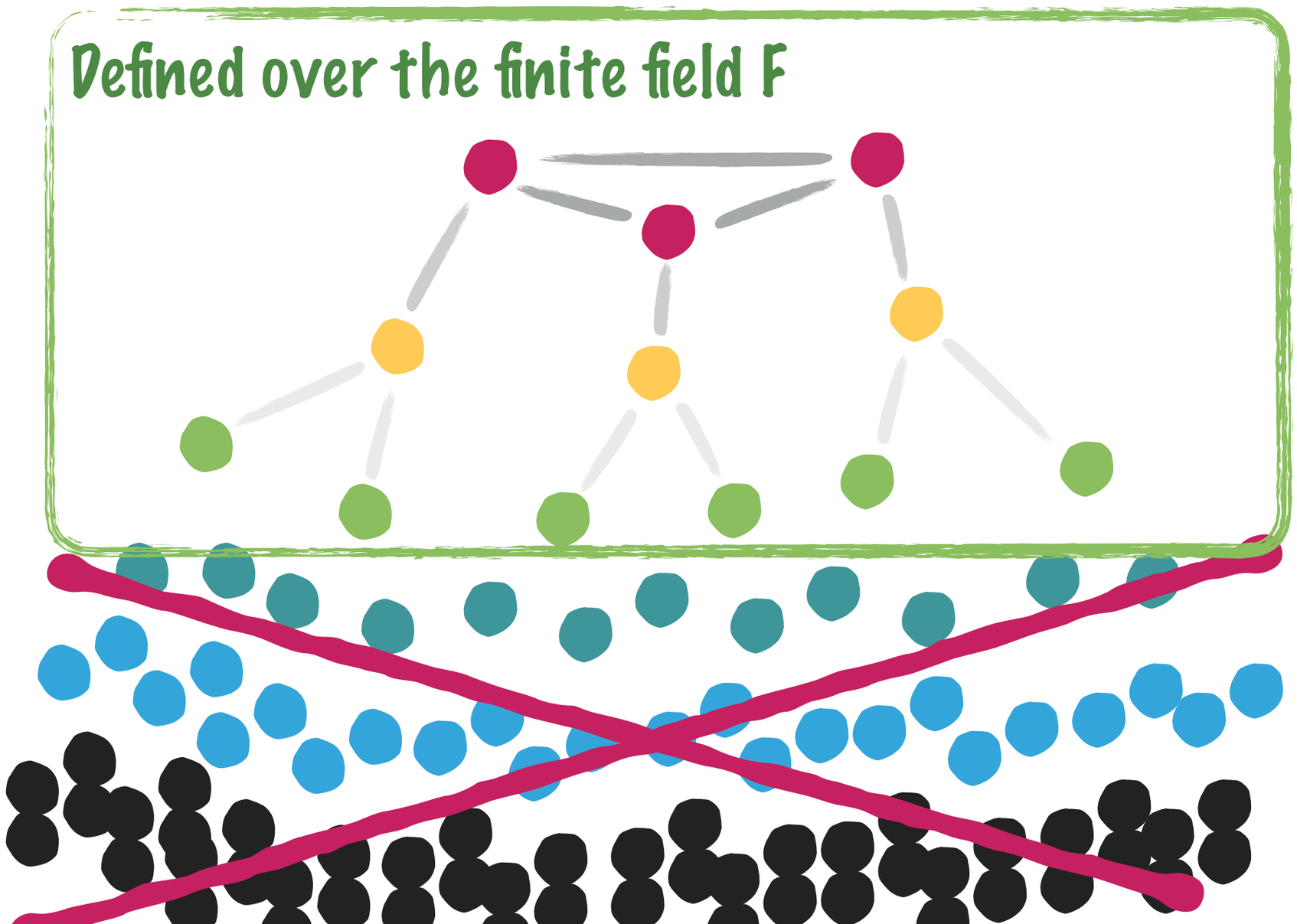
CONCLUDING

- 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 $\mathfrak{I}$ is principal (the edges are undirected).

A NOTE ON FINITENESS

- Some earlier slide claimed:

$$\#(\text{level } i+1) = N(\mathfrak{I}) \cdot \#(\text{level } i) \quad \text{for } i \geq 1$$



The graph is infinite… **over the algebraic closure**

Over a finite field, only a finite part remains

IN DIMENSION 2:

(ℓ,ℓ)-ISOGENIES

(ℓ,ℓ)-ISOGENIES

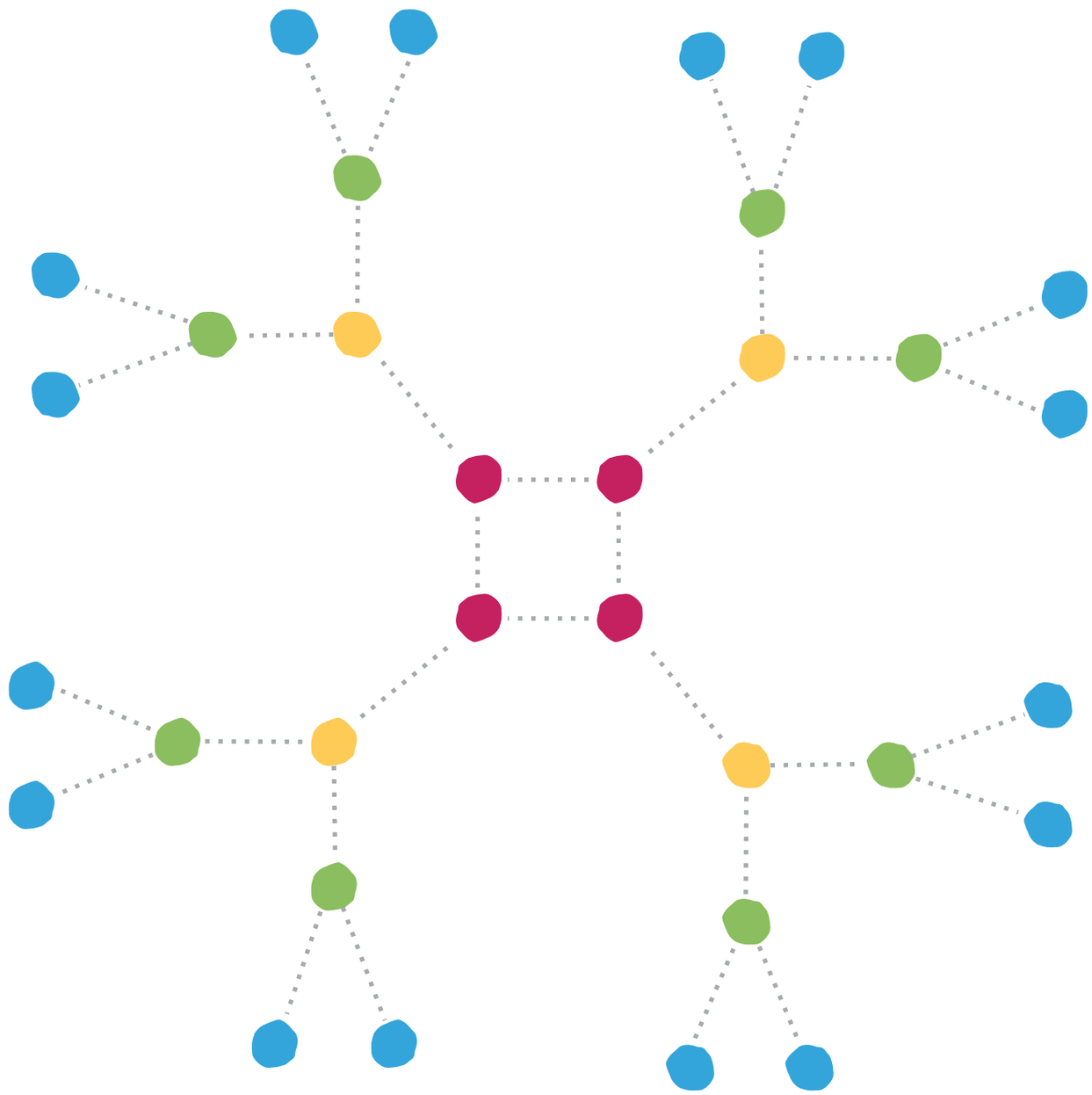
- Let $\mathscr{A}$ be a principally polarised, ordinary abelian surface.
- An (ℓ,ℓ)-isogeny is an isogeny $\mathscr{A} \to \mathscr{B}$ whose kernel is a maximal isotropic subgroup of $\mathscr{A}[\ell]$ for the Weil pairing.
- (ℓ,ℓ)-isogenies are easier to compute! Much more efficient than $\mathfrak{l}$-isogenies...

(ℓ,ℓ)-ISOGENIES

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

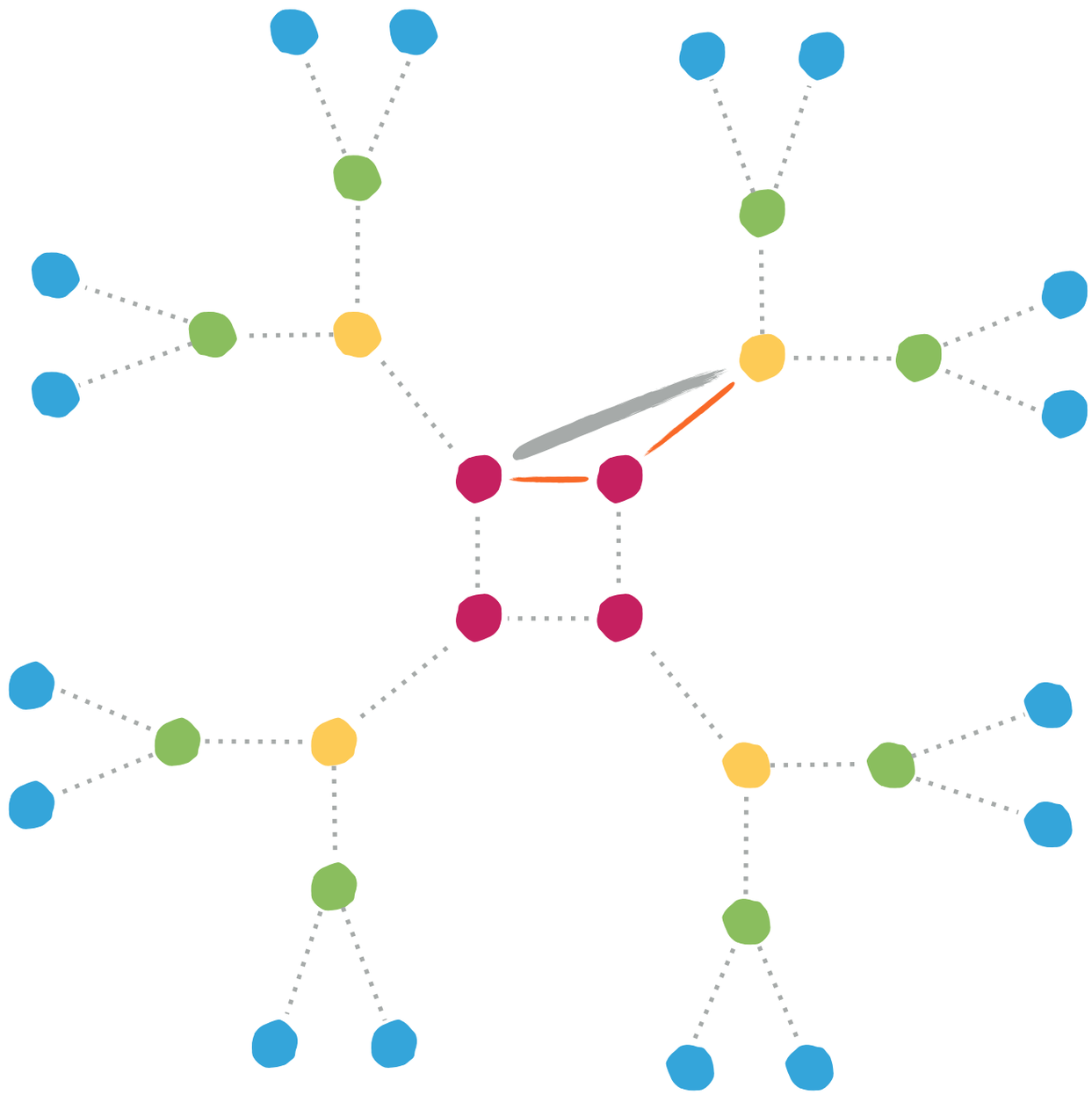
- The $\mathfrak{l}$-isogenies if ℓ is inert in K_0 (i.e., $\mathfrak{l} = \ell\mathcal{O}_{K_0}$)
- The compositions of an $\mathfrak{l}_1$-isogeny with an $\mathfrak{l}_2$-isogeny if ℓ splits or ramifies as $\ell\mathcal{O}_{K_0} = \mathfrak{l}_1\mathfrak{l}_2$ (the split case generalises a result of [Ionica and Thomé, 2014])

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



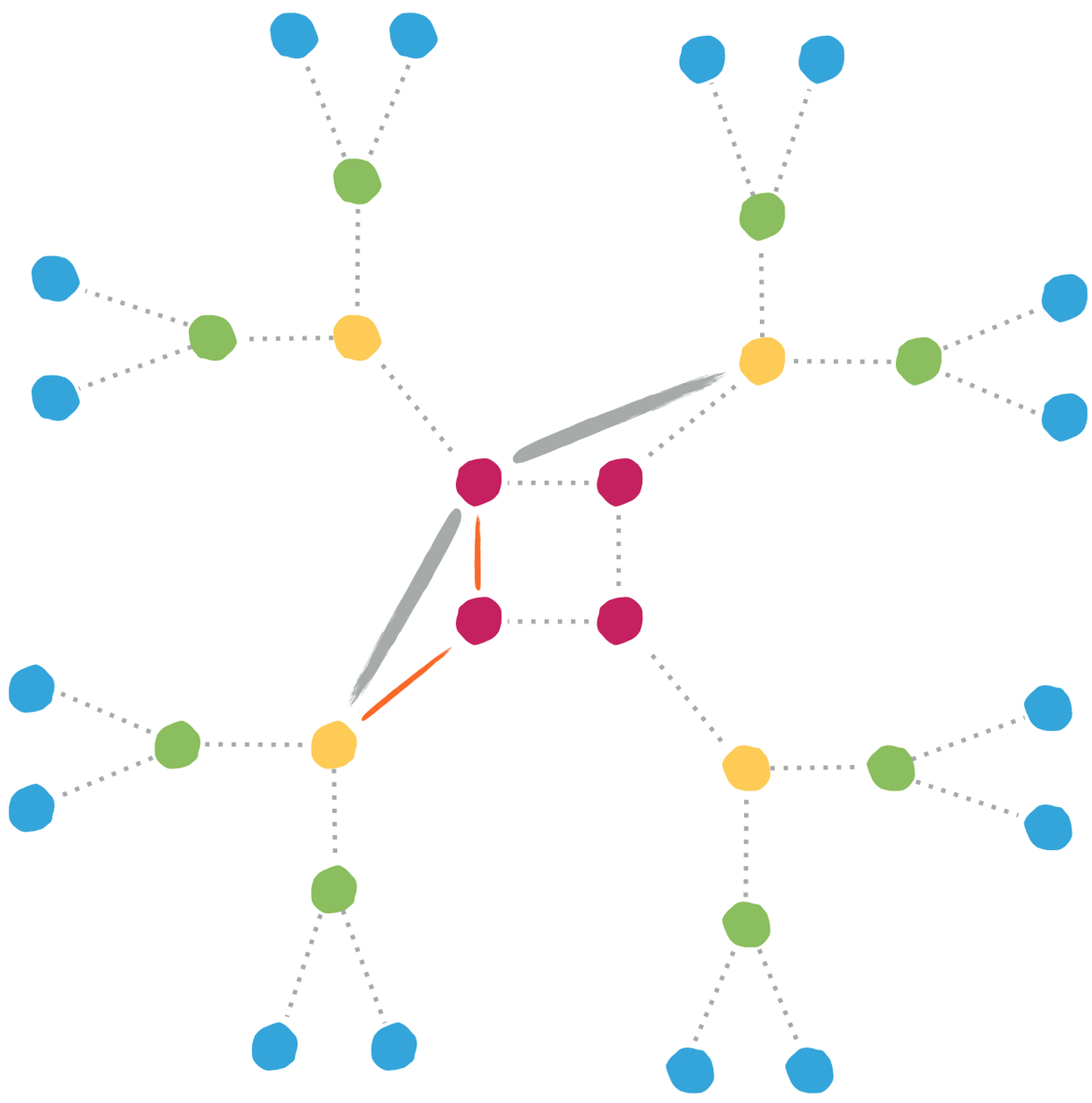
Assume $\ell \mathcal{O}_{K_0} = \mathfrak{l}^2$

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



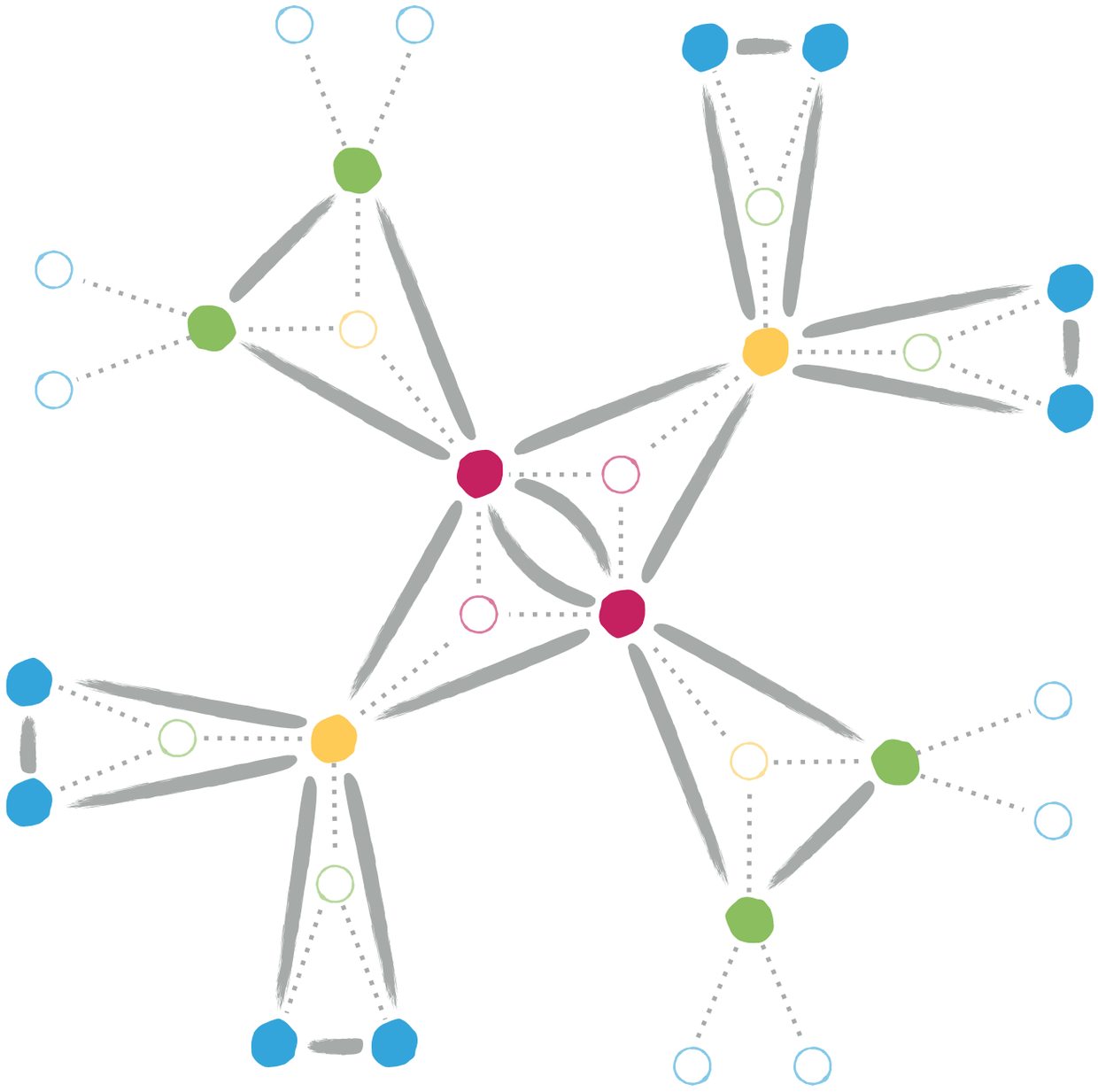
Assume $\ell \mathcal{O}_{K_0} = \mathfrak{l}^2$

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



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

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



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

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.

REFERENCES

[Bröker et al., 2012] R. Broker, K. Lauter and A. Sutherland, *Modular polynomials via isogeny volcanoes*, Math. Comp. 81, 2012

[Fouquet and Morain, 2002] M. Fouquet and F. Morain, *Isogeny volcanoes and the SEA algorithm*, ANTS 2002

[Ionica and Thomé, 2014] S. Ionica and E. Thomé, *Isogeny graphs with maximal real multiplication*, arXiv:1407.6672v1, 2014

[Jao et al., 2005] D. Jao, S. D. Miller, and R. Venkatesan, *Do all elliptic curves of the same order have the same difficulty of discrete log?*, Asiacrypt 2005

[Kohel, 1996] D. Kohel, *Endomorphism rings of elliptic curves over finite fields*, PhD thesis, University of California, Berkeley, 1996

[Sutherland, 2012] A. Sutherland, *Computing Hilbert class polynomials with the Chinese remainder theorem*, Math. Comp. 80, 2011

[Martindale, 2017] C. Martindale, *Isogeny graphs, modular polynomials, and applications*, forthcoming PhD thesis, 2017

[Main reference] E. Brooks, D. Jetchev and B. Wesolowski, *Isogeny graphs of ordinary abelian varieties*, Research in Number Theory 3:28, 2017 (open access http://rdcu.be/x0fg)

ERNEST HUNTER BROOKS

DIMITAR JETCHEV

BENJAMIN WESOLOWSKI

ISOGENY GRAPHS OF ORDINARY ABELIAN VARIETIES

PRESENTED AT ECC 2017, NIJMEGEN, THE NETHERLANDS BY BENJAMIN WESOLOWSKI FROM EPFL, SWITZERLAND