EPFL, Lausanne, Switzerland

E. Hunter Brooks Dimitar Jetchev Benjamin Wesolowski

GRAPHES D'ISOGÉNIES DE VARIÉTÉS ABÉLIENNES ORDINAIRES

Aux Journées Codage et Cryptographie 2017, La Bresse

UNE INTRODUCTION
NON-VIOLENTE AUX

GRAPHES D'ISOGÉNIES

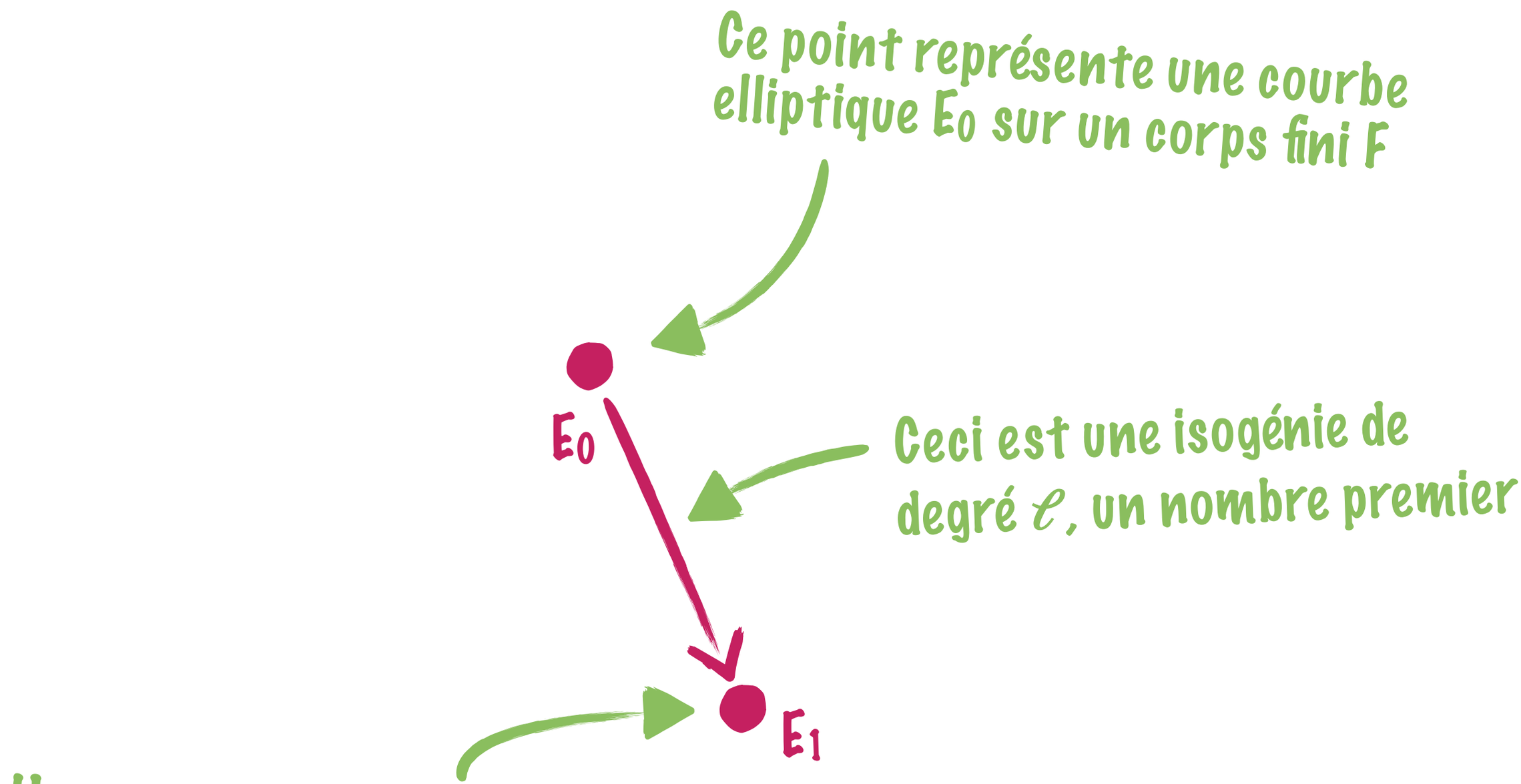
GRAPHES D'ISOGÉNIES DE COURBES ELLIPTIQUES (ORDINAIRES)

GRAPHES D'ISOGÉNIES DE COURBES ELLIPTIQUES (ORDINAIRES)

Ce point représente une courbe elliptique E_0 sur un corps fini F

E_0

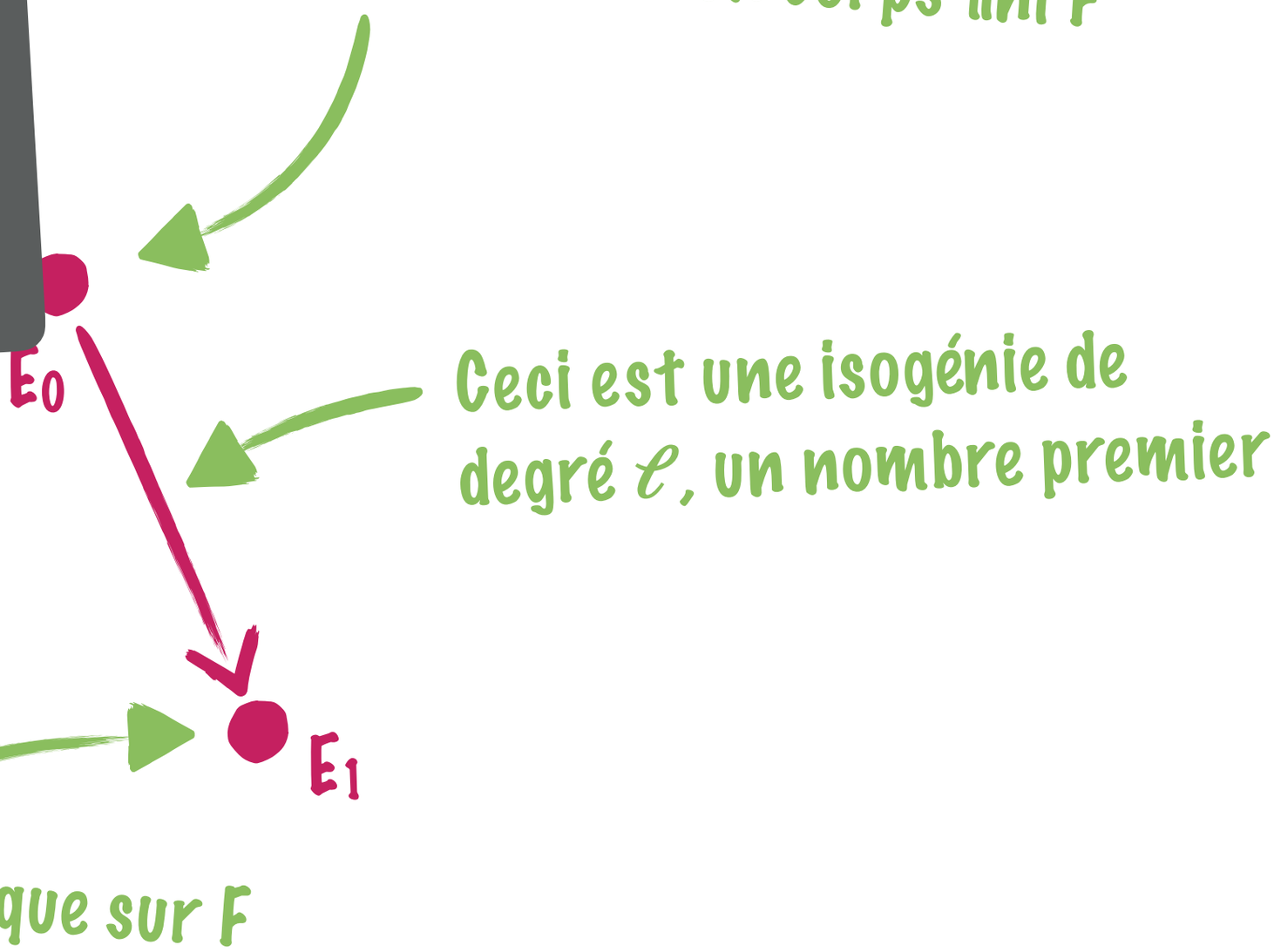
GRAPHES D'ISOGÉNIES DE COURBES ELLIPTIQUES (ORDINAIRES)



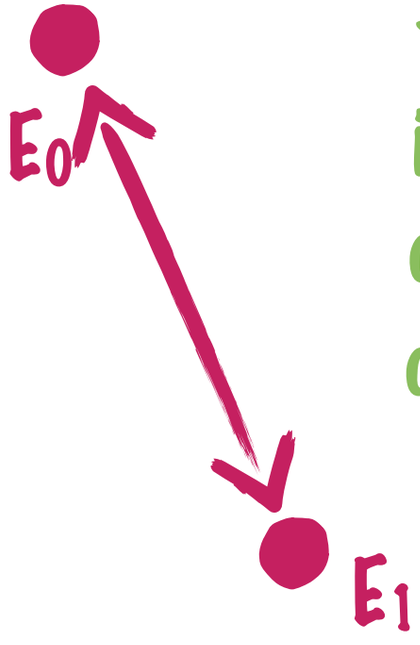
GRAPHES D'ISOGÉNIES DE COURBES ELLIPTIQUES (ORDINAIRES)

Une isogénie est un morphisme de noyau fini entre deux courbes elliptiques.

Le degré d'une isogénie est la taille de son noyau (nos isogénies sont séparables...)

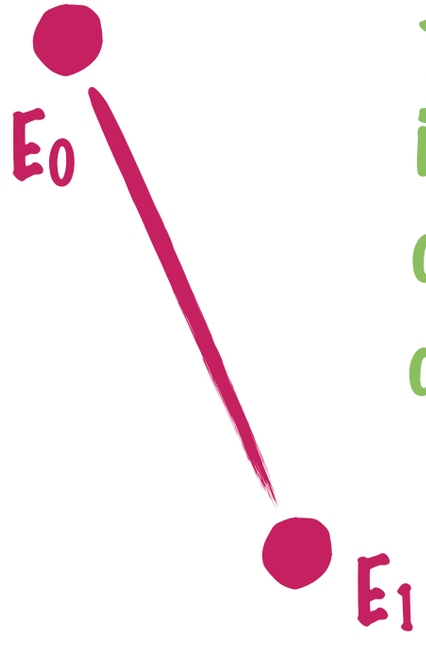


GRAPHES D'ISOGÉNIES DE COURBES ELLIPTIQUES (ORDINAIRES)



Toute isogénie a une isogénie duale de même degré (ici ℓ) allant dans la direction opposée

GRAPHES D'ISOGÉNIES DE COURBES ELLIPTIQUES (ORDINAIRES)

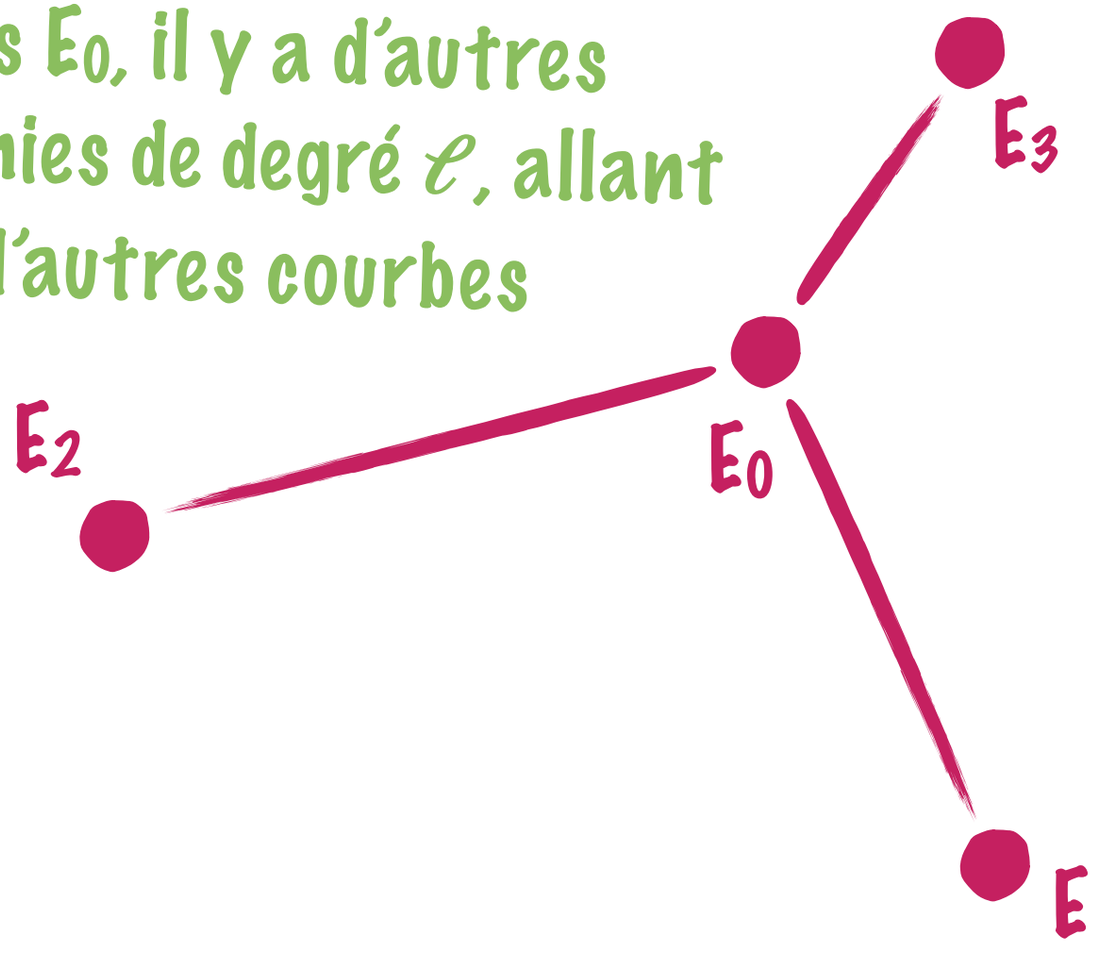


Toute isogénie a une isogénie duale de même degré (ici ℓ) allant dans la direction opposée

Donc on la représente comme une arête non-orientée

GRAPHES D'ISOGÉNIES DE COURBES ELLIPTIQUES (ORDINAIRES)

Depuis E_0, il y a d'autres isogénies de degré ℓ, allant vers d'autres courbes



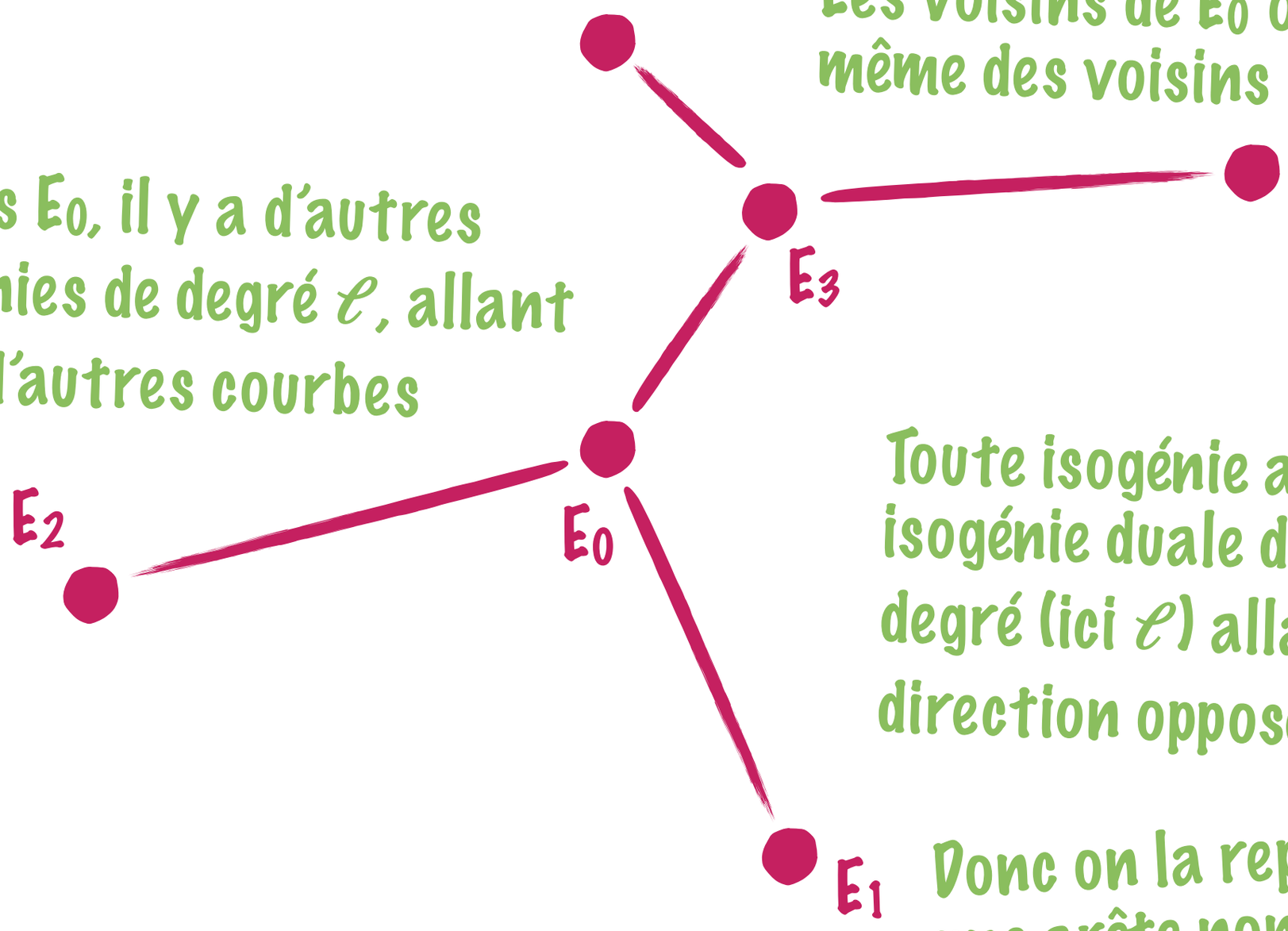
Toute isogénie a une isogénie duale de même degré (ici ℓ) allant dans la direction opposée

Donc on la représente comme une arête non-orientée

GRAPHES D'ISOGÉNIES DE COURBES ELLIPTIQUES (ORDINAIRES)

Les voisins de E_0 ont eux-même des voisins

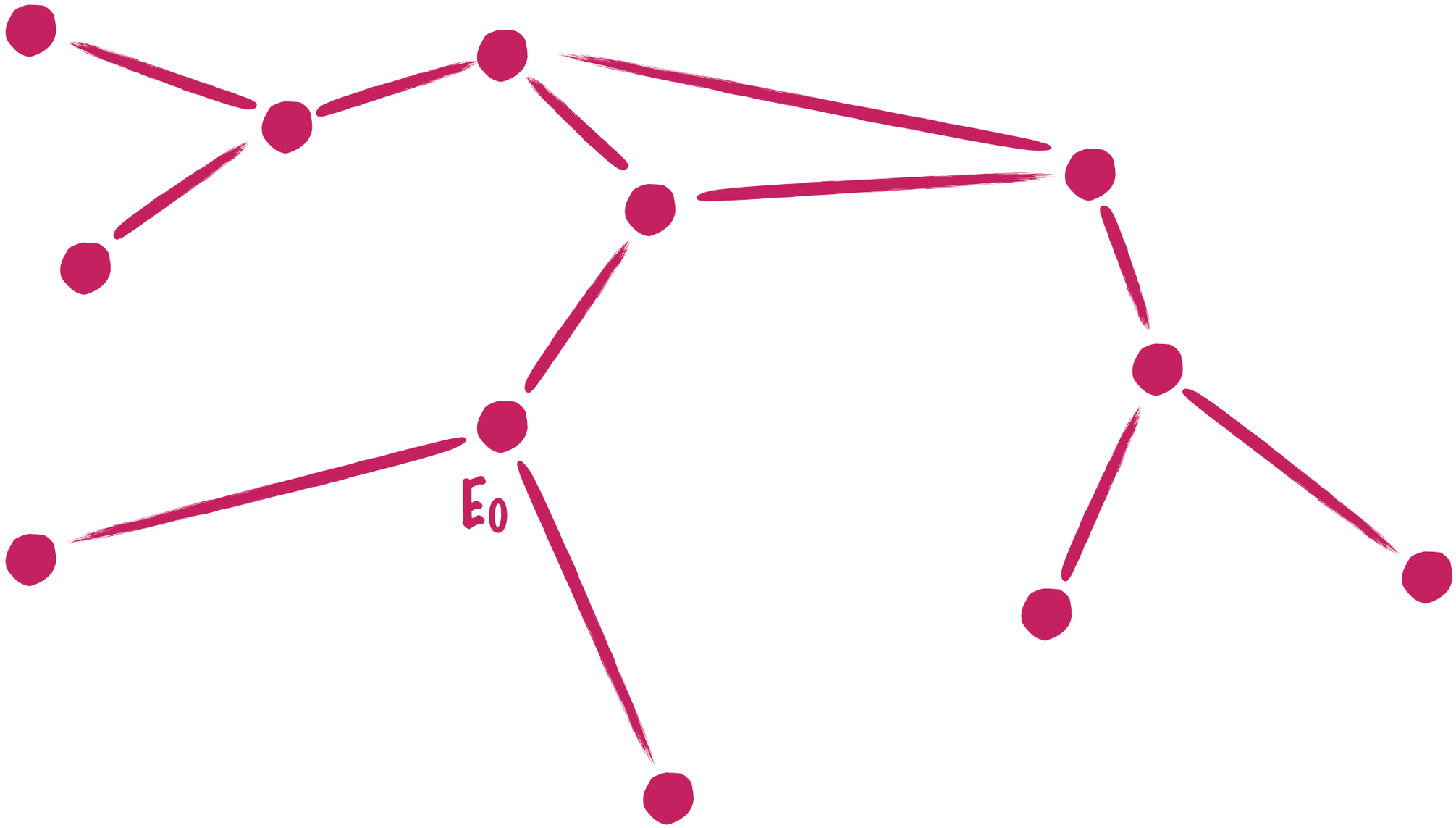
Depuis E_0, il y a d'autres isogénies de degré ℓ, allant vers d'autres courbes



Toute isogénie a une isogénie duale de même degré (ici ℓ) allant dans la direction opposée

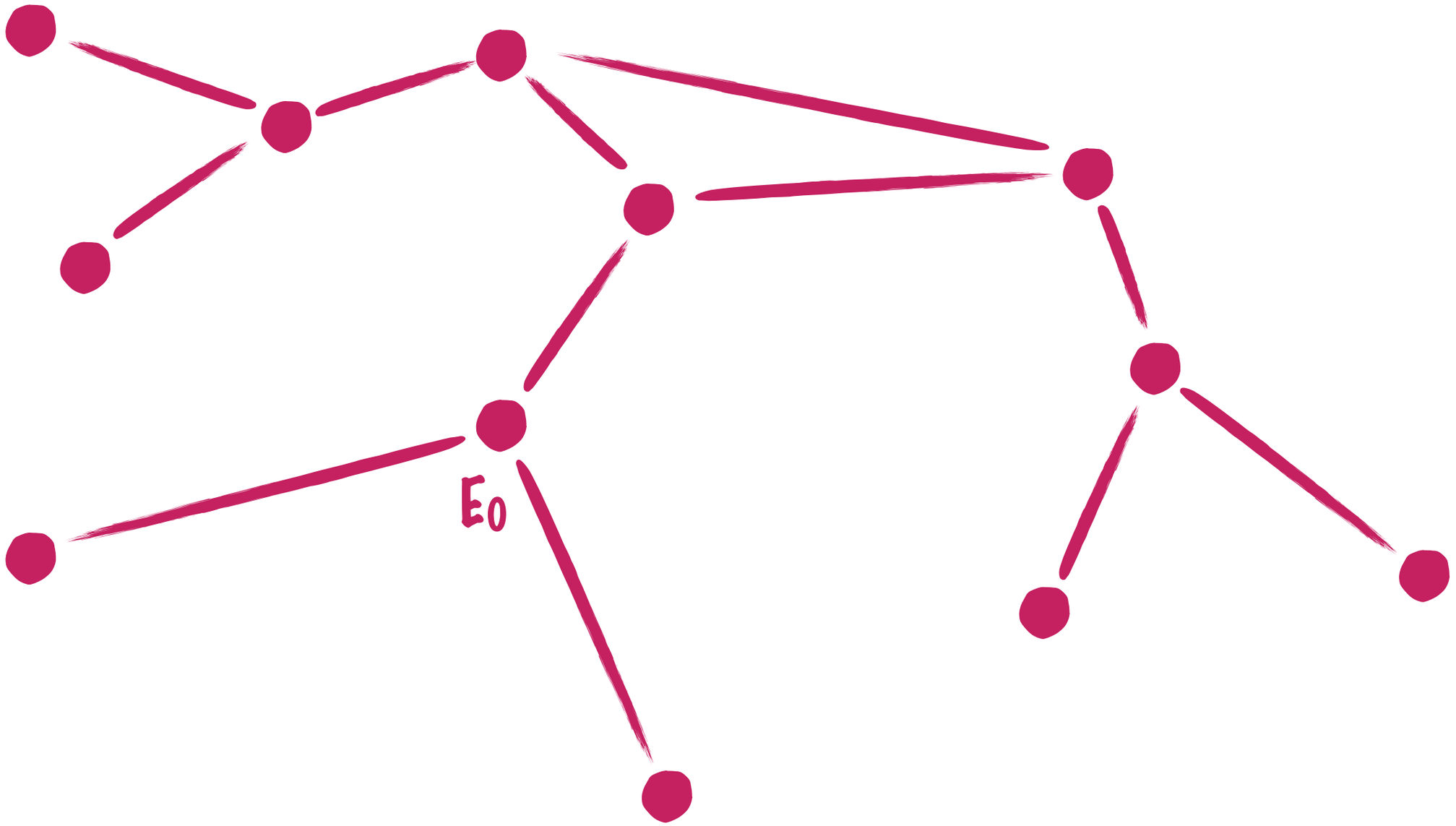
Donc on la représente comme une arête non-orientée

GRAPHES D'ISOGÉNIES DE COURBES ELLIPTIQUES (ORDINAIRES)



Une fois qu'on a atteint tous les voisins possibles,
on a le graphe connexe de ℓ-isogenies de E_0

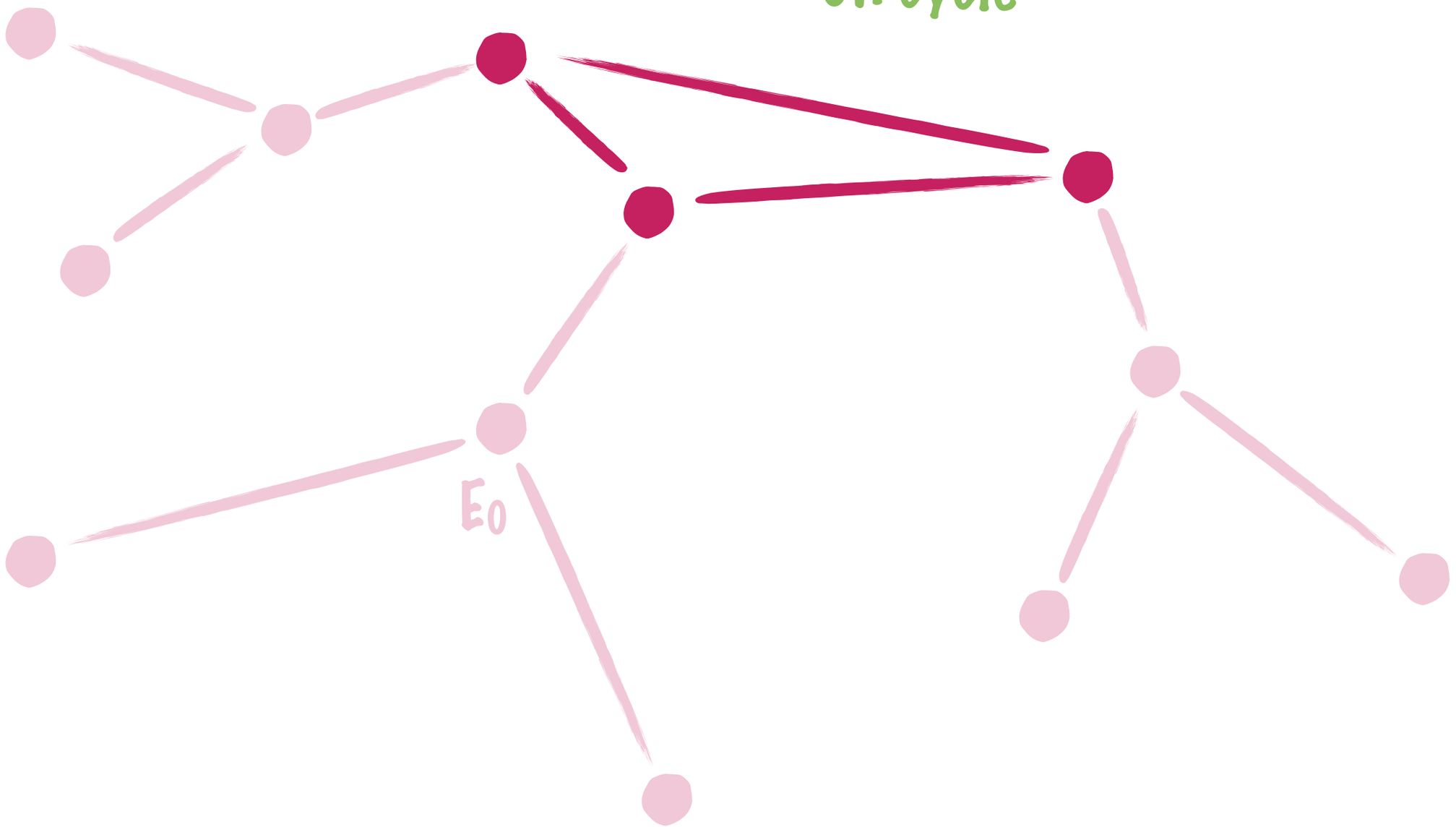
GRAPHES D'ISOGÉNIES DE COURBES ELLIPTIQUES (ORDINAIRES)



Et celui-ci est un exemple typique !

GRAPHES D'ISOGÉNIES DE COURBES ELLIPTIQUES (ORDINAIRES)

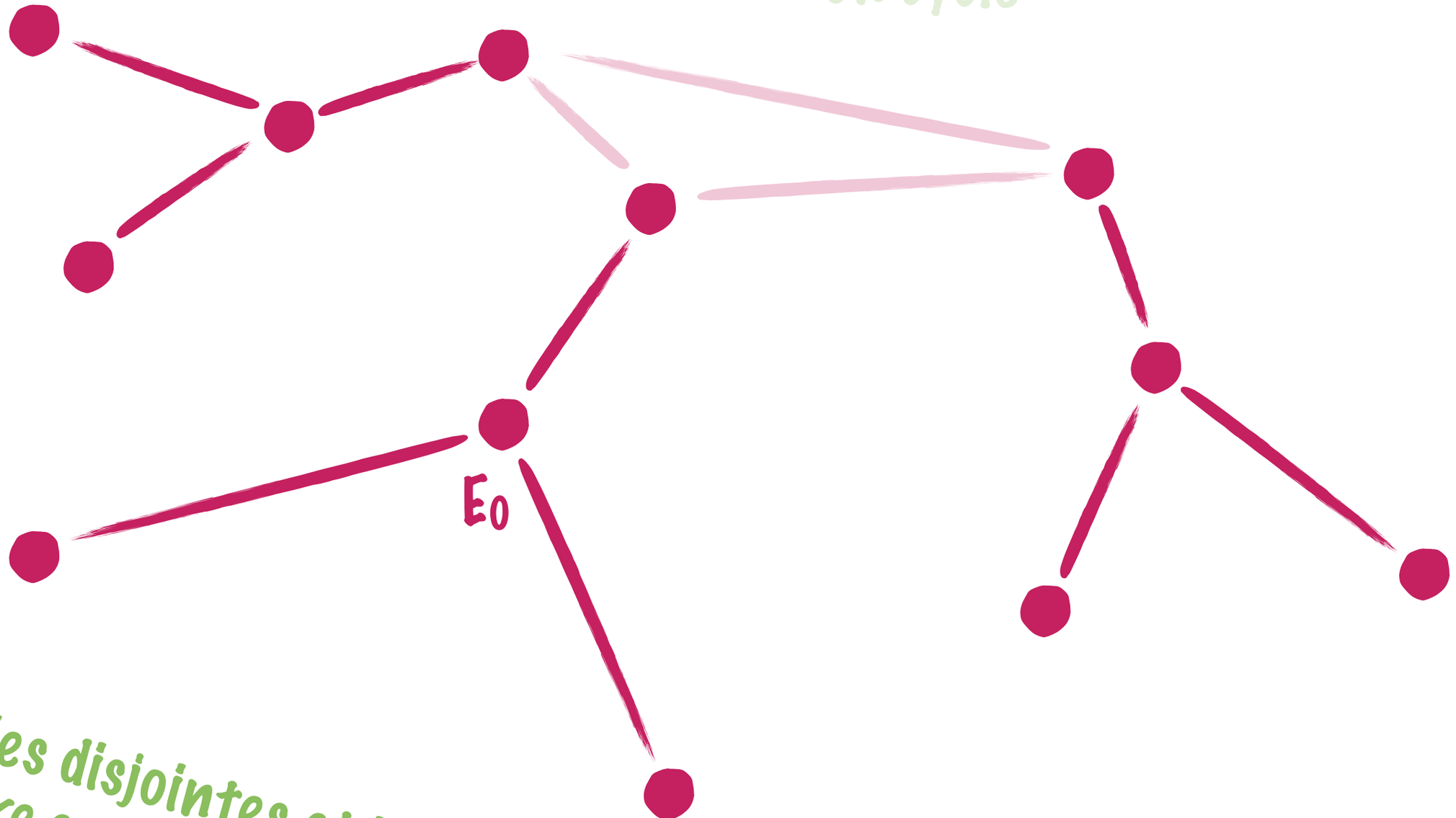
Un cycle



Et celui-ci est un exemple typique !

GRAPHES D'ISOGÉNIES DE COURBES ELLIPTIQUES (ORDINAIRES)

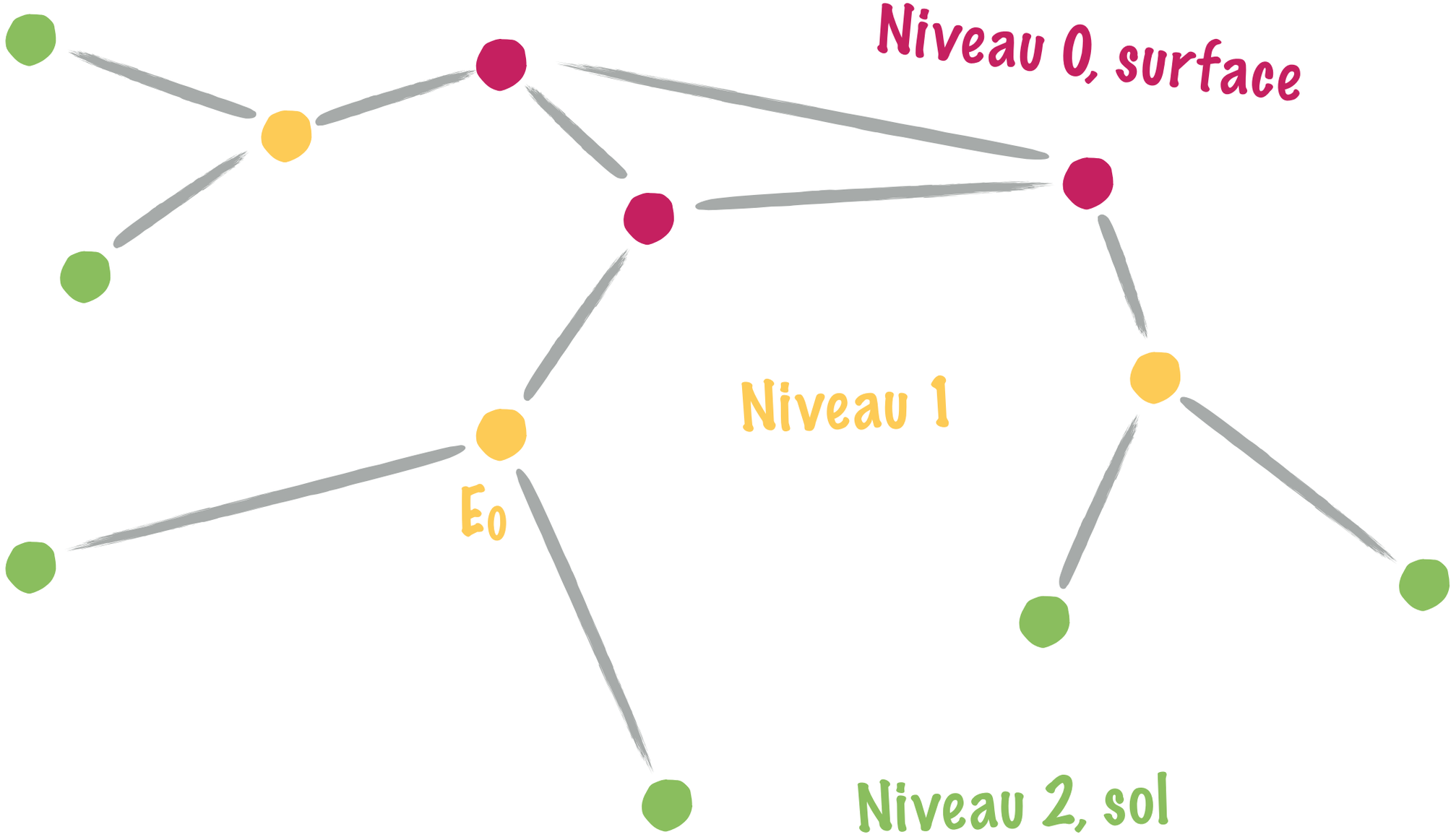
Un cycle



Des copies disjointes et isomorphes d'un arbre enraciné sur le cycle

Et celui-ci est un exemple typique !

GRAPHES D'ISOGÉNIES DE COURBES ELLIPTIQUES (ORDINAIRES)



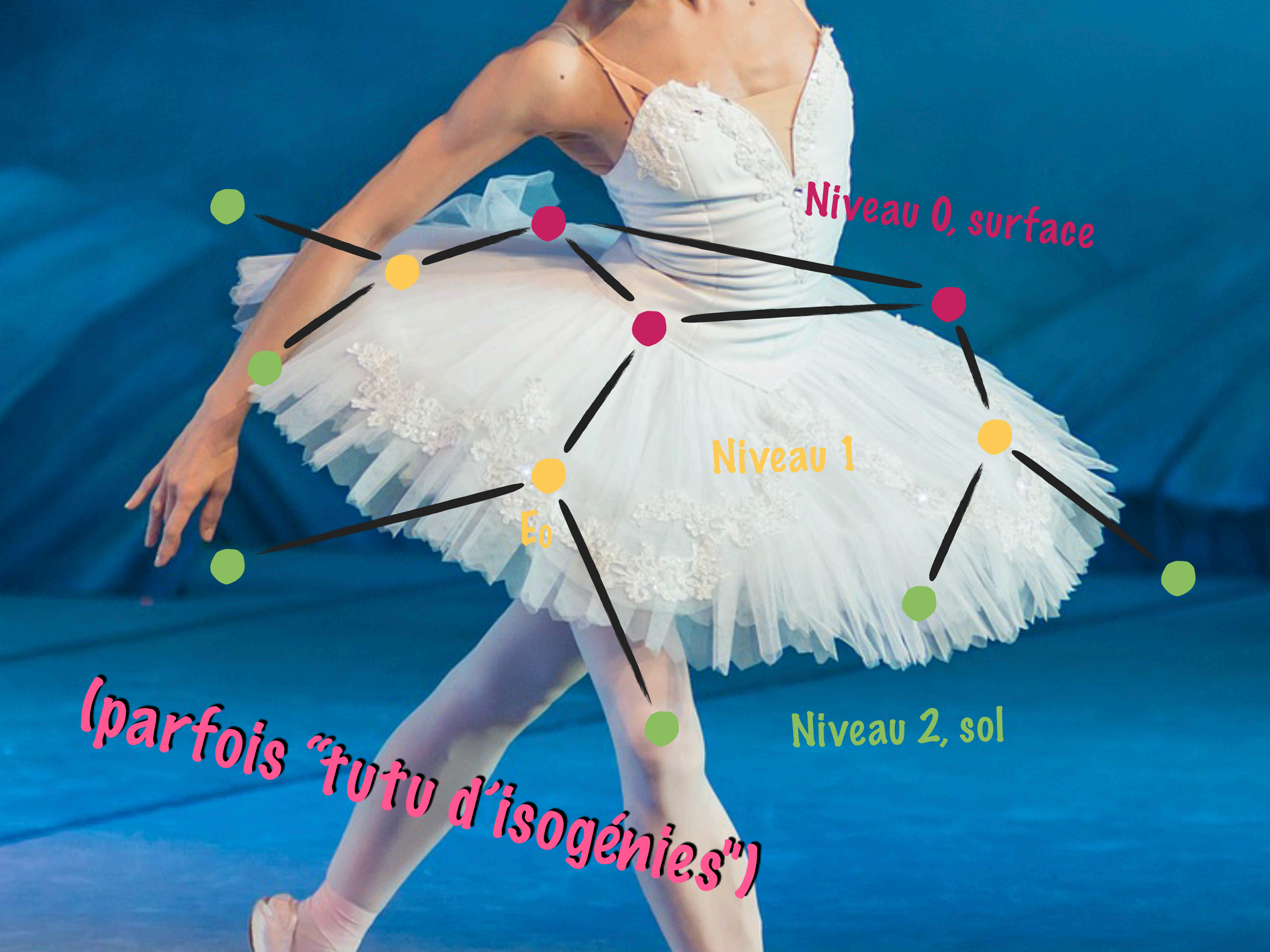
Un volcan d'isogénies

Niveau 0, surface

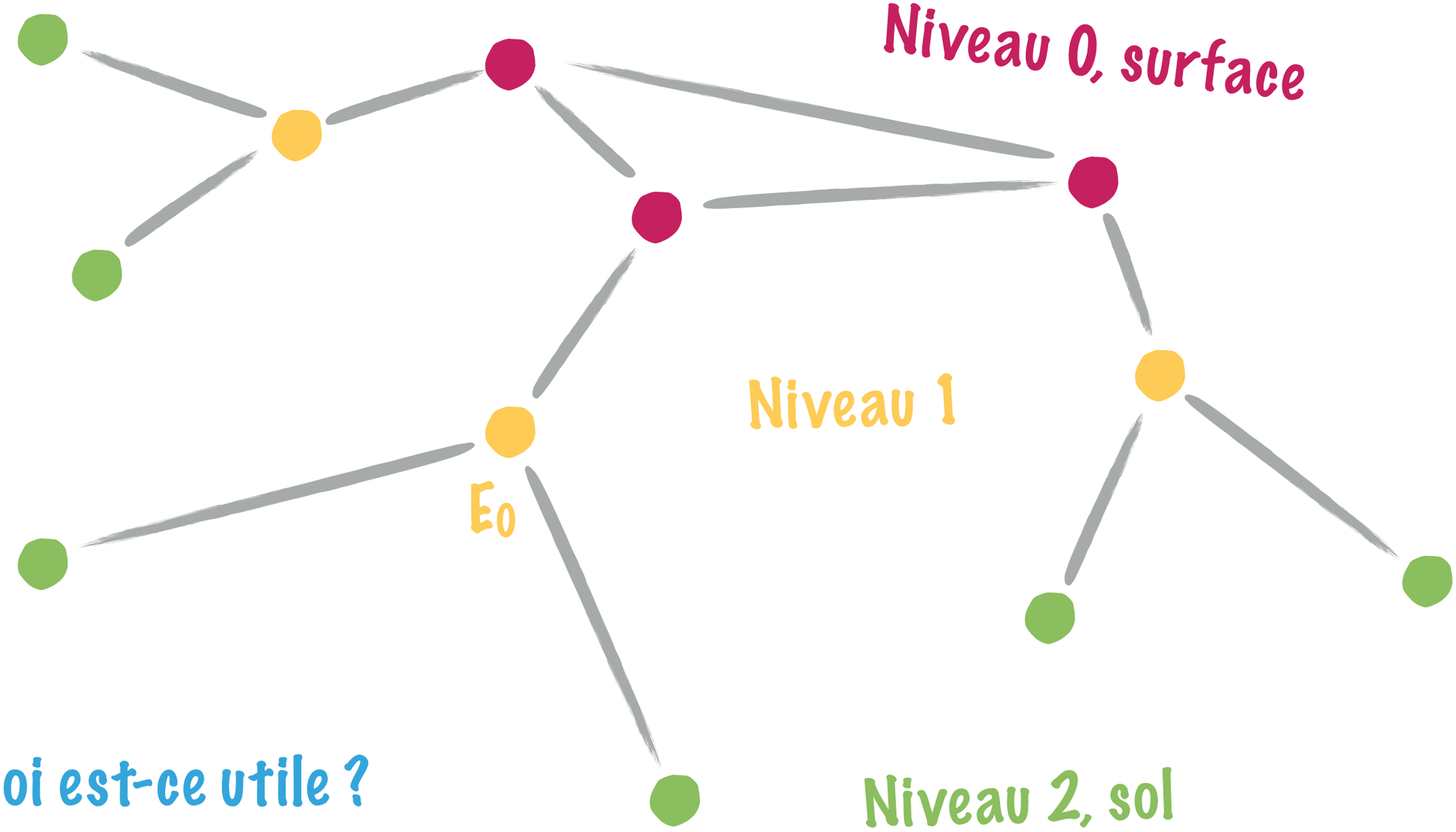
Niveau 1

E_0

Niveau 2, sol


Niveau 0, surface
Niveau 1
E0
Niveau 2, sol
(parfois "tutu d'isogénies")

GRAPHES D'ISOGÉNIES DE COURBES ELLIPTIQUES (ORDINAIRES)



Pourquoi est-ce utile ?

En regardant **seulement** la structure de ce graphe, on peut déterminer que E_0 est de "niveau 1" en ℓ... Et ça en dit long sur l'anneau des endomorphismes de E_0 !

APPLICATIONS

- Calcul de l'anneau des endomorphismes d'une courbe elliptique [Kohel, 1996],
- Comptage de points [Fouquet et Morain, 2002],
- Auto-réductibilité aléatoire du problème du logarithme discret [Jao et al., 2005] (réduction pire cas vers cas moyen)
- Accélérer la méthode CM [Sutherland 2012],
- Calcul de polynômes modulaires [Bröker et al., 2012]

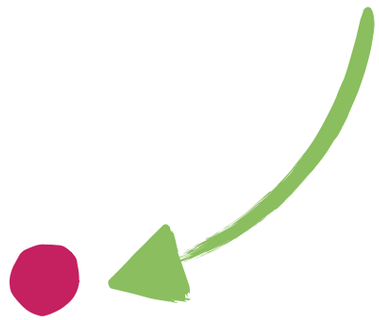
GÉNÉRALISER AUX VARIÉTÉS ABÉLIENNES ORDINAIRES…

- Toutes ces applications motivent la recherche d'une généralisation aux autres variétés abéliennes…

GÉNÉRALISER AUX VARIÉTÉS ABÉLIENNES…

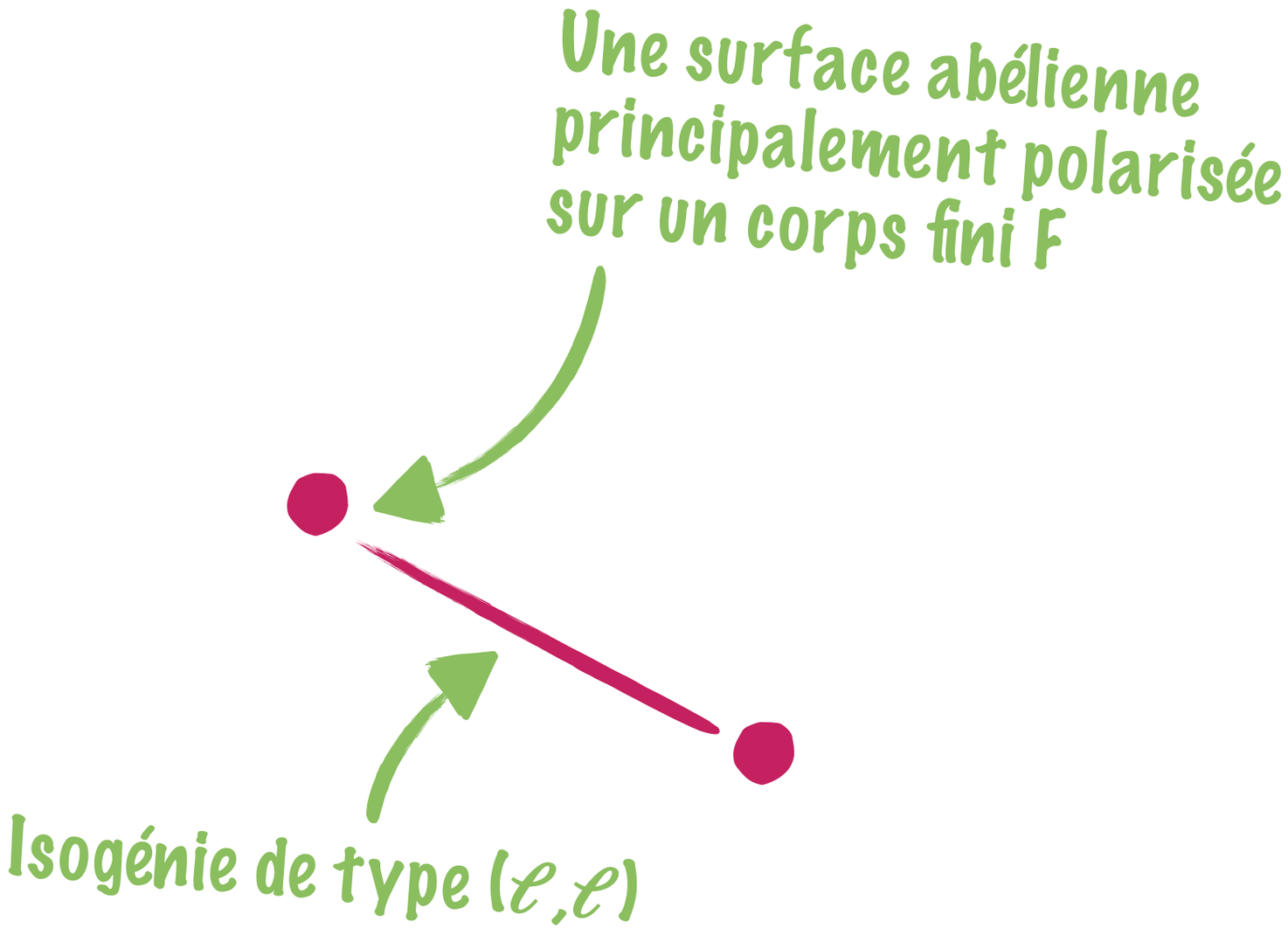
- Toutes ces applications motivent la recherche d'une généralisation aux autres variétés abéliennes…

Une surface abélienne principalement polarisée sur un corps fini F



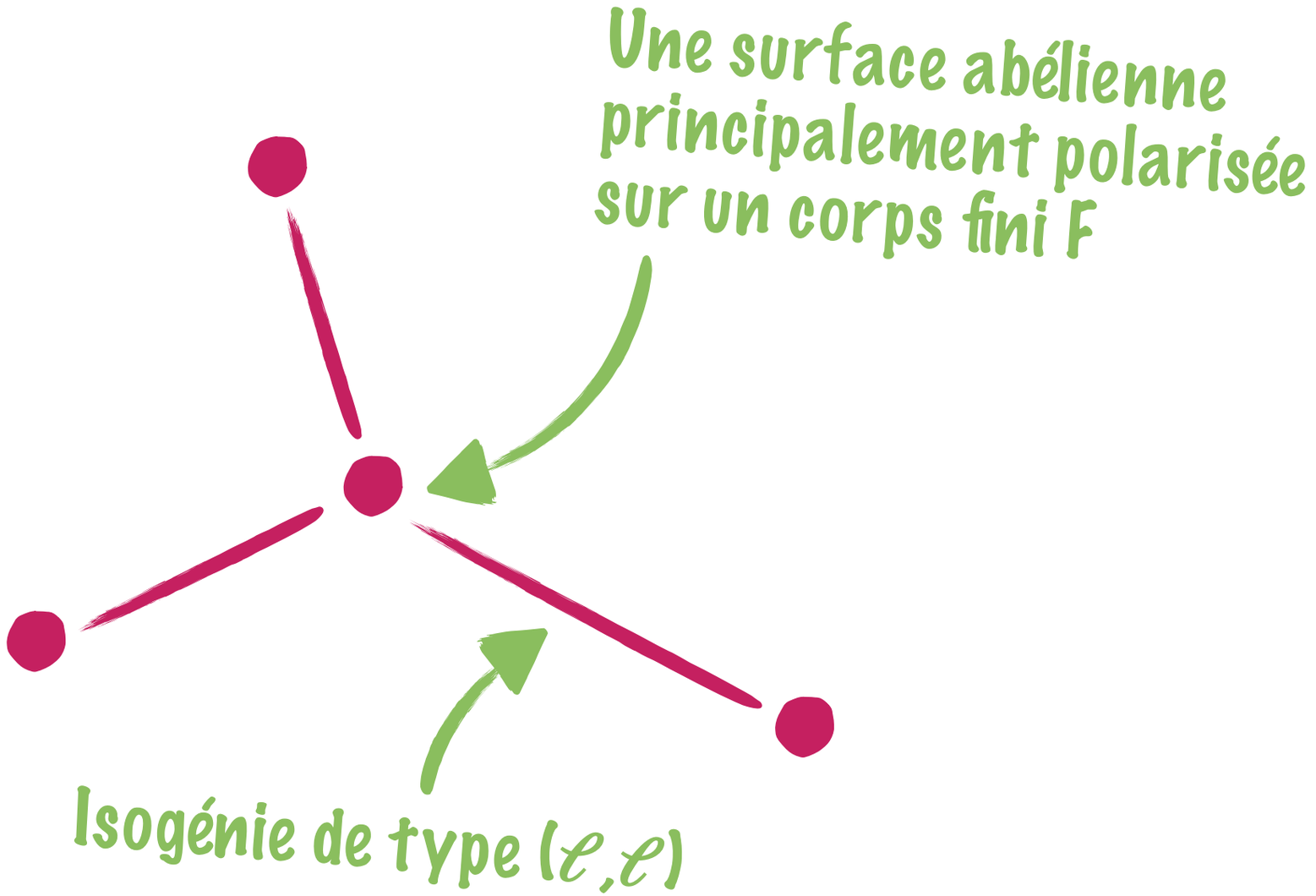
GÉNÉRALISER AUX VARIÉTÉS ABÉLIENNES ORDINAIRES…

- Toutes ces applications motivent la recherche d'une généralisation aux autres variétés abéliennes…



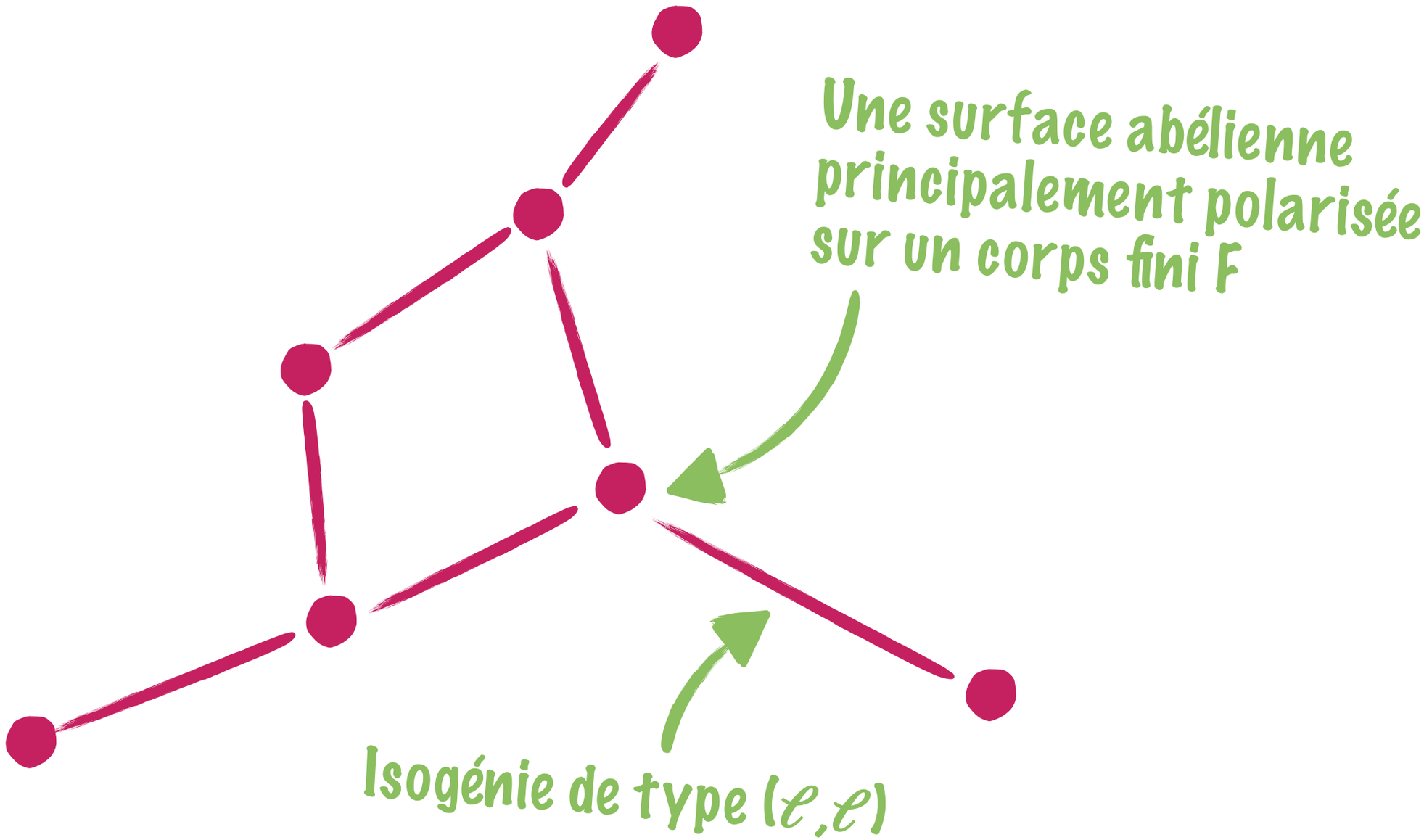
GÉNÉRALISER AUX VARIÉTÉS ABÉLIENNES ORDINAIRES…

- Toutes ces applications motivent la recherche d'une généralisation aux autres variétés abéliennes…



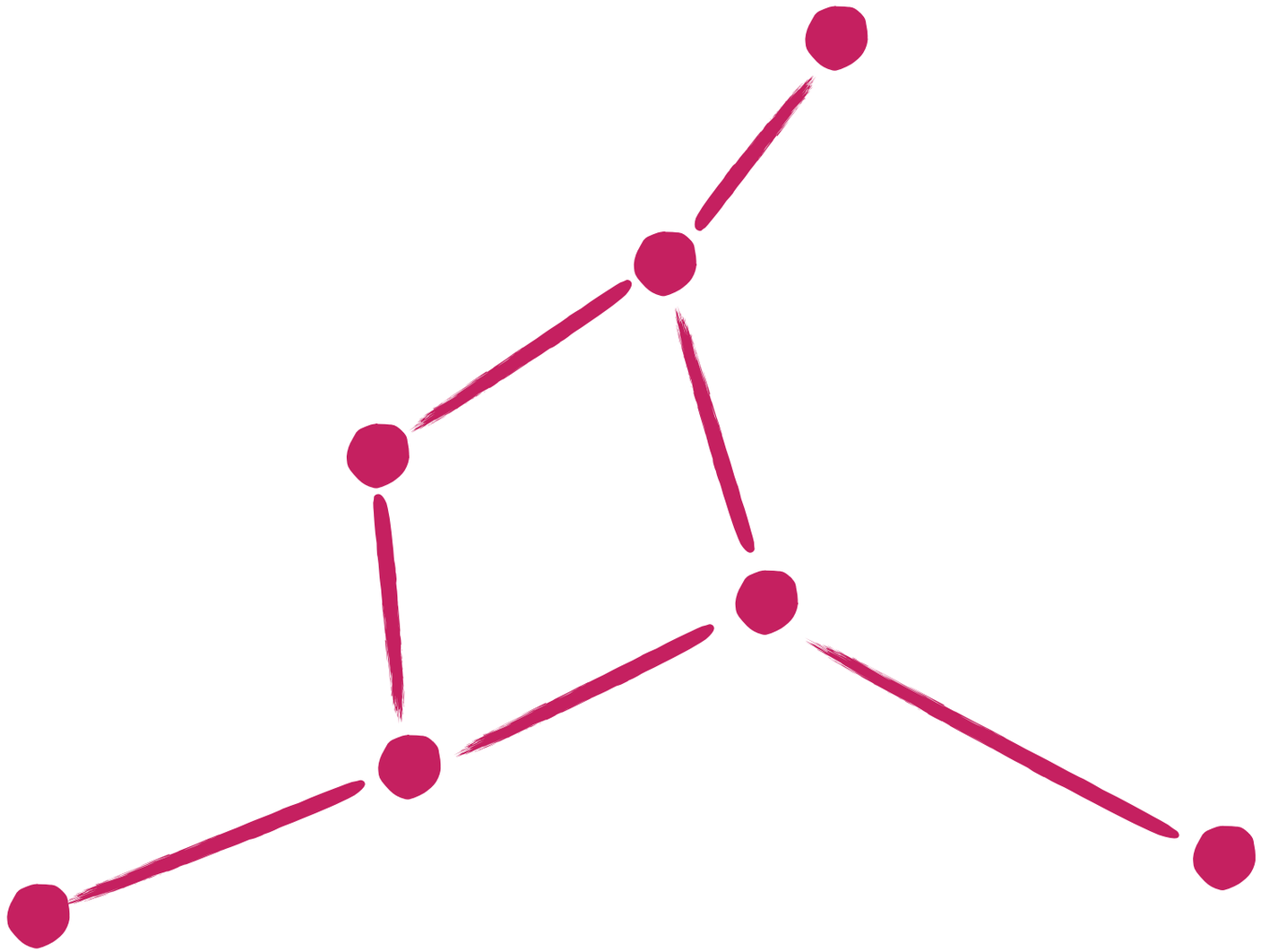
GÉNÉRALISER AUX VARIÉTÉS ABÉLIENNES ORDINAIRES…

- Toutes ces applications motivent la recherche d'une généralisation aux autres variétés abéliennes…



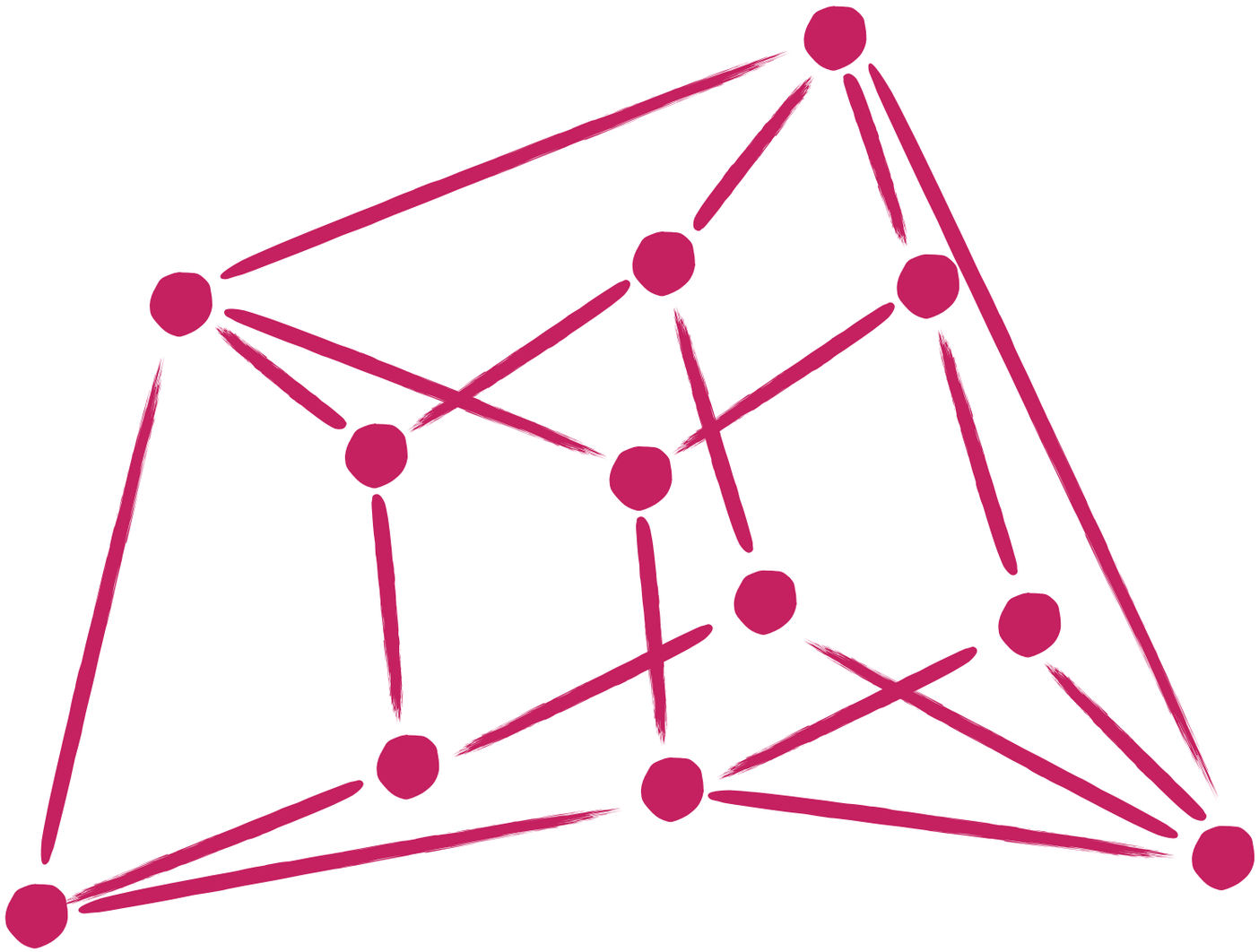
GÉNÉRALISER AUX VARIÉTÉS ABÉLIENNES…

- Toutes ces applications motivent la recherche d'une généralisation aux autres variétés abéliennes…



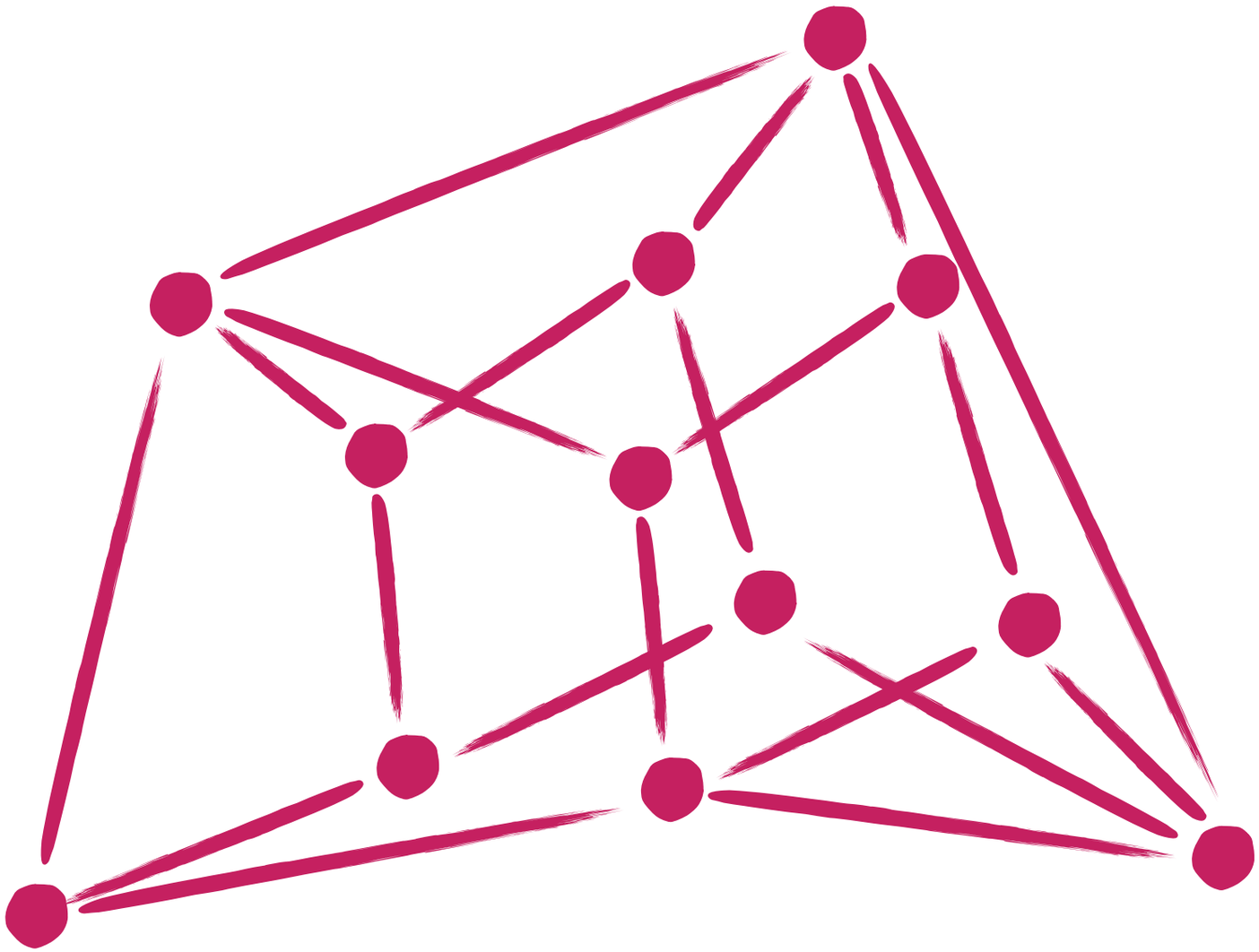
GÉNÉRALISER AUX VARIÉTÉS ABÉLIENNES ORDINAIRES…

- Toutes ces applications motivent la recherche d'une généralisation aux autres variétés abéliennes…



GÉNÉRALISER AUX VARIÉTÉS ABÉLIENNES ORDINAIRES…

- Toutes ces applications motivent la recherche d'une généralisation aux autres variétés abéliennes…



GÉNÉRALISER AUX VARIÉTÉS ABÉLIENNES ORDINAIRES…

- Toutes ces applications motivent la recherche d'une généralisation aux autres variétés abéliennes…

GÉNÉRALISER AUX VARIÉTÉS ABÉLIENNES ORDINAIRES...

Les isogénies (ℓ, ℓ) ne sont peut-être pas celles qu'il faut regarder ?

On ne cherche pas les bonnes structures ?

Faut-il se concentrer sur des sous-graphes ?

ANNEAU DES ENDOMORPHISMES

ALGÈBRE ET ANNEAU DES ENDOMORPHISMES

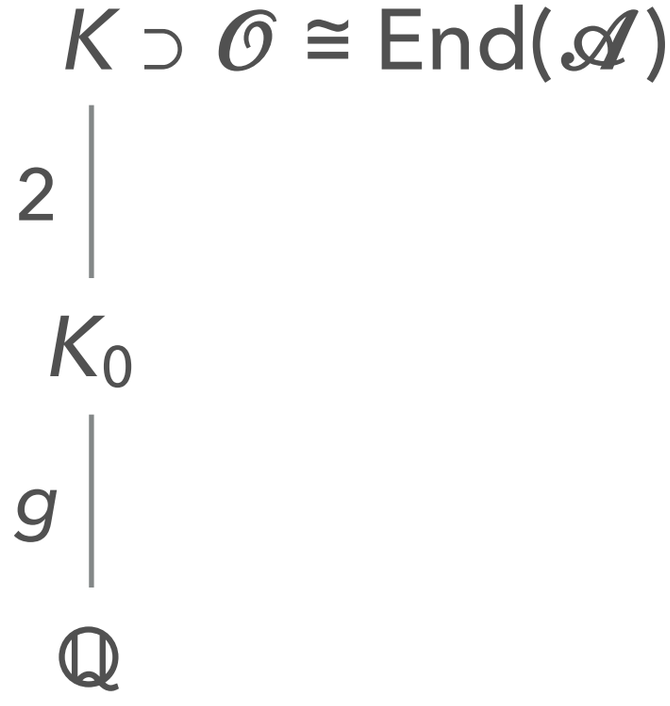
- Soit $\mathscr{A}$ une variété abélienne ordinaire de dimension g sur un corps fini $F = \mathbb{F}_q$.

ALGÈBRE ET ANNEAU DES ENDOMORPHISMES

- Soit $\mathscr{A}$ une variété abélienne ordinaire de dimension g sur un corps fini $F = \mathbb{F}_q$.
- Les endomorphismes de $\mathscr{A}$ forment un anneau $\mathrm{End}(\mathscr{A})$.

ALGÈBRE ET ANNEAU DES ENDOMORPHISMES

- Soit $\mathscr{A}$ une variété abélienne ordinaire de dimension g sur un corps fini $F = \mathbb{F}_q$.
- Les endomorphismes de $\mathscr{A}$ forment un anneau $\mathrm{End}(\mathscr{A})$.
- L'algèbre $K = \mathrm{End}(\mathscr{A}) \otimes \mathbb{Q}$ est un corps de nombres de degré $2g$ (un corps CM).



ALGÈBRE ET ANNEAU DES ENDOMORPHISMES

- Soit $\mathscr{A}$ une variété abélienne ordinaire de dimension g sur un corps fini $F = \mathbb{F}_q$.
- Les endomorphismes de $\mathscr{A}$ forment un anneau $\mathrm{End}(\mathscr{A})$.
- L'algèbre $K = \mathrm{End}(\mathscr{A}) \otimes \mathbb{Q}$ est un corps de nombres de degré $2g$ (un corps CM).
- $\mathrm{End}(\mathscr{A})$ est isomorphe à un ordre $\mathcal{O}$ de K (i.e. un réseau de dimension $2g$ dans K, qui est aussi un sous-anneau).

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

2

K_0

g

$\mathbb{Q}$

CAS DES COURBES ELLIPTIQUES

- Si $\mathscr{A} = E$ est une courbe elliptique, la dimension est $g = 1$.
- K a un **ordre maximal** $\mathcal{O}_K$, l'anneau des entiers de K.
- Tout ordre de K est de la forme

$$\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K,$$

pour un entier positif f, le **conducteur**.

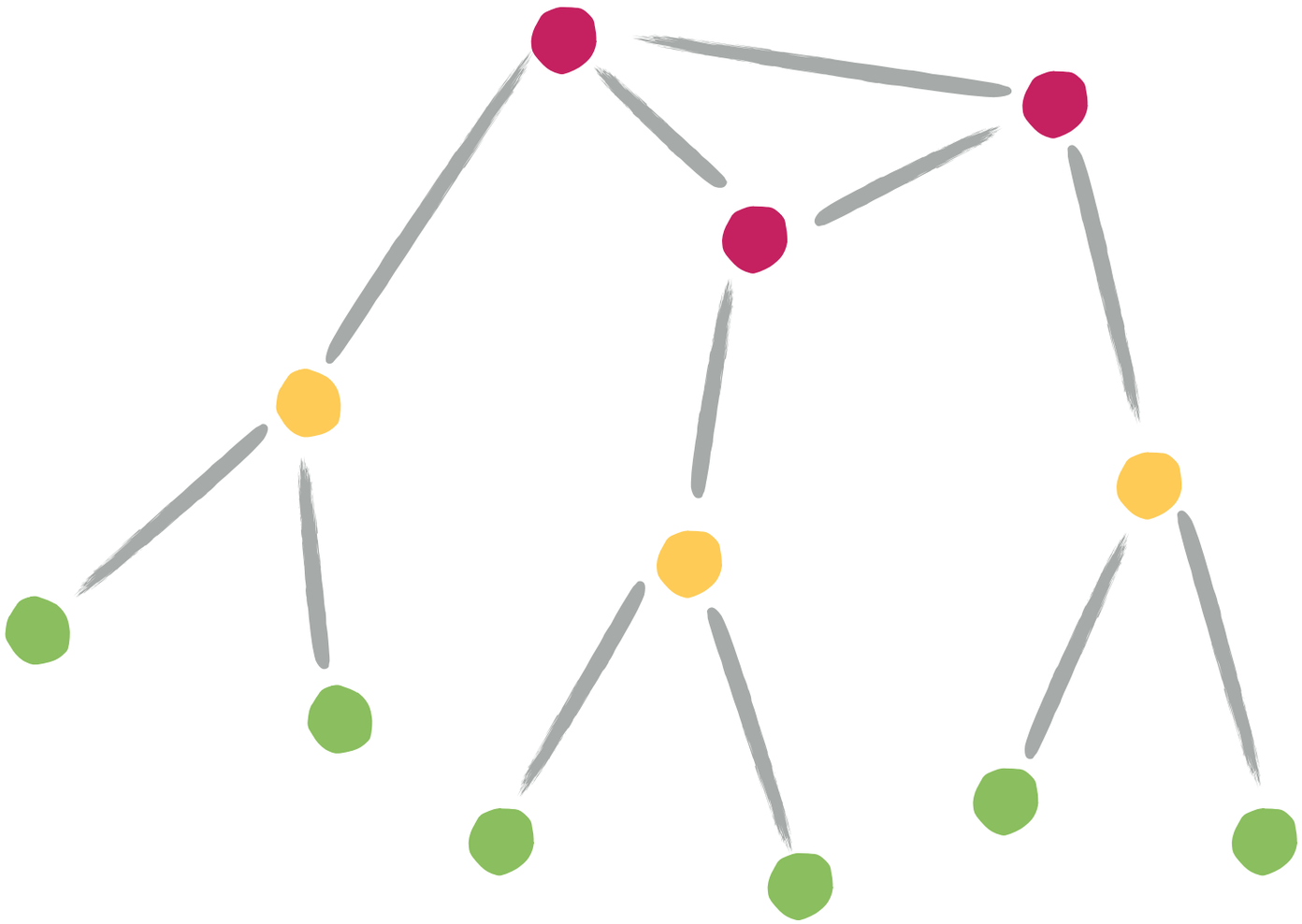
$$K \supset \mathcal{O} \cong \mathrm{End}(E)$$

$$2 \Big| \quad \Big|$$

$$K_0 = \mathbb{Q}$$

CAS DES COURBES ELLIPTIQUES

Les “niveaux” du volcan de ℓ-isogénies disent combien de fois ℓ divise le conducteur. Ici, $(f,\ell) = 1$.



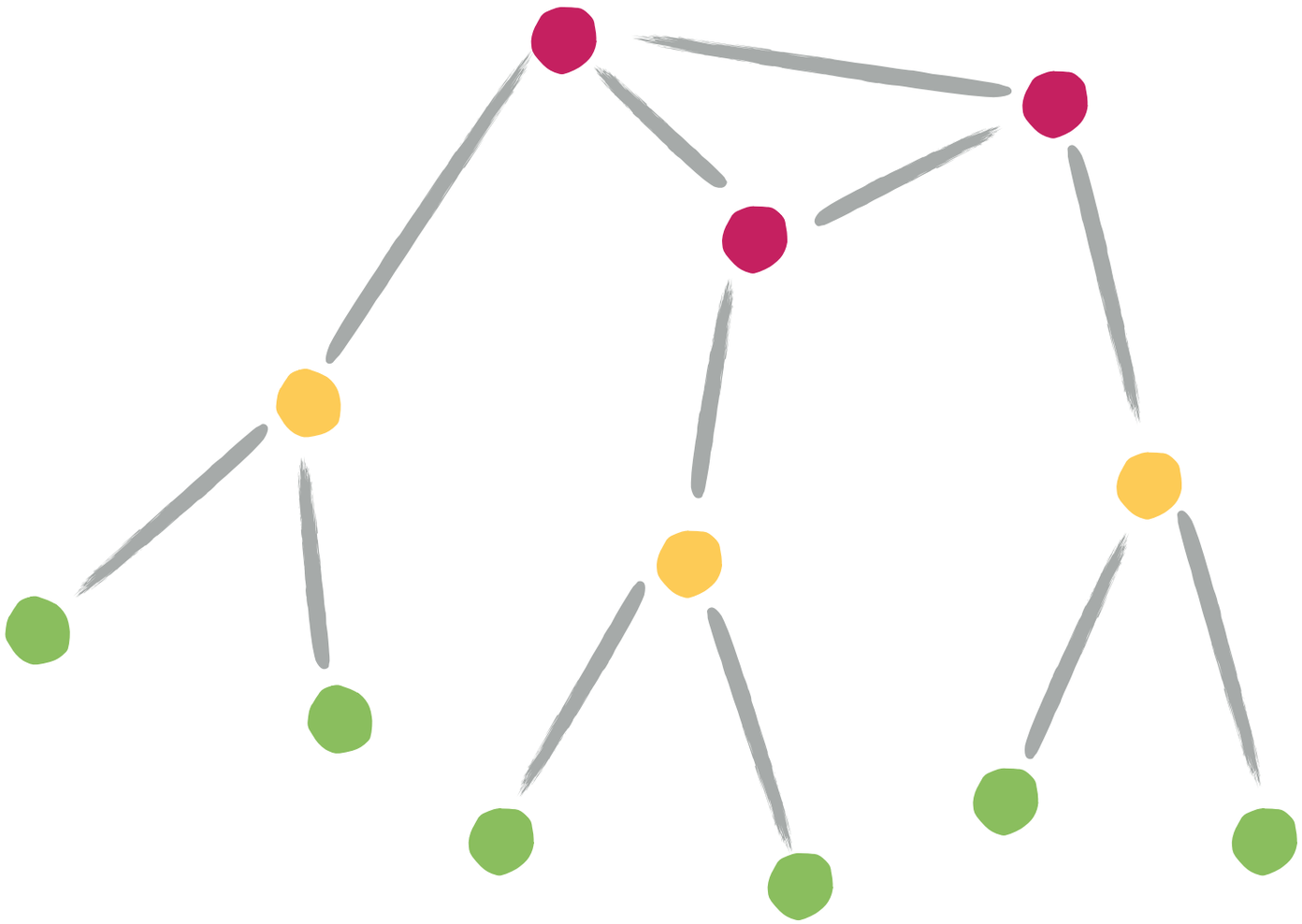
$\mathrm{End} \cong \mathbb{Z} + f\mathcal{O}_K$

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

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

CAS DES COURBES ELLIPTIQUES

Seule une ℓ-isogénie peut changer la valuation en ℓ du conducteur.



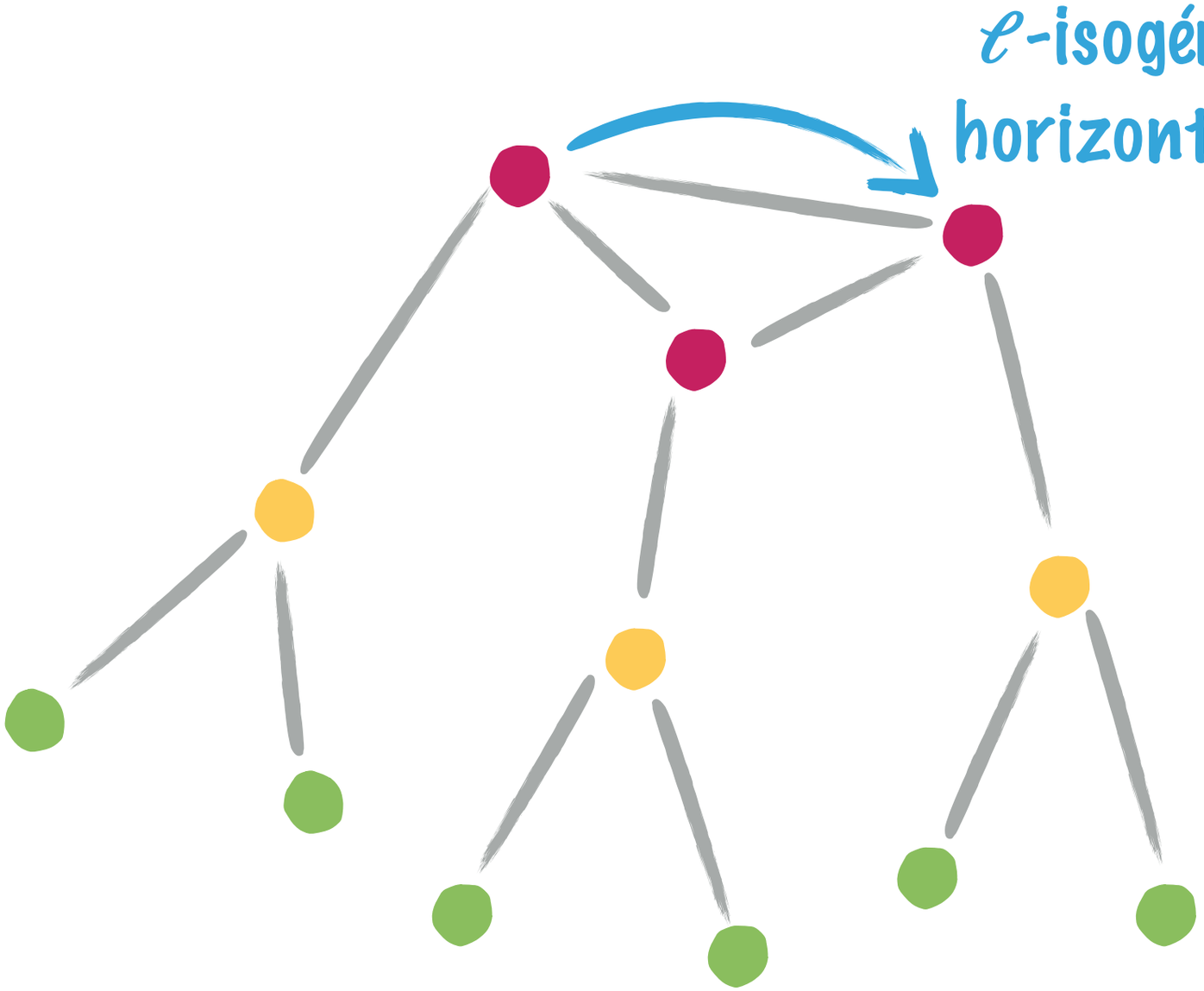
$\mathrm{End} \cong \mathbb{Z} + f\mathcal{O}_K$

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

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

CAS DES COURBES ELLIPTIQUES

Seule une ℓ-isogénie peut changer la valuation en ℓ du conducteur.



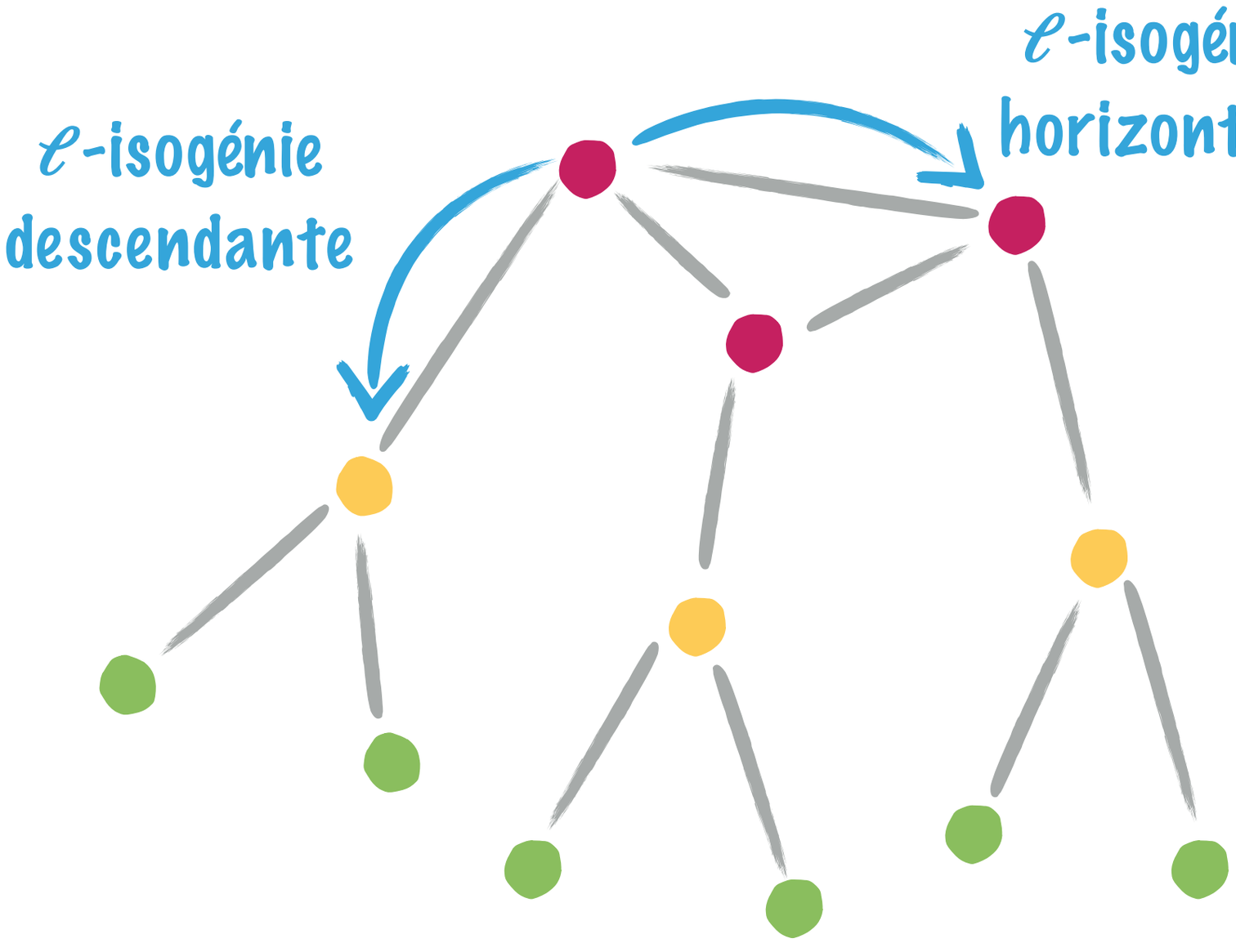
$\mathrm{End} \cong \mathbb{Z} + f\mathcal{O}_K$

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

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

CAS DES COURBES ELLIPTIQUES

Seule une ℓ-isogénie peut changer la valuation en ℓ du conducteur.



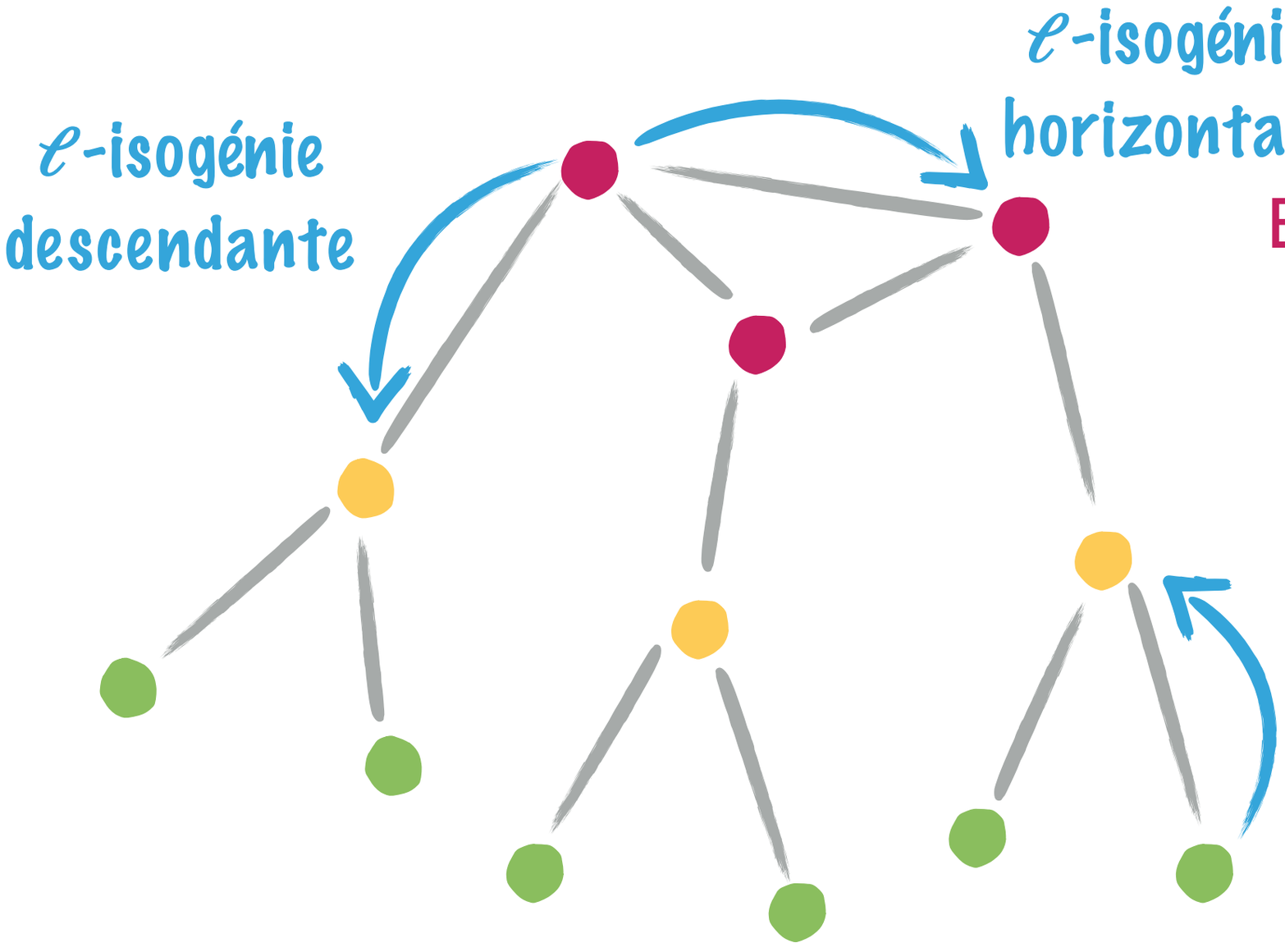
$\mathrm{End} \cong \mathbb{Z} + f\mathcal{O}_K$

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

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

CAS DES COURBES ELLIPTIQUES

Seule une ℓ-isogénie peut changer la valuation en ℓ du conducteur.



CLASSIFICATION DES ORDRES

- Cette classification des ordres dans les corps quadratiques est la clef de la structure de volcan pour les courbes elliptiques.
- Analogue en dimension $g > 1$? Pour tout corps K_0 et extension quadratique K/K_0, on montre que

CLASSIFICATION DES ORDRES

- Cette classification des ordres dans les corps quadratiques est la clef de la structure de volcan pour les courbes elliptiques.
- Analogue en dimension $g > 1$? Pour tout corps K_0 et extension quadratique K/K_0, on montre que

Tout ordre $\mathcal{O}$ de K contenant $\mathcal{O}_{K_0}$ est de la forme

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

pour un idéal $\mathfrak{f}$ de $\mathcal{O}_{K_0}$, le **conducteur** de $\mathcal{O}$.

CLASSIFICATION DES ORDRES

- Cette classification des ordres dans les corps quadratiques est la clef de la structure de volcan pour les courbes elliptiques.
- Analogue en dimension $g > 1$? Pour tout corps K_0 et extension quadratique K/K_0, on montre que

Tout ordre $\mathcal{O}$ de K contenant $\mathcal{O}_{K_0}$ est de la forme

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

pour un idéal $\mathfrak{f}$ de $\mathcal{O}_{K_0}$, le **conducteur** de $\mathcal{O}$.

On regarde en fait ce résultat "localement" en un premier ℓ, c'est-à-dire pour l'algèbre étale $K \otimes \mathbb{Q}_\ell$.

CLASSIFICATION DES ORDRES

Tout ordre $\mathcal{O}$ de K contenant $\mathcal{O}_{K_0}$ est de la forme

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

pour un idéal $\mathfrak{f}$ de $\mathcal{O}_{K_0}$, le **conducteur** de $\mathcal{O}$.

CLASSIFICATION DES ORDRES

Tout ordre $\mathcal{O}$ de K contenant $\mathcal{O}_{K_0}$ est de la forme

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

pour un idéal $\mathfrak{f}$ de $\mathcal{O}_{K_0}$, le **conducteur** de $\mathcal{O}$.

- C'est exactement $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$ lorsque $K_0 = \mathbb{Q}$!

CLASSIFICATION DES ORDRES

Tout ordre $\mathcal{O}$ de K contenant $\mathcal{O}_{K_0}$ est de la forme

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

pour un idéal $\mathfrak{f}$ de $\mathcal{O}_{K_0}$, le **conducteur** de $\mathcal{O}$.

- C'est exactement $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$ lorsque $K_0 = \mathbb{Q}$!
- Lorsque $\mathcal{O}$ contient $\mathcal{O}_{K_0}$, on dit que $\mathcal{O}$ a multiplication réelle (MR) maximale.

CLASSIFICATION DES ORDRES

Tout ordre $\mathcal{O}$ de K contenant $\mathcal{O}_{K_0}$ est de la forme

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

pour un idéal $\mathfrak{f}$ de $\mathcal{O}_{K_0}$, le **conducteur** de $\mathcal{O}$.

- C'est exactement $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$ lorsque $K_0 = \mathbb{Q}$!
- Lorsque $\mathcal{O}$ contient $\mathcal{O}_{K_0}$, on dit que $\mathcal{O}$ a multiplication réelle (MR) maximale.
- Pour $K_0 = \mathbb{Q}$, tous les ordres ont MR maximale, car $\mathcal{O}_{K_0} = \mathbb{Z}$.

DE NOUVEAUX VOLCANS

ℓ-ISOGÉNIES

- Pour une courbe elliptique, le conducteur est un nombre entier *f*, qui se décompose en nombres premiers : on regarde donc des ℓ-isogénies, où ℓ est un nombre premier

ℓ-ISOGÉNIES

- Pour une courbe elliptique, le conducteur est un nombre entier f, qui se décompose en nombres premiers : on regarde donc des ℓ-isogénies, où ℓ est un nombre premier
- Pour $g > 1$ et MR maximale, le conducteur est un idéal $\mathfrak{f}$ de $\mathcal{O}_{K_0}$, et se décompose en idéaux premiers…

$\mathfrak{l}$-ISOGÉNIES

- Pour une courbe elliptique, le conducteur est un nombre entier f, qui se décompose en nombres premiers : on regarde donc des ℓ-isogénies, où ℓ est un nombre premier
- Pour $g > 1$ et MR maximale, le conducteur est un idéal $\mathfrak{f}$ de $\mathcal{O}_{K_0}$, et se décompose en idéaux premiers…
- Notion de $\mathfrak{l}$-isogénie, où $\mathfrak{l}$ est un idéal premier de $\mathcal{O}_{K_0}$?

$\mathfrak{l}$-ISOGÉNIES

- Pour une courbe elliptique, le conducteur est un nombre entier f, qui se décompose en nombres premiers : on regarde donc des ℓ-isogénies, où ℓ est un nombre premier
- Pour $g > 1$ et MR maximale, le conducteur est un idéal $\mathfrak{f}$ de $\mathcal{O}_{K_0}$, et se décompose en idéaux premiers…
- Notion de $\mathfrak{l}$-isogénie, où $\mathfrak{l}$ est un idéal premier de $\mathcal{O}_{K_0}$?

> Une $\mathfrak{l}$-isogénie depuis $\mathcal{A}$ est une isogénie dont le noyau est un $\mathcal{O}_{K_0}$-sous-module cyclique de $\mathcal{A}[\mathfrak{l}]$.

Seule une $\mathfrak{l}$-isogénie peut changer la valuation en $\mathfrak{l}$ du conducteur.

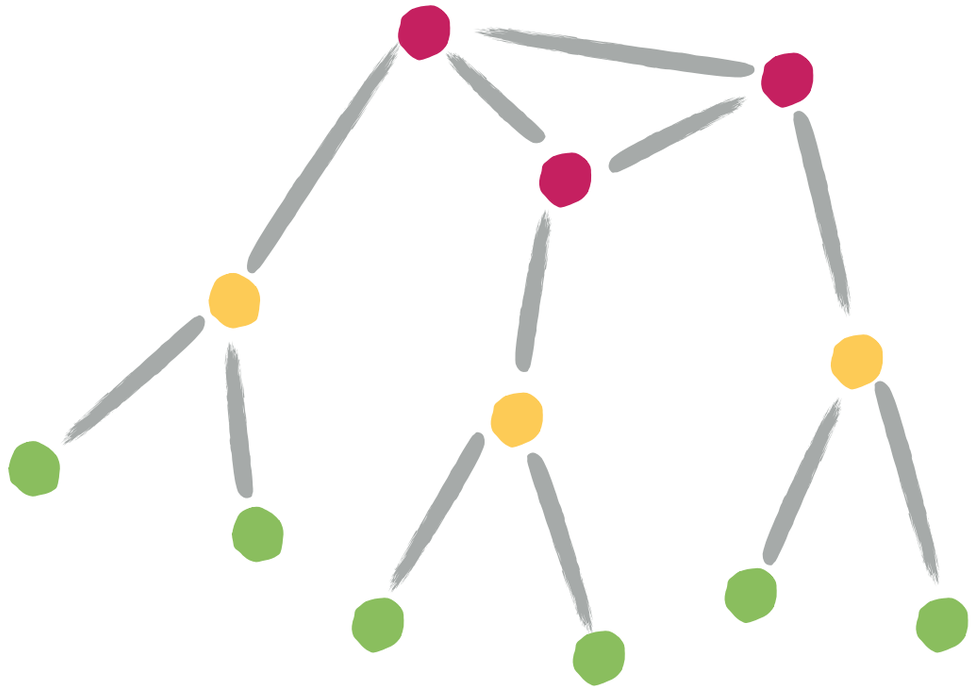
DE NOUVEAU DES VOLCANS?

Si $\mathscr{A}$ a MR maximale (localement en ℓ), et $\mathfrak{I}$ est un ideal premier de $\mathcal{O}_{K_0}$ au dessus de ℓ, alors le graphe des $\mathfrak{I}$-isogénies est-il un volcan ?

DE NOUVEAU DES VOLCANS?

Si $\mathscr{A}$ a MR maximale (localement en ℓ), et $\mathfrak{I}$ est un ideal premier de $\mathcal{O}_{K_0}$ au dessus de ℓ, alors le graphe des $\mathfrak{I}$-isogénies est-il un volcan ?

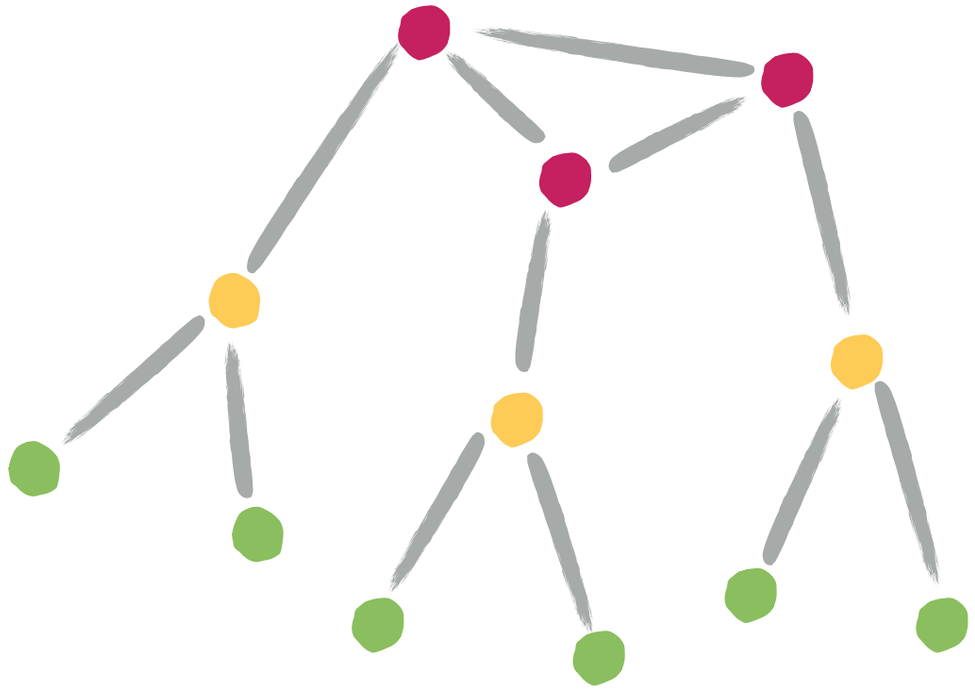
Théorème: oui !... du moins si $\mathfrak{I}$ est principal, et que toutes les unités de $\mathcal{O}_K$ sont totalement réelles!



DE NOUVEAU DES VOLCANS?

Si $\mathscr{A}$ a MR maximale (localement en ℓ), et $\mathfrak{I}$ est un ideal premier de $\mathcal{O}_{K_0}$ au dessus de ℓ, alors le graphe des $\mathfrak{I}$-isogénies est-il un volcan ?

Théorème: oui !... du moins si $\mathfrak{I}$ est principal, et que toutes les unités de $\mathcal{O}_K$ sont totalement réelles!



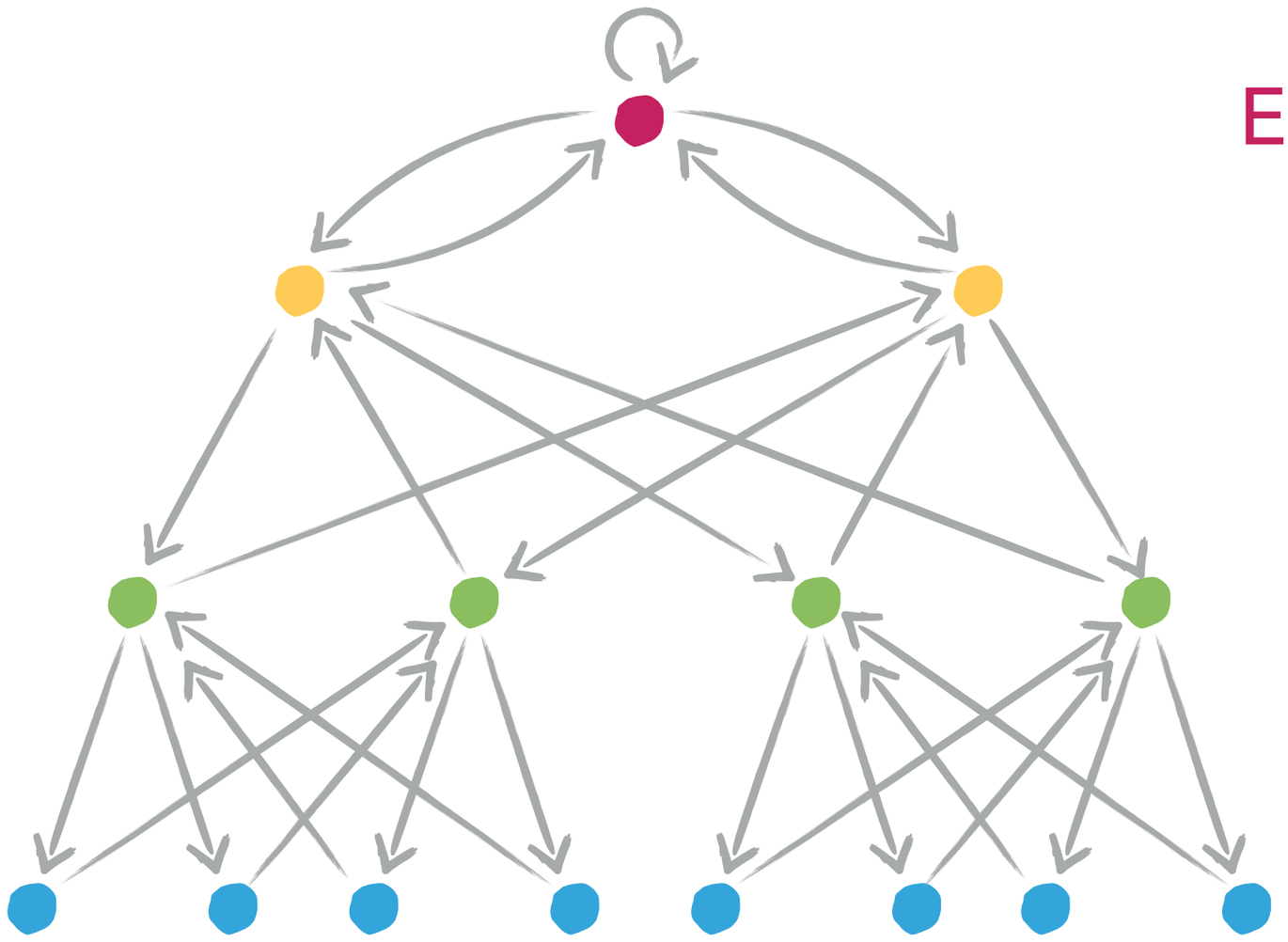
End $\cong \mathcal{O}_{K_0} + \mathfrak{f}\mathcal{O}_K$

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

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

DE NOUVEAU DES VOLCANS?

Si $\mathfrak{I}$ n'est pas principal ? Le graphe est orienté !



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

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

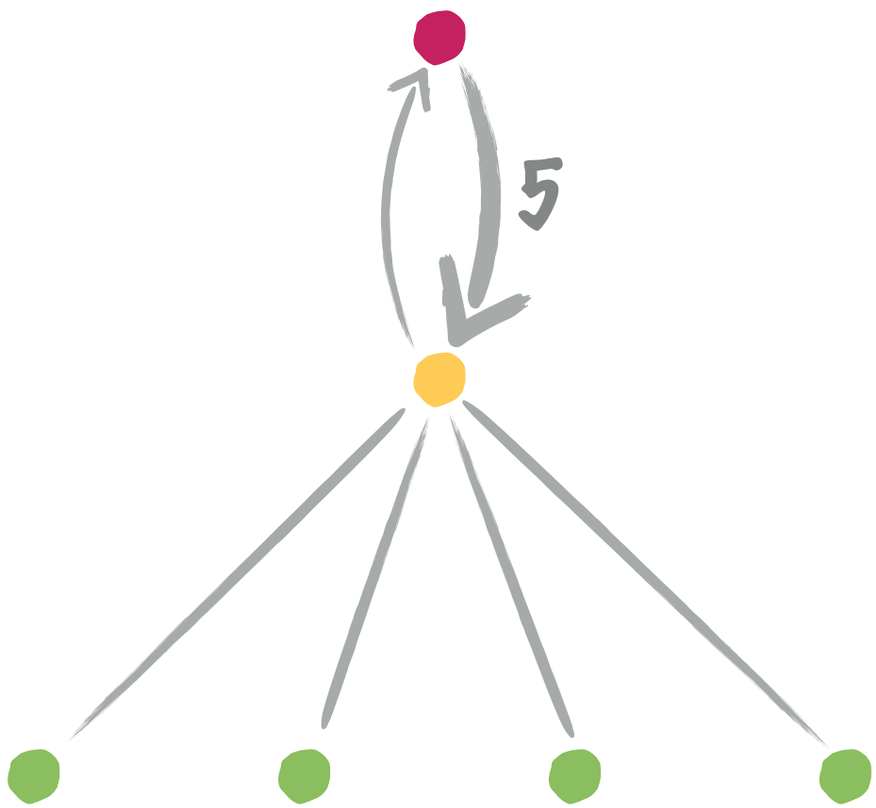
$\mathrm{End} \cong \mathcal{O}_{K0} + \mathfrak{I}^2\mathfrak{f}\mathcal{O}_K$

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

DE NOUVEAU DES VOLCANS?

Si $\mathcal{O}_K$ a des unités complexes ? Des multiplicités apparaissent

Regardons $K = \mathbb{Q}(\zeta_5)$, $K_0 = \mathbb{Q}\left(\zeta_5 + \zeta_5^{-1}\right)$, et $\mathfrak{I} = 2\mathcal{O}_{K_0}$.



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

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

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

EN DIMENSION 2

(ℓ,ℓ)-ISOGÉNIES

(ℓ,ℓ)-ISOGÉNIES

- Soit $\mathscr{A}$ une surface abélienne ordinaire principalement polarisée.
- Une (ℓ,ℓ)-isogénie est une isogénie $\mathscr{A} \to \mathscr{B}$ dont le noyau est un sous-groupe maximal isotrope de $\mathscr{A}[\ell]$ pour le pairing de Weil.
- Les (ℓ,ℓ)-isogénies sont les plus faciles à calculer! Bien plus efficace que les $\mathfrak{l}$-isogénies...

(ℓ,ℓ)-ISOGÉNIES

On montre que les (ℓ,ℓ)-isogénies préservant la MR maximale sont exactement:

(ℓ,ℓ)-ISOGÉNIES

On montre que les (ℓ,ℓ)-isogénies préservant la MR maximale sont exactement:

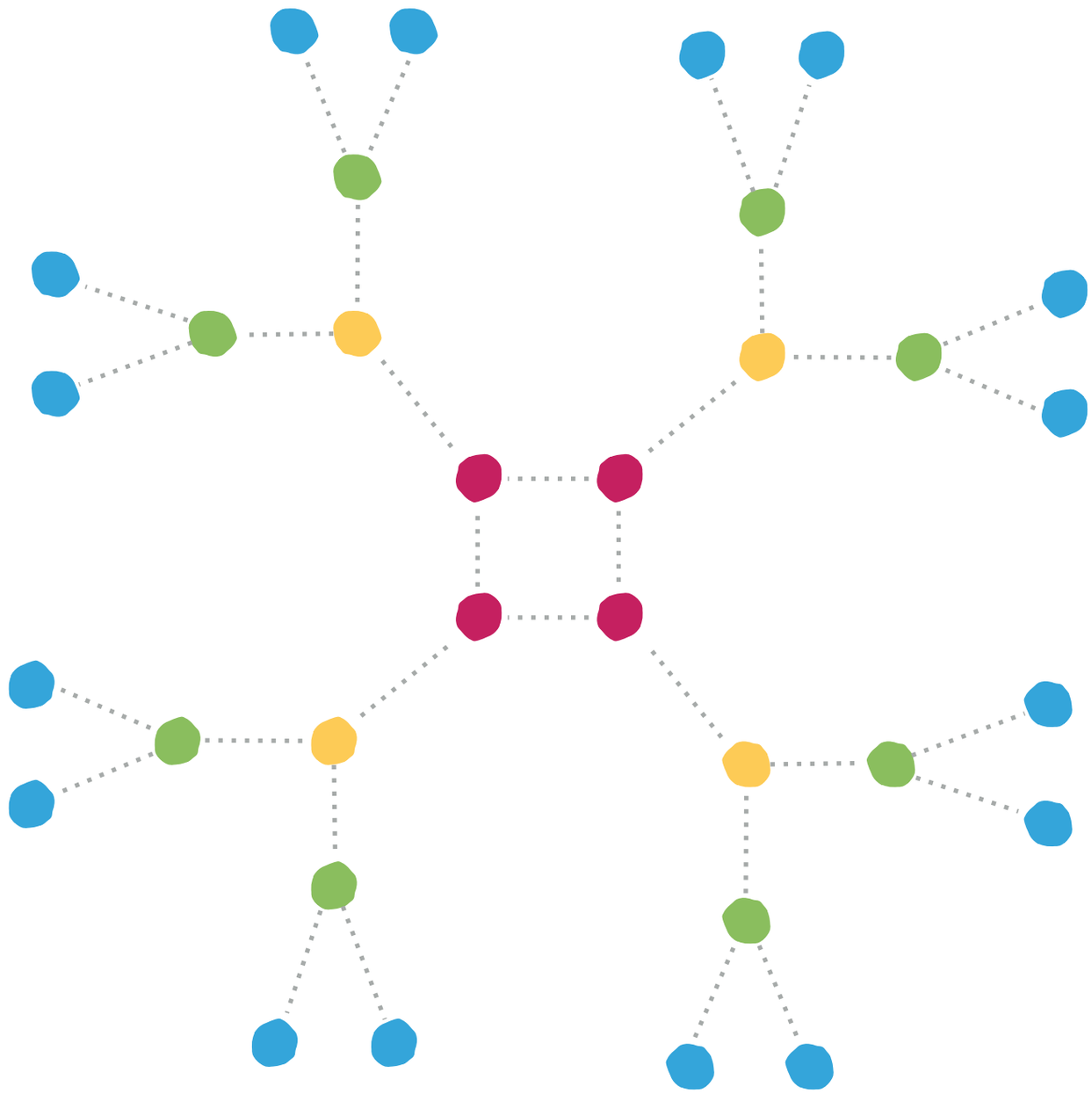
- Les $\mathfrak{I}$-isogénies si ℓ est inerte dans K_0 (i.e., $\mathfrak{I} = \ell\mathcal{O}_{K_0}$)

(ℓ,ℓ)-ISOGÉNIES

On montre que les (ℓ,ℓ)-isogénies préservant la MR maximale sont exactement:

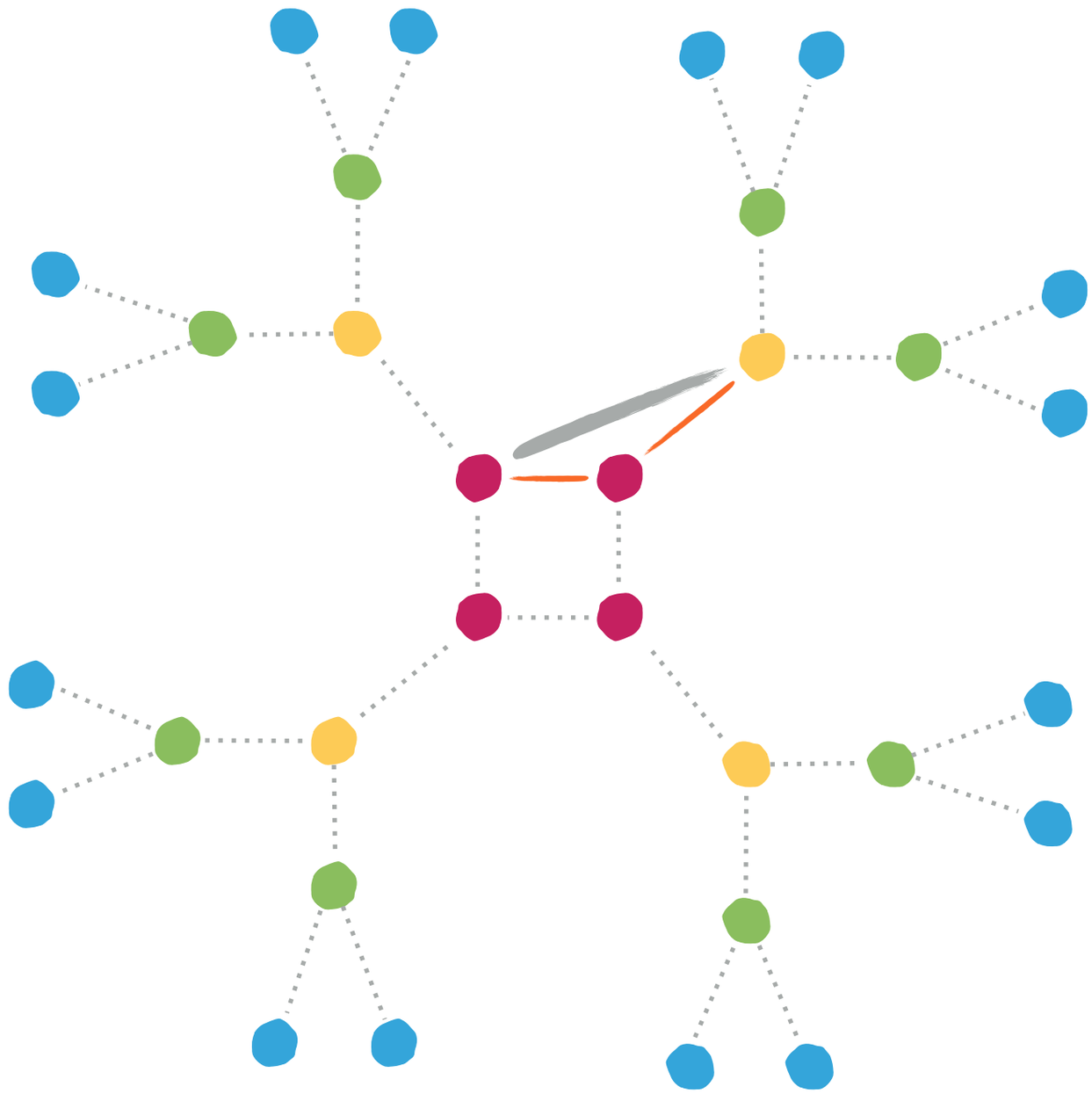
- Les $\mathfrak{I}$-isogénies si ℓ est inerte dans K_0 (i.e., $\mathfrak{I} = \ell\mathcal{O}_{K_0}$)
- Les compositions d'une $\mathfrak{I}_1$-isogénie avec une $\mathfrak{I}_2$-isogénie si ℓ se sépare ou se ramifie en $\ell\mathcal{O}_{K_0} = \mathfrak{I}_1\mathfrak{I}_2$.

GRAPHES DE (ℓ,ℓ)-ISOGÉNIES PRÉSERVANT LA MR



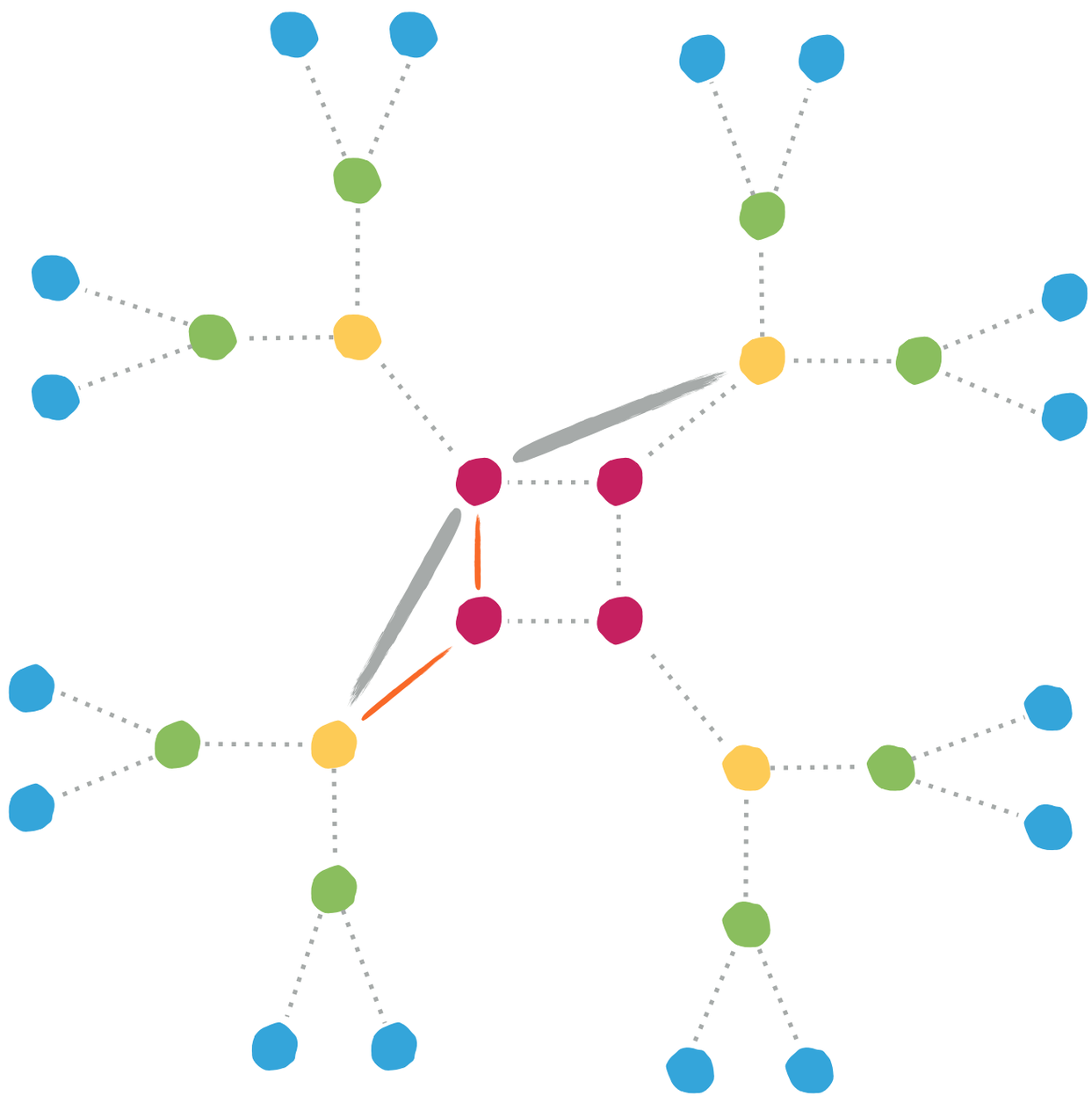
Supposons $\ell \mathcal{O}_{K_0} = I^2$

GRAPHES DE (ℓ,ℓ)-ISOGÉNIES PRÉSERVANT LA MR



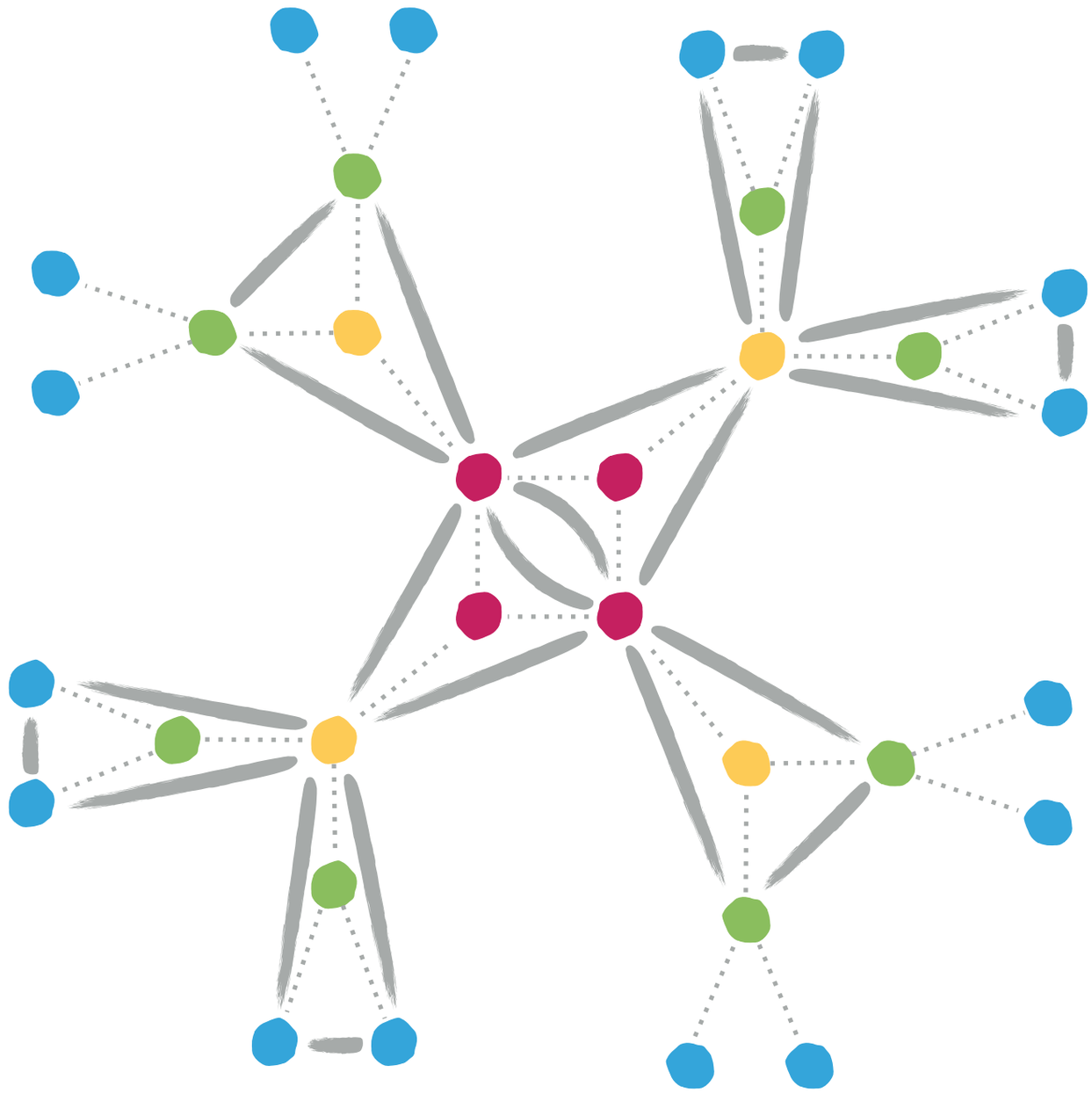
Supposons $\ell \mathcal{O}_{K_0} = \mathfrak{l}^2$

GRAPHES DE (ℓ,ℓ)-ISOGÉNIES PRÉSERVANT LA MR



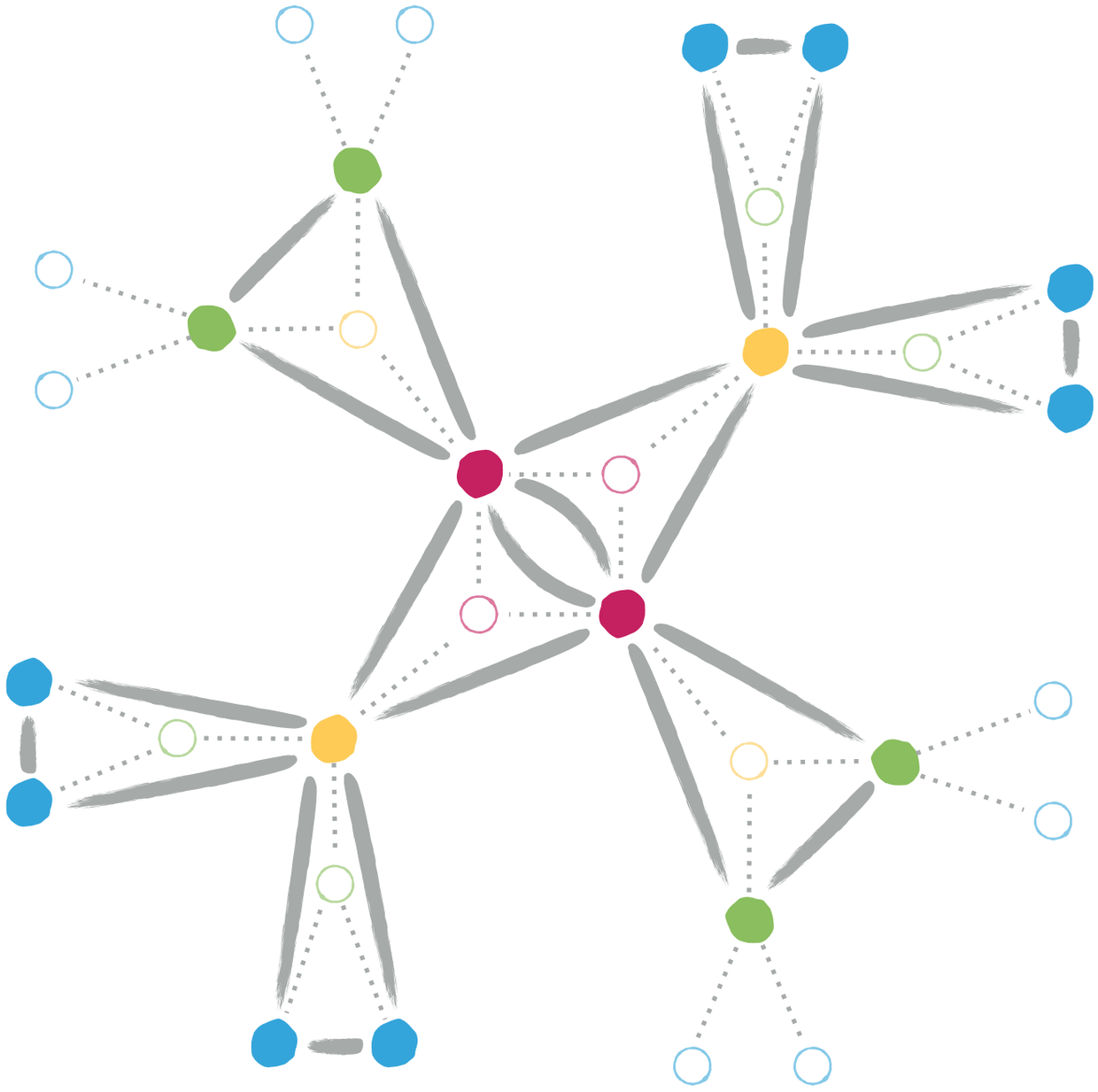
Supposons $\ell \mathcal{O}_{K_0} = I^2$

GRAPHES DE (ℓ,ℓ)-ISOGÉNIES PRÉSERVANT LA MR



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

GRAPHES DE (ℓ,ℓ)-ISOGÉNIES PRÉSERVANT LA MR



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

ET AVEC ÇA ?

- On a décrit la structure des graphes de (ℓ,ℓ)-isogénies préservant la MR maximale.
- Il est aussi intéressant de regarder les (ℓ,ℓ)-isogénies qui changent la MR. On peut décrire ce graphe localement.
- En particulier, si la MR n'est pas maximale, on montre qu'il y a toujours une (ℓ,ℓ)-isogénie qui augmente la MR.
- Une première application : on utilise ces résultats pour décrire un algorithme cherchant une suite de (ℓ,ℓ)-isogénies vers une variété dont l'anneau des endomorphisme est maximal.

TECHNIQUES

RÉSEAUX ℓ-ADIQUES ET MULTIPLICATION COMPLEXE

MODULE DE TATE ET RÉSEAUX

- Le module de Tate $T = T_\ell(\mathscr{A})$ de la variété abélienne $\mathscr{A}$ est un réseau dans le $\mathbb{Q}_\ell$-espace vectoriel $V = T \otimes \mathbb{Q}_\ell$.

MODULE DE TATE ET RÉSEAUX

- Le module de Tate $T = T_\ell(\mathscr{A})$ de la variété abélienne $\mathscr{A}$ est un réseau dans le $\mathbb{Q}_\ell$-espace vectoriel $V = T \otimes \mathbb{Q}_\ell$.

- Il y a une correspondance bijective :

$$\{\text{réseaux dans } V \text{ contenant } T\} \leftrightarrow \{\text{sous-groupes finis de } \mathscr{A}[\ell^\infty]\}$$

MODULE DE TATE ET RÉSEAUX

- Le module de Tate $T = T_\ell(\mathscr{A})$ de la variété abélienne $\mathscr{A}$ est un réseau dans le $\mathbb{Q}_\ell$-espace vectoriel $V = T \otimes \mathbb{Q}_\ell$.
- Il y a une correspondance bijective :

{réseaux dans V contenant T} $\leftrightarrow$ {sous-groupes finis de $\mathscr{A}[\ell^\infty]$}

- $\mathrm{End}(\mathscr{A})$ agit sur T, et $K_\ell = \mathrm{End}(\mathscr{A}) \otimes \mathbb{Q}_\ell$ agit sur V.

MODULE DE TATE ET RÉSEAUX

- Le module de Tate $T = T_\ell(\mathscr{A})$ de la variété abélienne $\mathscr{A}$ est un réseau dans le $\mathbb{Q}_\ell$-espace vectoriel $V = T \otimes \mathbb{Q}_\ell$.

- Il y a une correspondance bijective :

{réseaux dans V contenant T} $\leftrightarrow$ {sous-groupes finis de $\mathscr{A}[\ell^\infty]$}

- $\mathrm{End}(\mathscr{A})$ agit sur T, et $K_\ell = \mathrm{End}(\mathscr{A}) \otimes \mathbb{Q}_\ell$ agit sur V.

- Si L est un réseau dans V contenant T, l'ensemble des éléments de K_ℓ préservant L est un ordre de K_ℓ, noté $\mathcal{O}(L)$.

MODULE DE TATE ET RÉSEAUX

- Le module de Tate $T = T_\ell(\mathscr{A})$ de la variété abélienne $\mathscr{A}$ est un réseau dans le $\mathbb{Q}_\ell$-espace vectoriel $V = T \otimes \mathbb{Q}_\ell$.

- Il y a une correspondance bijective :

{réseaux dans V contenant T} $\leftrightarrow$ {sous-groupes finis de $\mathscr{A}[\ell^\infty]$}

- $\mathrm{End}(\mathscr{A})$ agit sur T, et $K_\ell = \mathrm{End}(\mathscr{A}) \otimes \mathbb{Q}_\ell$ agit sur V.

- Si L est un réseau dans V contenant T, l'ensemble des éléments de K_ℓ préservant L est un ordre de K_ℓ, noté $\mathcal{O}(L)$.

- Si L correspond au sous-groupe G, alors $\mathcal{O}(L) \cong \mathrm{End}(\mathscr{A}/G)$.

RECHERCHE DE POINTS FIXES

{réseaux dans V contenant T} $\leftrightarrow$ {sous-groupes finis de $\mathscr{A}[\ell^\infty]$}

RECHERCHE DE POINTS FIXES

{réseaux dans V contenant T} $\leftrightarrow$ {sous-groupes finis de $\mathscr{A}[\ell^\infty]$}

$\cup$

{noyaux de $\mathfrak{l}$-isogénies}

RECHERCHE DE POINTS FIXES

$$\{\text{réseaux dans } V \text{ contenant } T\} \leftrightarrow \{\text{sous-groupes finis de } \mathscr{A}[\ell^\infty]\}$$

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

$$\left\{\begin{array}{c}\text{réseaux } L \text{ tels que } T \subset L \subset \mathfrak{I}^{-1}T \\ \text{et } L/T \text{ est un } \mathcal{O}_{K_0}/\mathfrak{I}\text{-sous-esp.} \\ \text{vect. de rang 1 de } \mathfrak{I}^{-1}T/T\end{array}\right\} \leftrightarrow \{\text{noyaux de } \mathfrak{I}\text{-isogénies}\}$$

- $F = \mathcal{O}_{K_0}/\mathfrak{I}$ est un corps fini, et $\mathfrak{I}^{-1}T/T$ un F-esp. vect. de dim. 2

RECHERCHE DE POINTS FIXES

$$\{\text{réseaux dans } V \text{ contenant } T\} \leftrightarrow \{\text{sous-groupes finis de } \mathscr{A}[\ell^\infty]\}$$

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

$$\left\{\begin{array}{c}\text{réseaux } L \text{ tels que } T \subset L \subset \mathfrak{l}^{-1}T \\ \text{et } L/T \text{ est un } \mathcal{O}_{K_0}/\mathfrak{l}\text{-sous-esp.} \\ \text{vect. de rang 1 de } \mathfrak{l}^{-1}T/T\end{array}\right\} \leftrightarrow \{\text{noyaux de } \mathfrak{l}\text{-isogénies}\}$$

- $F = \mathcal{O}_{K_0}/\mathfrak{l}$ est un corps fini, et $\mathfrak{l}^{-1}T/T$ un F-esp. vect. de dim. 2
- On étudie les droites dans cet espace vectoriel:

$$\mathbb{P}^1(T/\mathfrak{l}T) \quad \leftrightarrow \quad \{\text{noyaux de } \mathfrak{l}\text{-isogénies}\}$$

RECHERCHE DE POINTS FIXES

$$\{\text{réseaux dans } V \text{ contenant } T\} \leftrightarrow \{\text{sous-groupes finis de } \mathscr{A}[\ell^\infty]\}$$

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

$$\left\{\begin{array}{c}\text{réseaux } L \text{ tels que } T \subset L \subset \mathfrak{l}^{-1}T \\ \text{et } L/T \text{ est un } \mathcal{O}_{K_0}/\mathfrak{l}\text{-sous-esp.} \\ \text{vect. de rang 1 de } \mathfrak{l}^{-1}T/T\end{array}\right\} \leftrightarrow \{\text{noyaux de } \mathfrak{l}\text{-isogénies}\}$$

- $F = \mathcal{O}_{K_0}/\mathfrak{l}$ est un corps fini, et $\mathfrak{l}^{-1}T/T$ un F-esp. vect. de dim. 2
- On étudie les droites dans cet espace vectoriel:

$$\mathbb{P}^1(T/\mathfrak{l}T) \quad \leftrightarrow \quad \{\text{noyaux de } \mathfrak{l}\text{-isogénies}\}$$

- $\mathcal{O}(T)^\times = \mathrm{End}(\mathscr{A})^\times$ agit sur $\mathbb{P}^1(T/\mathfrak{l}T)$, et les points fixes correspondent aux isogénies montantes ou horizontales !

EPFL, Lausanne, Switzerland

E. Hunter Brooks Dimitar Jetchev Benjamin Wesolowski

GRAPHES D'ISOGÉNIES DE VARIÉTÉS ABÉLIENNES ORDINAIRES

Aux Journées Codage et Cryptographie 2017, La Bresse