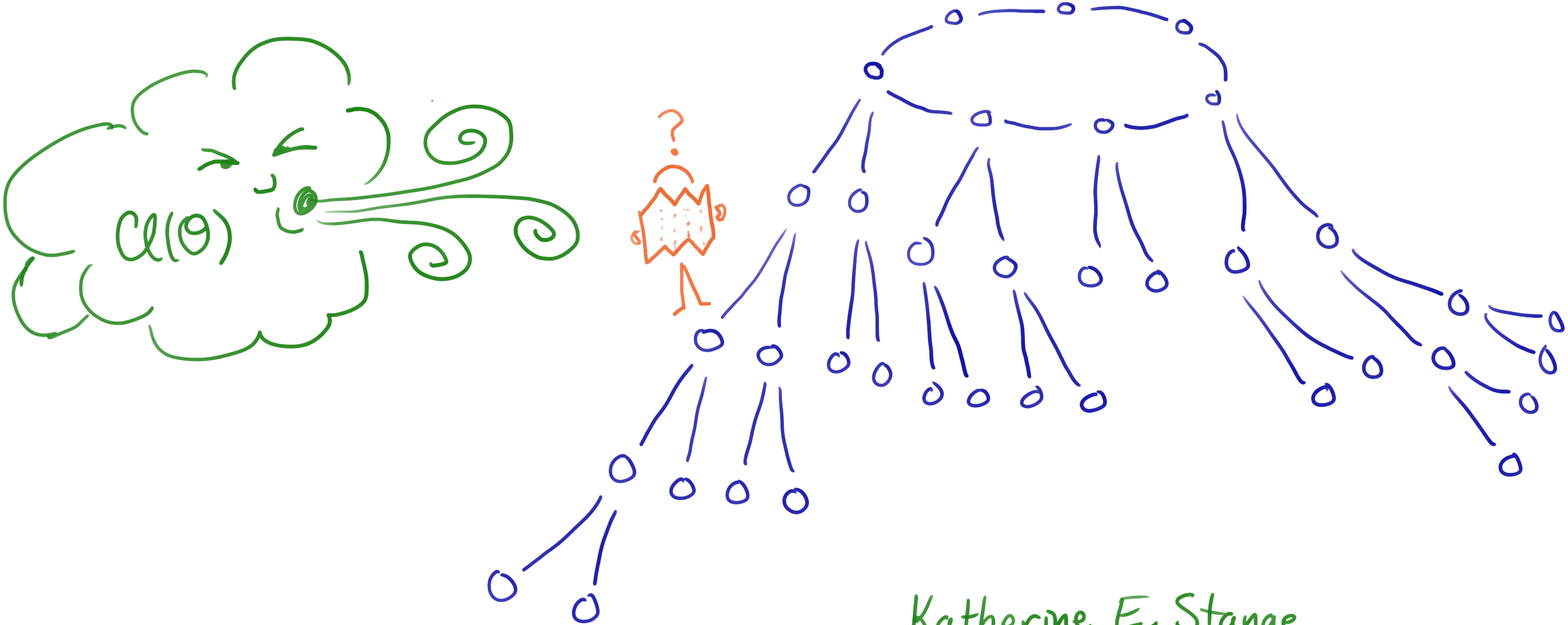
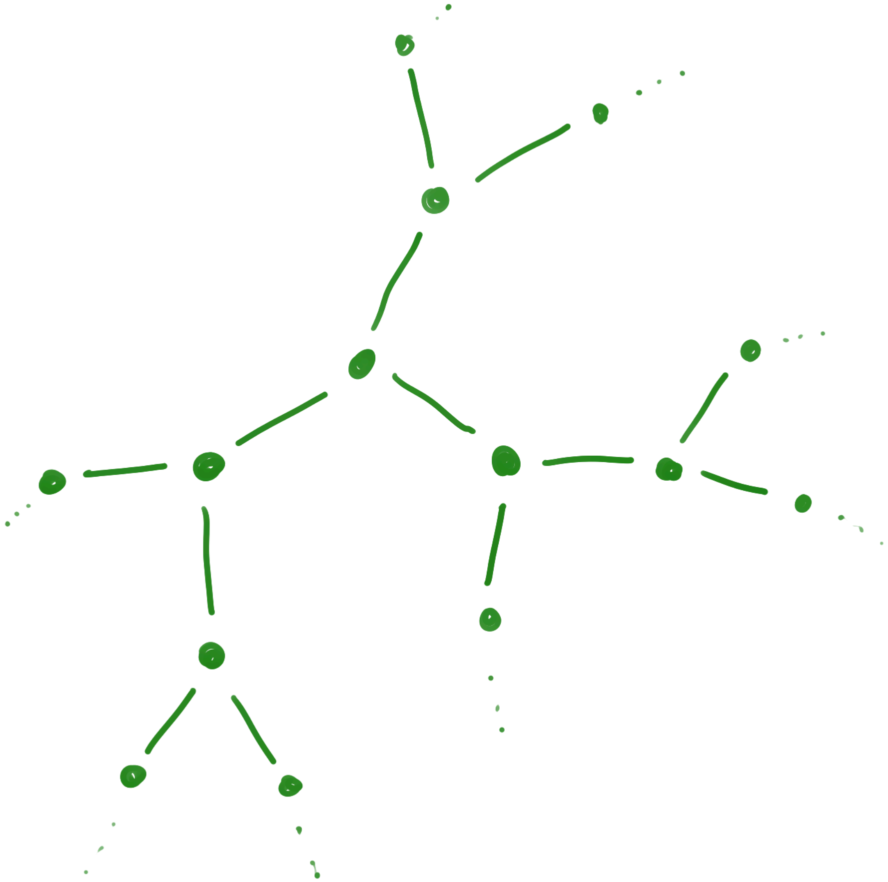
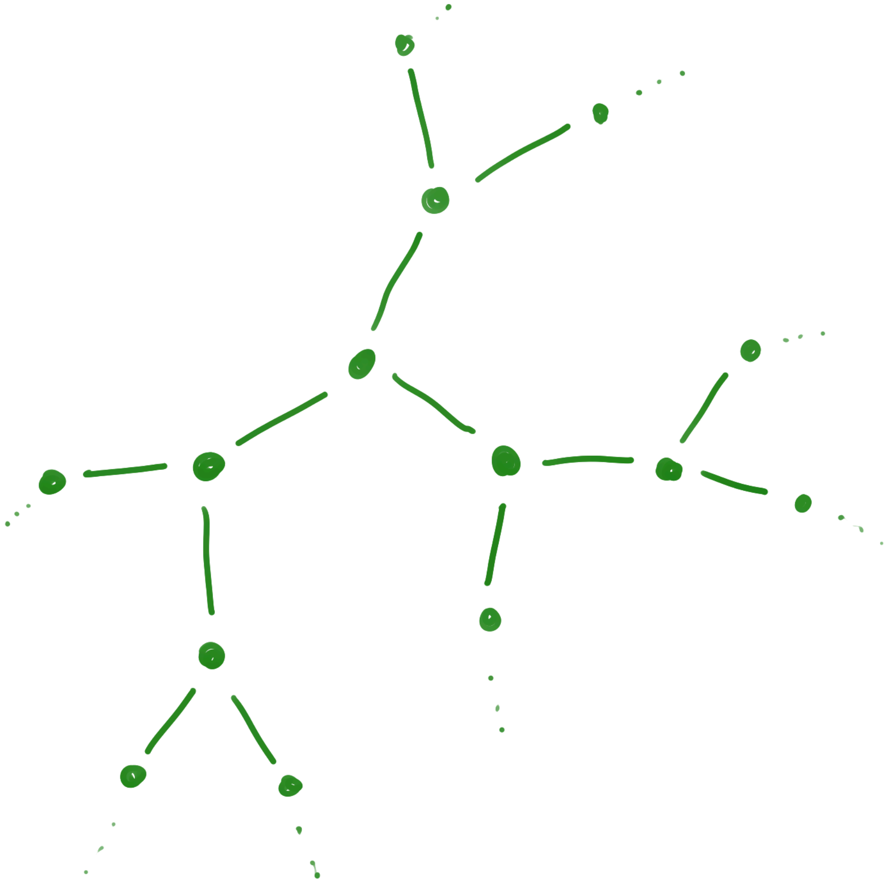
Orienteering on isogeny volcanoes

joint with Sarah Arpin, Mingjie Chen,
Kristin E. Lauter, Renate Scheidler,
Ha T. N. Tran



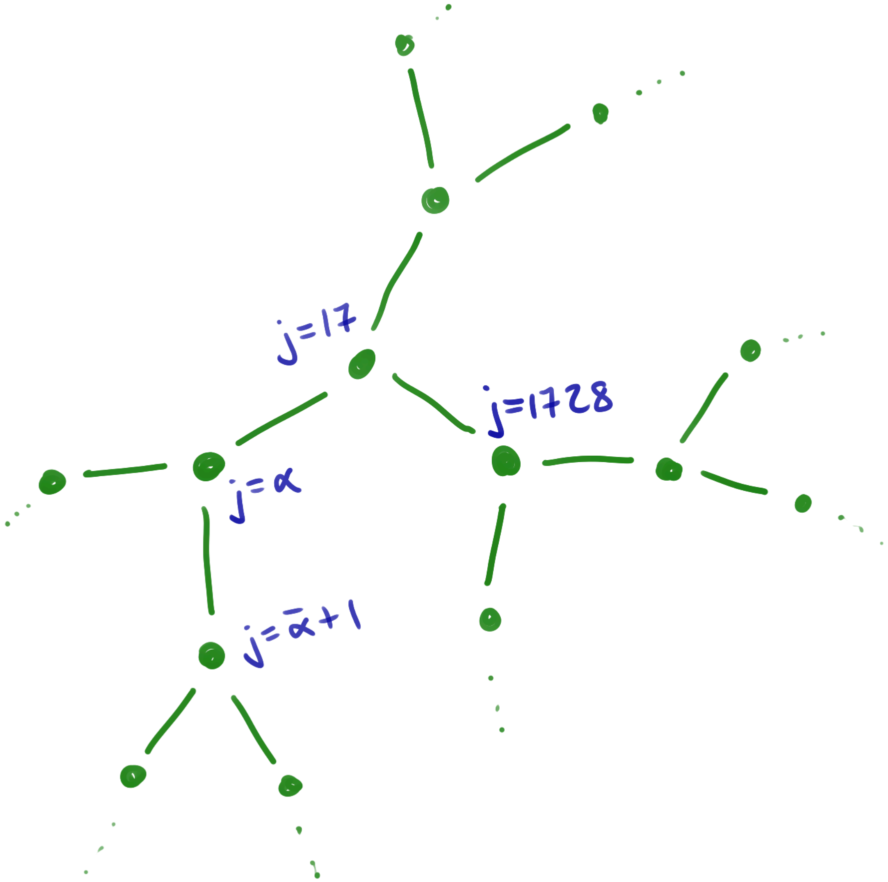
Katherine E. Stange
University of Colorado Boulder





ℓ-isogeny graph

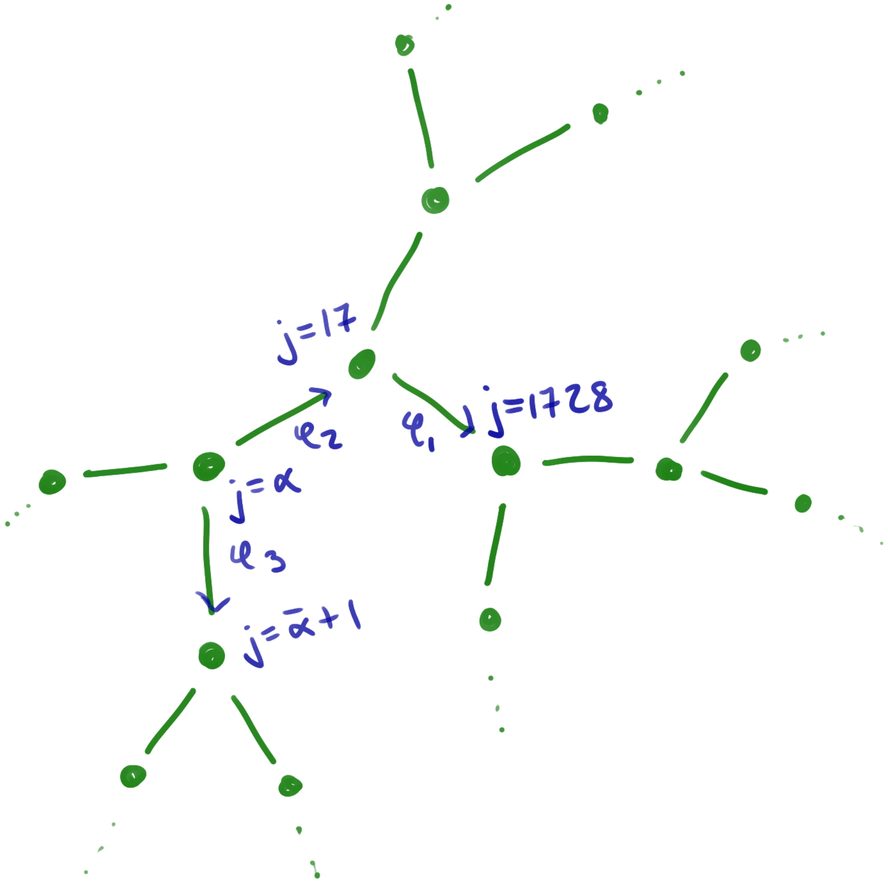
ℓ = small prime



ℓ-isogeny graph

ℓ = small prime
p = large prime

vertices = elliptic curves $/\overline{\mathbb{F}}_p$ up to isom.

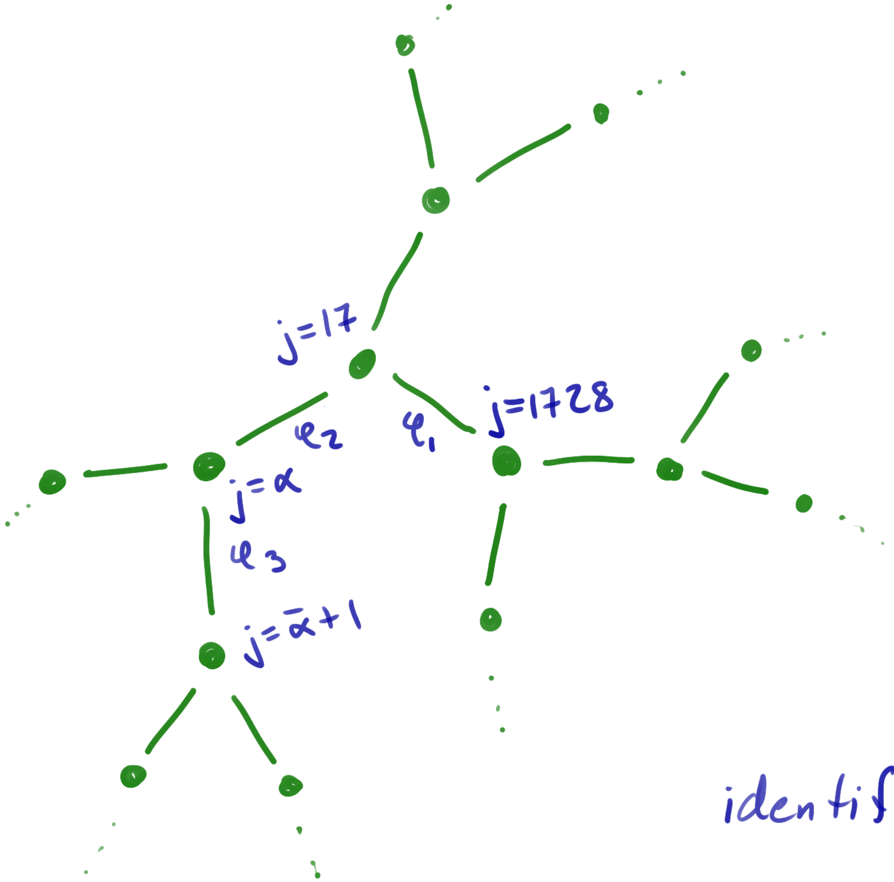


ℓ-isogeny graph

ℓ = small prime
p = large prime

vertices = elliptic curves $/\overline{\mathbb{F}_p}$ up to isom.

edges = isogenies of degree ℓ up to equiv. ✱



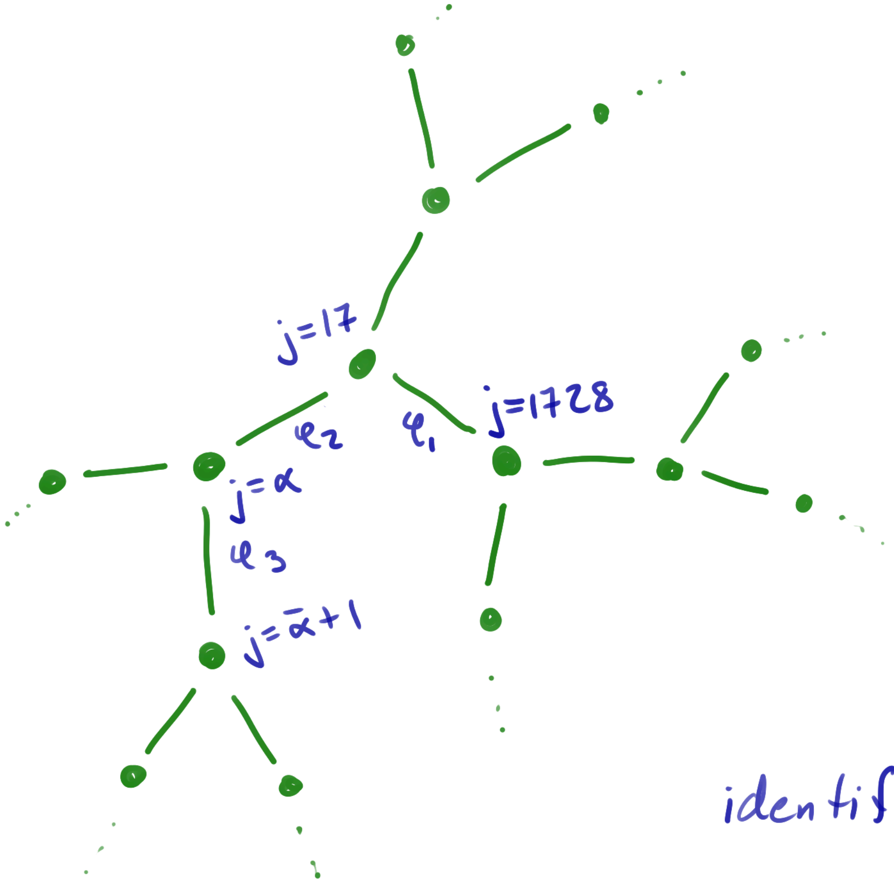
ℓ-isogeny graph

vertices = elliptic curves $/\overline{\mathbb{F}_p}$ up to isom.

edges = isogenies of degree ℓ up to equiv.

identifying φ with $\hat{\varphi}$ gives an undirected $(\ell+1)$-regular graph

$$\begin{tikzcd}\bullet \arrow[r, shift left, "\varphi"] & \bullet \arrow[l, shift left, "\hat{\varphi}"]\end{tikzcd}$$



ℓ-isogeny graph

vertices = elliptic curves $/\overline{\mathbb{F}_p}$ up to isom.

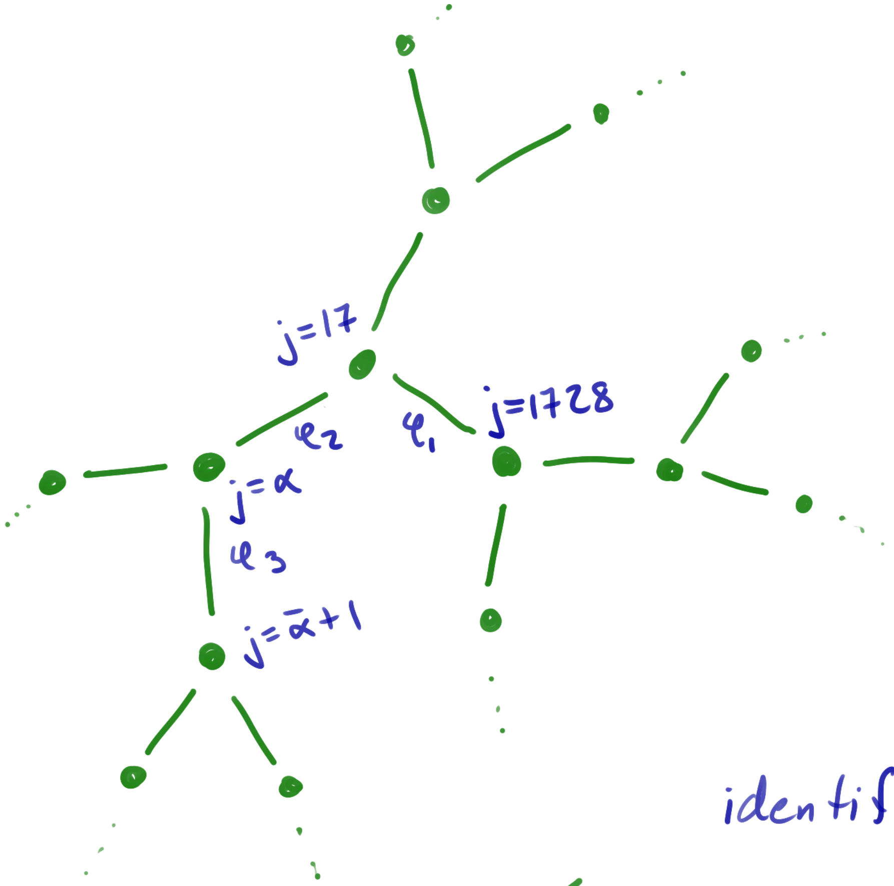
edges = isogenies of degree ℓ up to equiv.

identifying φ with $\hat{\varphi}$ gives an undirected $(\ell+1)$-regular graph

(except near j=0, 1728)

$$\begin{tikzcd} \bullet \arrow[r, shift left, "\varphi"] & \bullet \arrow[l, shift left, "\hat{\varphi}"] \end{tikzcd}$$

ℓ-isogeny graph



vertices = elliptic curves $/\overline{\mathbb{F}_p}$ up to isom.

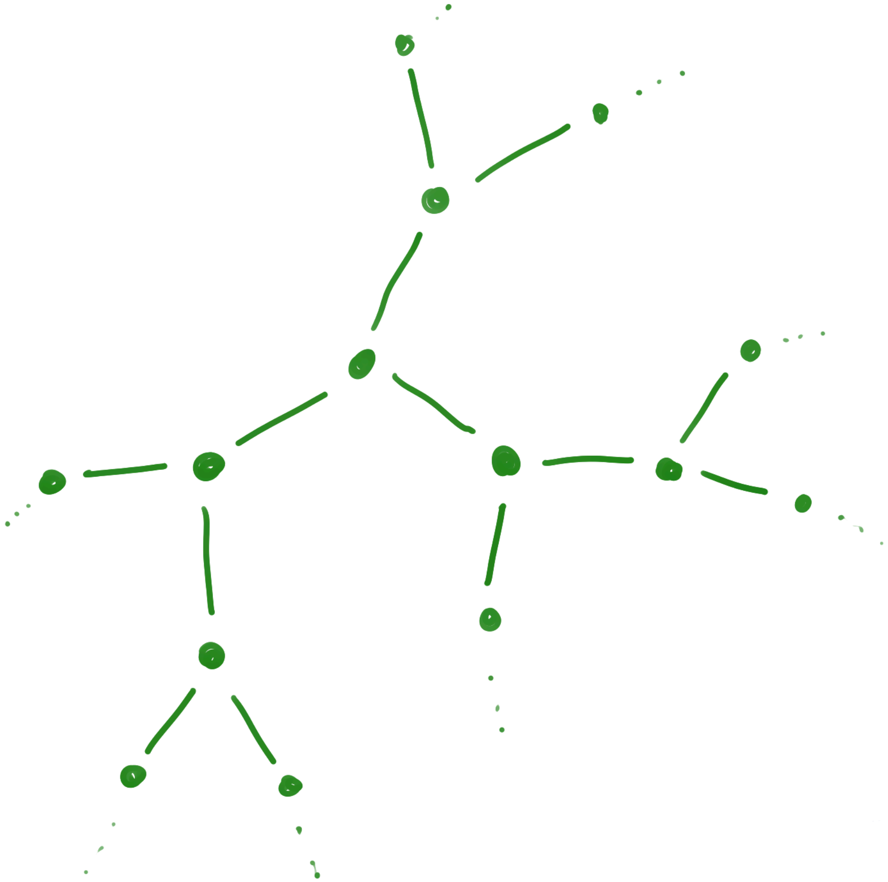
edges = isogenies of degree ℓ up to equiv.

identifying φ with $\hat{\varphi}$ gives an undirected (ℓ+1)-regular graph (except near j=0, 1728)

$$\begin{tikzcd}\bullet \arrow[r, shift left, "\varphi"] & \bullet \arrow[l, shift left, "\hat{\varphi}"]\end{tikzcd}$$

End(E)

imag. quad. order
or
quaternion order

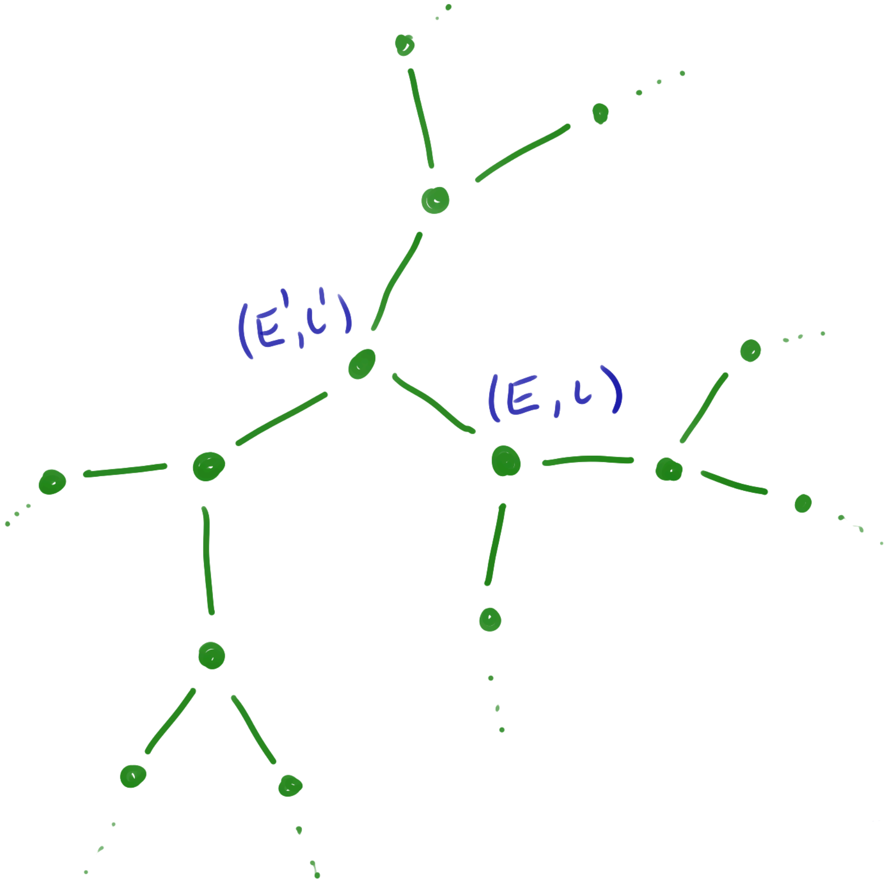


K-oriented ℓ-isogeny graph

K = quadratic imag. # fld

vertices = elliptic curves $/\overline{\mathbb{F}_p}$ up to isom.

edges = isogenies of degree ℓ up to equiv.



K-oriented
ℓ-isogeny graph

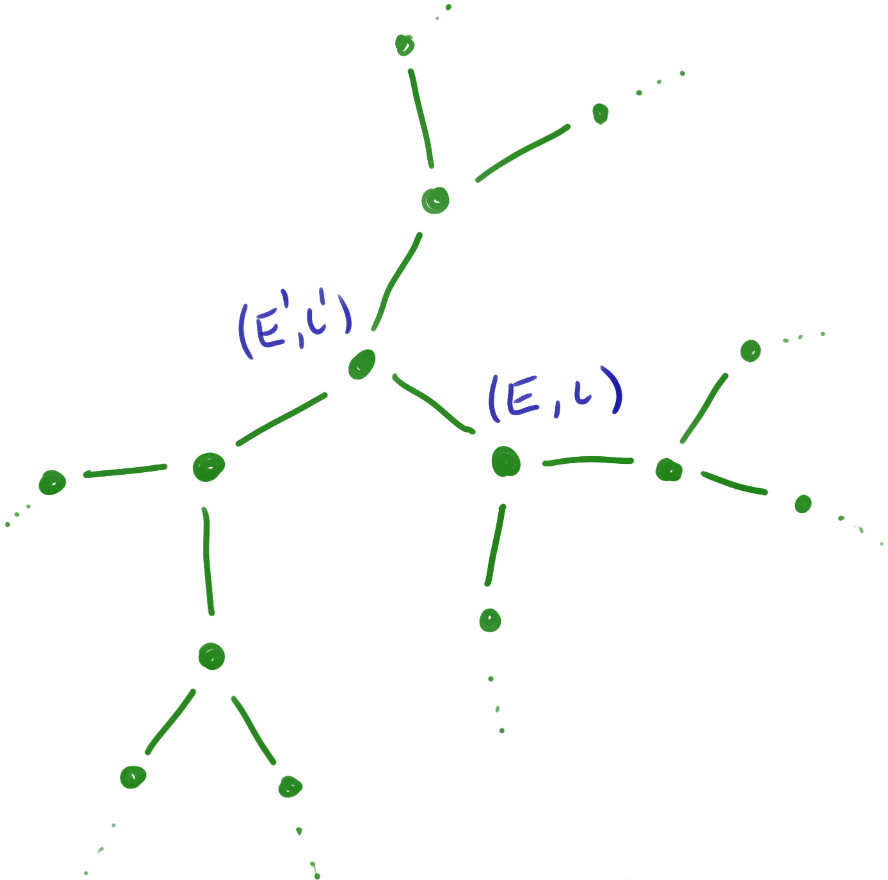
K = quadratic imag. # fld

vertices = elliptic curves $/\overline{\mathbb{F}_p}$ up to isom. together with a K-orientation

edges = isogenies of degree ℓ up to equiv.

K-oriented ℓ-isogeny graph

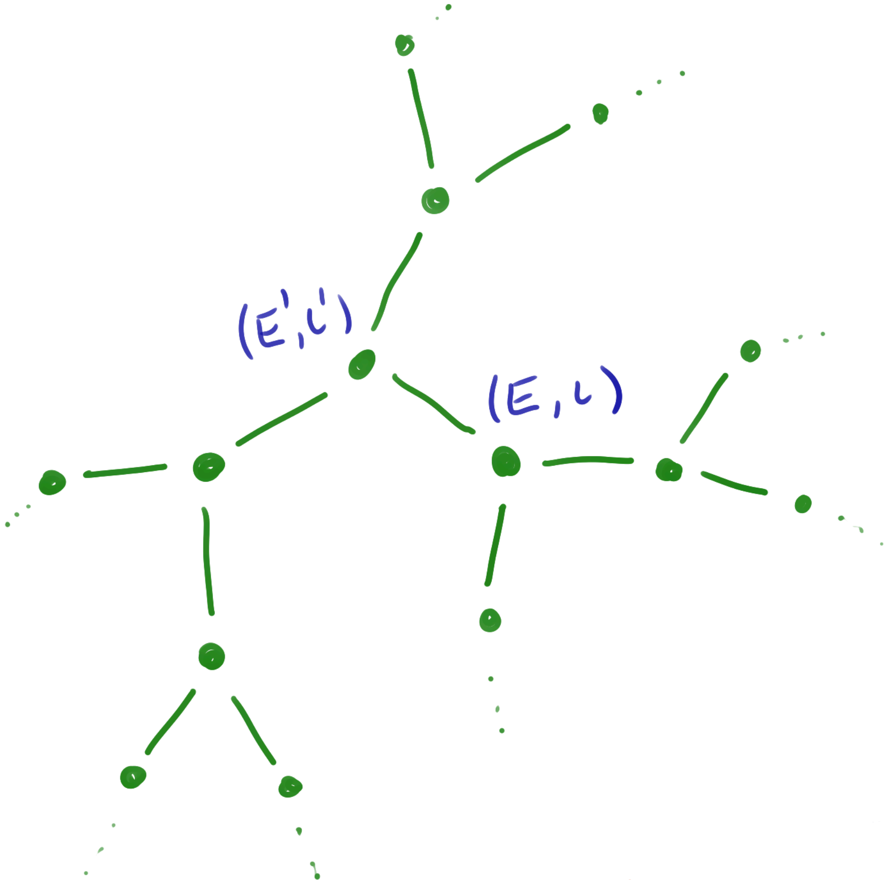
K = quadratic imag. # fld



vertices = elliptic curves / $\overline{\mathbb{F}}_p$ up to isom. together with a K-orientation

edges = isogenies of degree ℓ up to equiv.

$\iota : K \hookrightarrow \mathrm{End}(E) \otimes \mathbb{Q}$



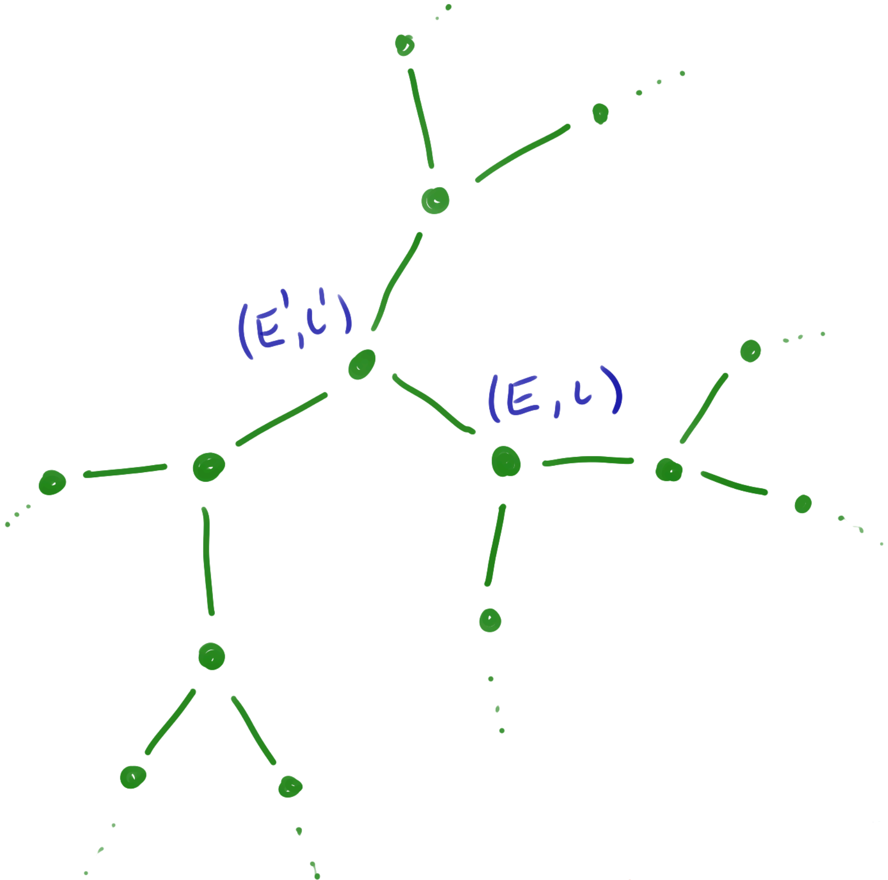
K-oriented
ℓ-isogeny graph

$K =$ quadratic imag. # fld

vertices = elliptic curves $/\overline{\mathbb{F}_p}$ up to isom.
together with a K-orientation

edges = isogenies of degree ℓ up to equiv.
respecting the orientation

$$\iota : K \hookrightarrow \mathrm{End}(E) \otimes \mathbb{Q}$$



K-oriented ℓ-isogeny graph

K = quadratic imag. # fld

vertices = elliptic curves / $\overline{\mathbb{F}}_p$ up to isom. together with a K-orientation

edges = isogenies of degree ℓ up to equiv. respecting the orientation

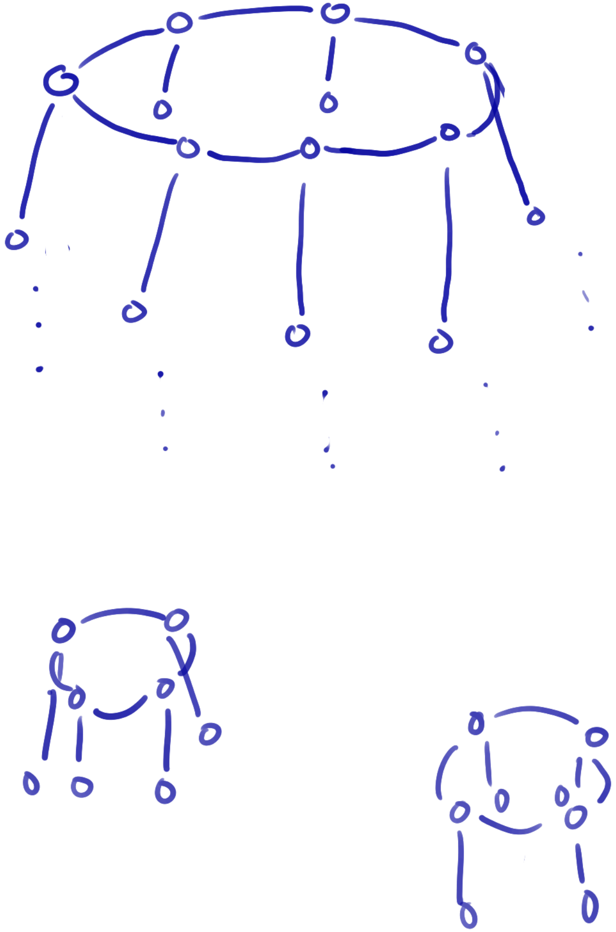
$$\iota : K \hookrightarrow \mathrm{End}(E) \otimes \mathbb{Q}$$

$$\begin{tikzcd}
E \arrow[r, "\varphi"] \arrow[d, "\iota(\alpha)"] & E' \arrow[d, "\iota'(\alpha)"] \\
E \arrow[r, "\varphi"] & E'
\end{tikzcd}$$

$$\iota'(\alpha) = \varphi\, \iota(\alpha)\, \hat{\varphi}$$

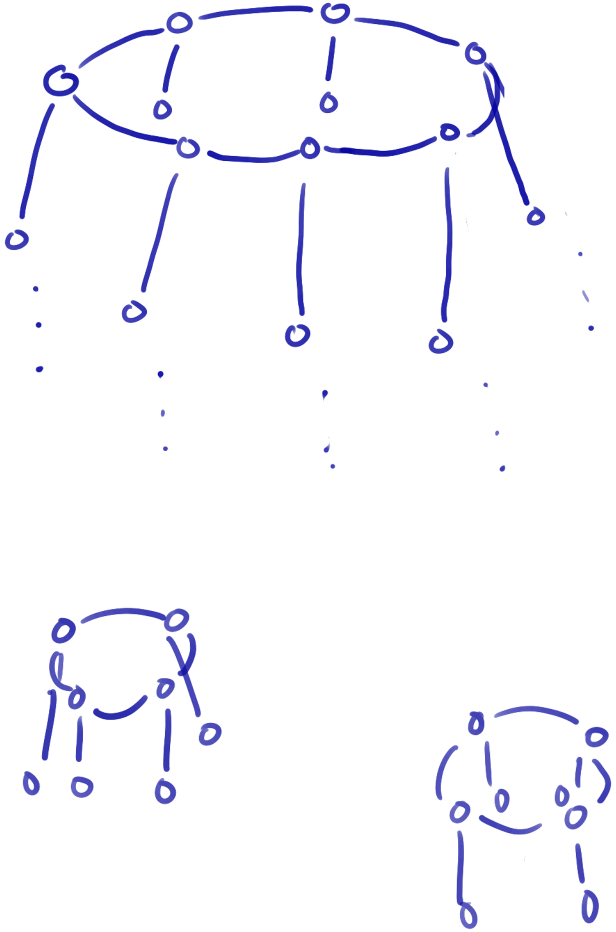
ℓ-isogeny graphs

ordinary

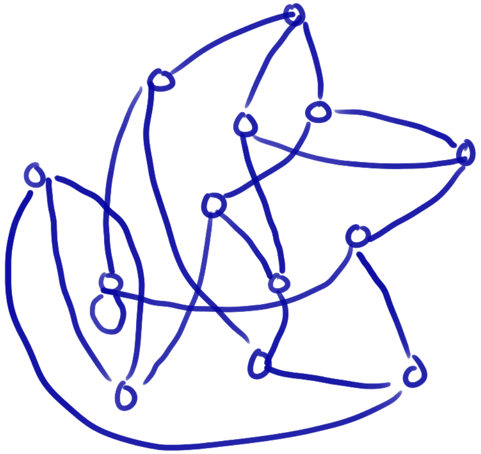


ℓ-isogeny graphs

ordinary

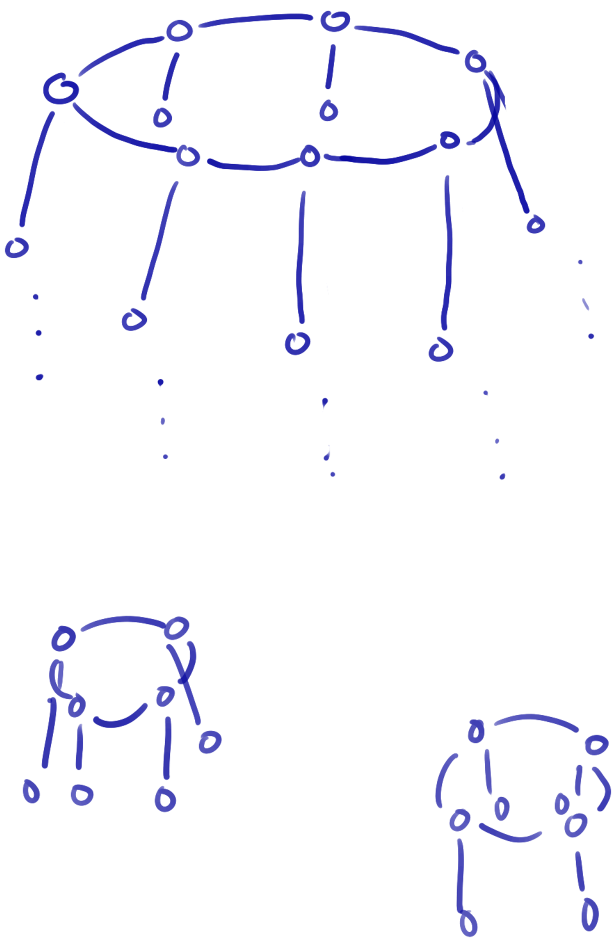


supersingular

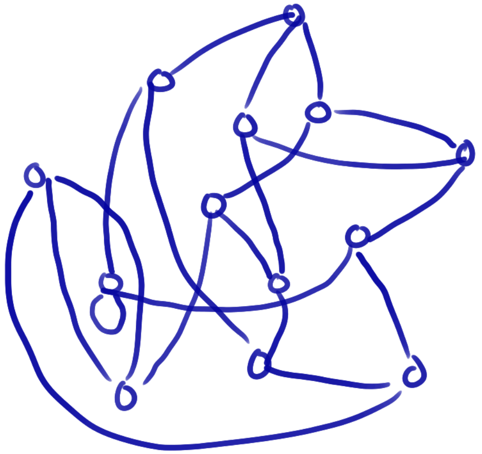


ℓ-isogeny graphs

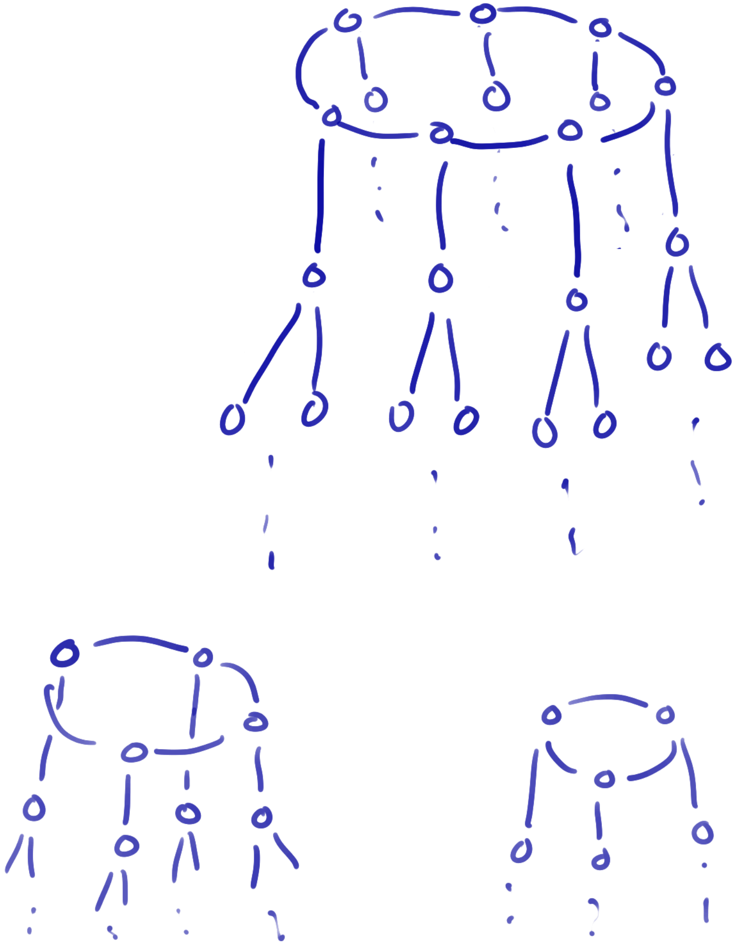
ordinary



supersingular

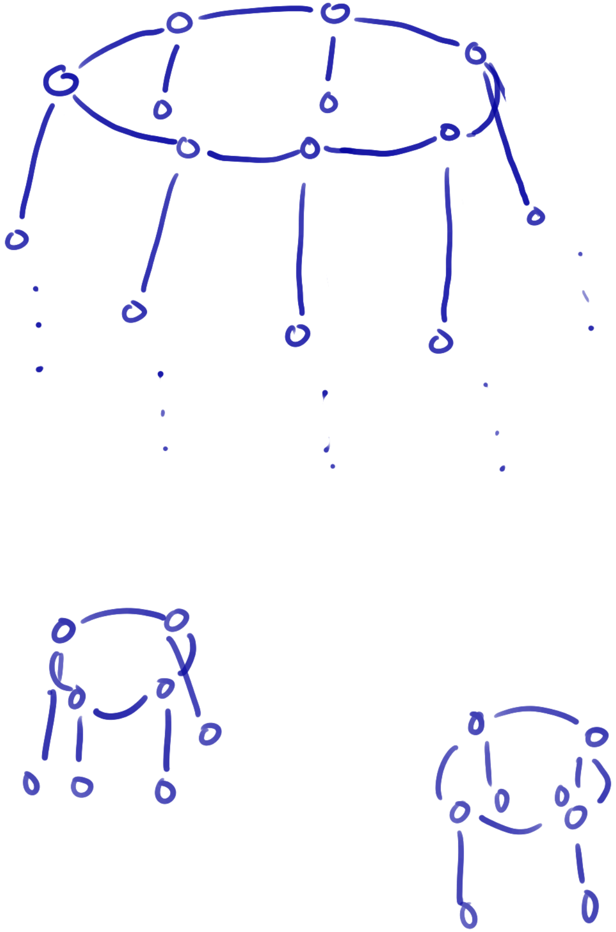


K-oriented supersingular

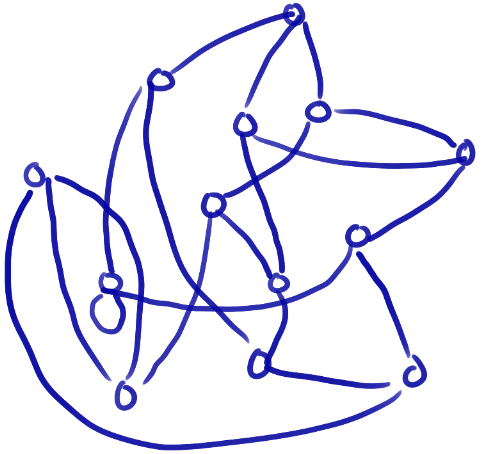


ℓ-isogeny graphs

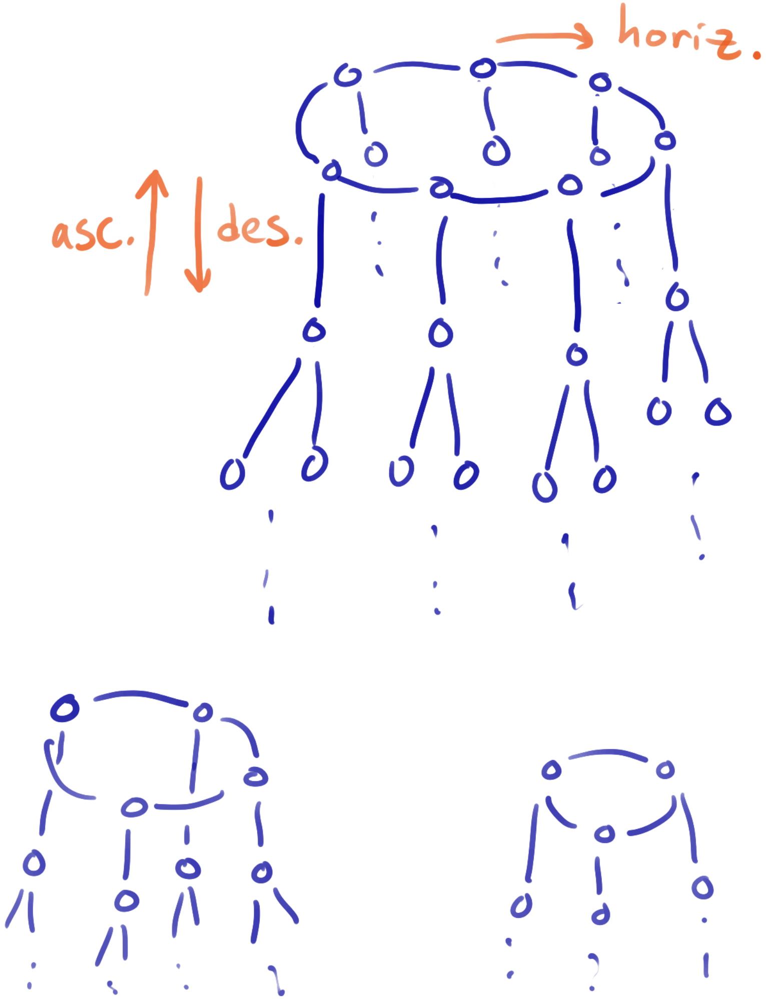
ordinary



supersingular



K-oriented supersingular

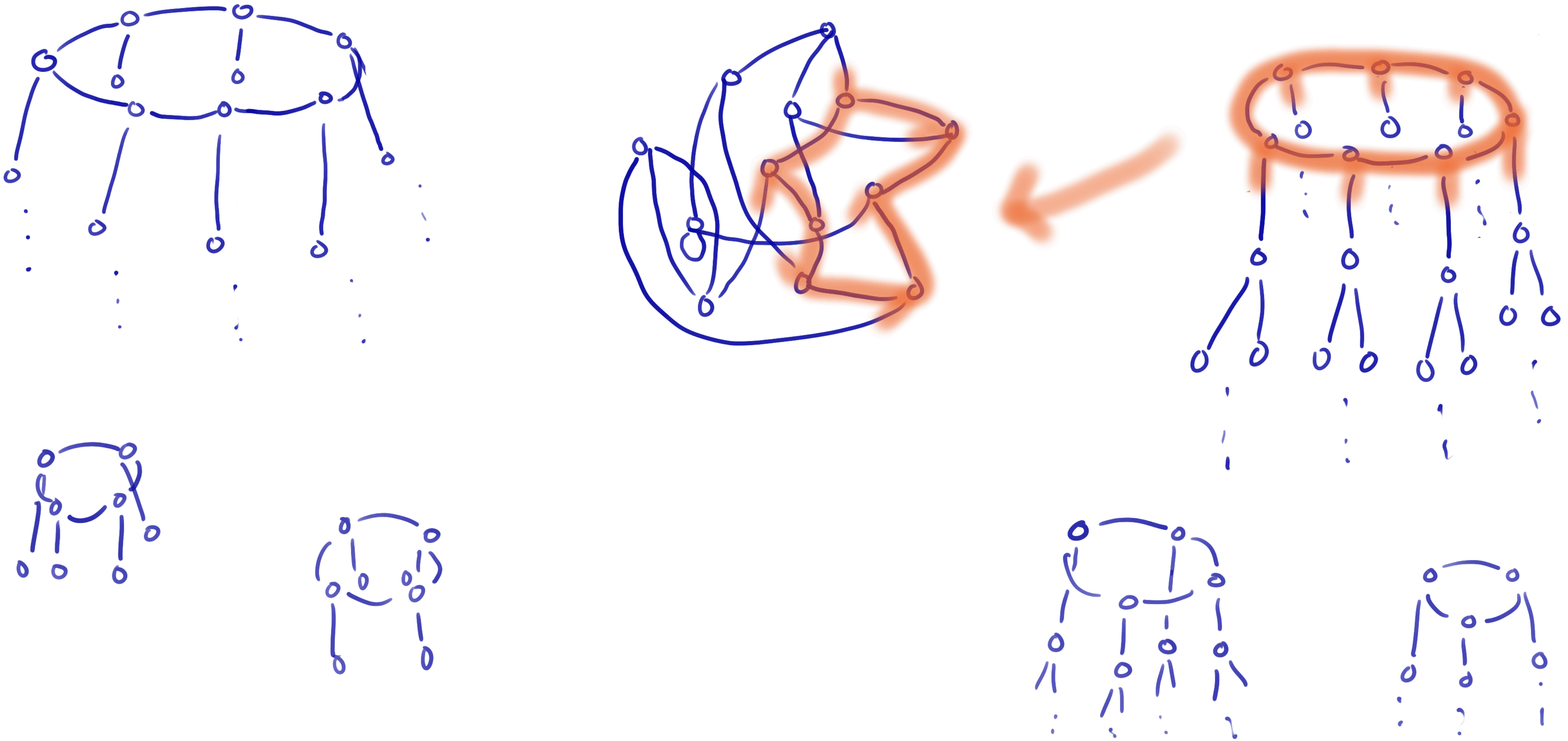


ℓ-isogeny graphs

ordinary

supersingular

K-oriented supersingular



$SS_{\Theta}^{pr}(p) = \{ (E, \iota) : \iota \text{ is } \Theta\text{-primitive} \}$

quadratic order

$$SS^{pr}_{\mathcal{O}}(p) = \{ (E, \iota) : \iota \text{ is } \mathcal{O}\text{-primitive} \}$$

$$\iota(K) \cap \mathrm{End}(E) = \iota(\mathcal{O})$$

$$SS^{pr}_{\mathcal{O}}(p) = \{ (E,\iota) : \iota \text{ is } \overset{\text{quadratic order}}{\mathcal{O}}\text{-primitive} \}$$

$$\iota(K) \cap \mathrm{End}(E) = \iota(\mathcal{O})$$

$$E[\mathfrak{a}] := \bigcap_{\alpha \in \iota(\mathfrak{a})} \ker(\alpha) \quad \text{for } \mathfrak{a} \subseteq \mathcal{O} \text{ } \overset{\text{inv.}}{\text{ideal}}$$

$$SS^{pr}_{\overset{\text{quadratic order}}{\mathcal{O}}}(p) = \{ (E,\iota) : \iota \text{ is } \mathcal{O}\text{-}\underset{\iota(K)\cap \mathrm{End}(E) = \iota(\mathcal{O})}{\text{primitive}} \}$$

$$E[\mathfrak{a}] := \bigcap_{\alpha\in\iota(\mathfrak{a})} \ker(\alpha) \quad \text{for } \mathfrak{a}\subseteq\mathcal{O} \ \overset{\text{inv.}}{\text{ideal}}$$

$$[\mathfrak{a}]\cdot E = E/E[\mathfrak{a}]$$

$$SS^{pr}_{\mathcal{O}}(p) = \{ (E,\iota) : \iota \text{ is } \overset{\text{quadratic order}}{\mathcal{O}}\text{-primitive}\} \xrightarrow{\quad} \begin{array}{l}\iota(K)\cap \mathrm{End}(E)\\ = \iota(\mathcal{O})\end{array}$$

$$E[\mathfrak{a}] := \bigcap_{\alpha \in \iota(\mathfrak{a})} \ker(\alpha) \quad \text{for } \mathfrak{a} \subseteq \mathcal{O} \ \overset{\text{inv.}}{\text{ideal}}$$

$$[\mathfrak{a}]\cdot E = E/E[\mathfrak{a}]$$

$Cl(\mathcal{O})$ acts freely on $SS^{pr}_{\mathcal{O}}(p)$

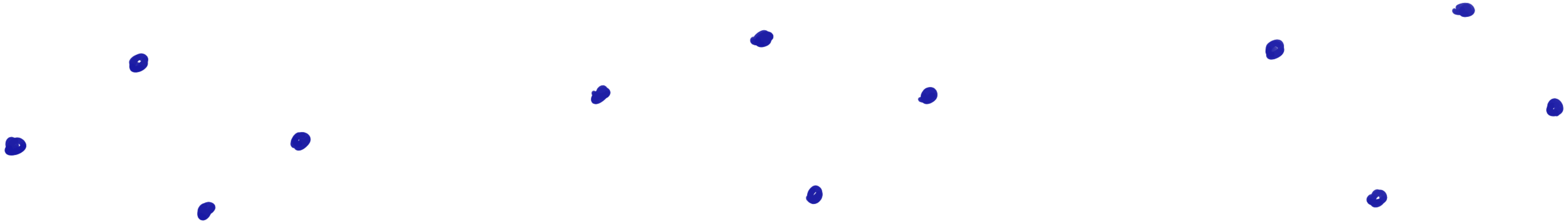
with 1 or 2 orbits

$Cl(\mathcal{O})$ acts freely on $SS_{\mathcal{O}}^{pr}(p)$

$[\mathfrak{a}] \cdot E = E / E[\mathfrak{a}]$

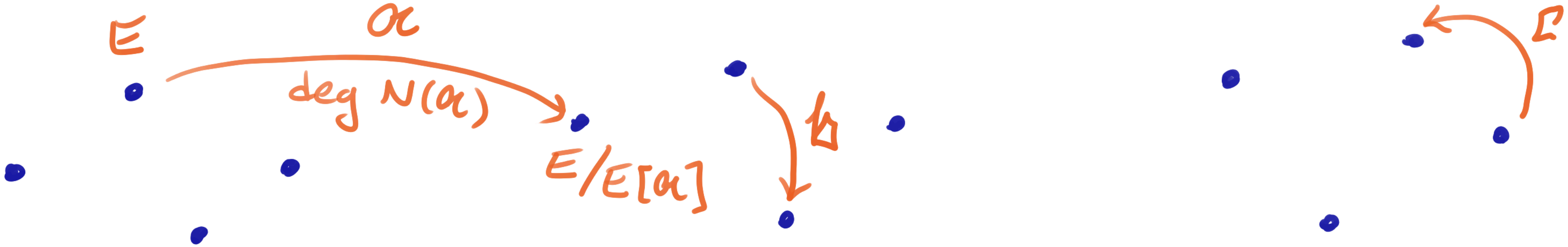
$\mathrm{Cl}(\mathcal{O})$ acts freely on $SS^{pr}_{\mathcal{O}}(p)$

$[\mathfrak{a}]\cdot E = E/E[\mathfrak{a}]$



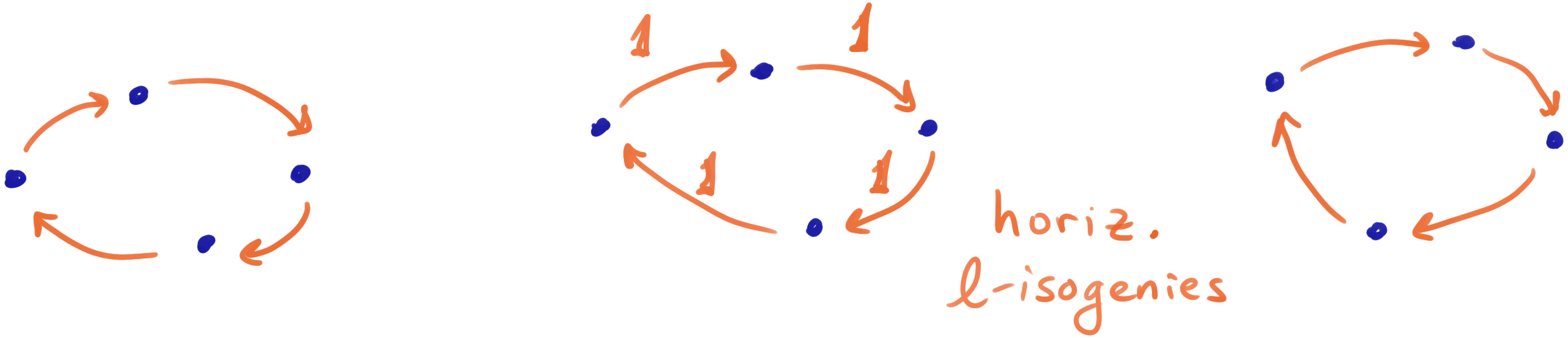
$Cl(\mathcal{O})$ acts freely on $SS_{\mathcal{O}}^{pr}(p)$

$[\alpha]\cdot E = E/E[\alpha]$



$Cl(\mathcal{O})$ acts freely on $SS^{pr}_{\mathcal{O}}(p)$

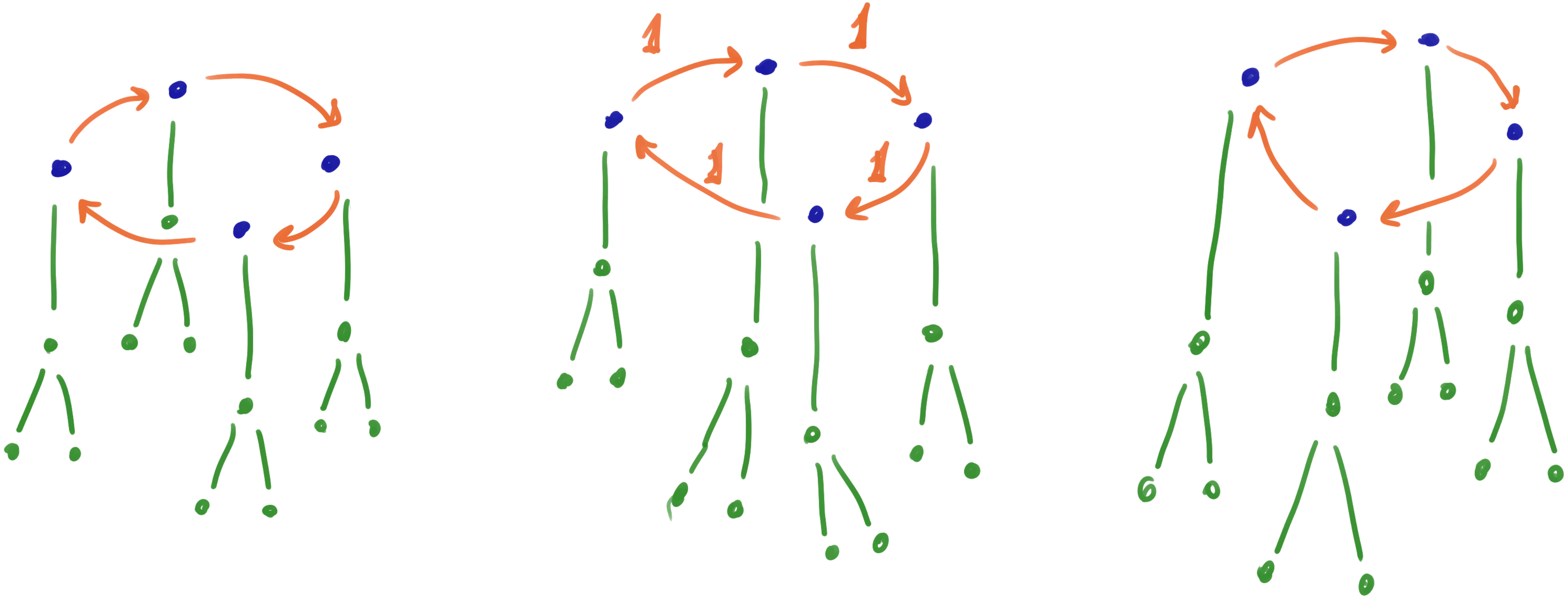
$[\mathfrak{a}]\cdot E = E/E[\mathfrak{a}]$



$(\ell) = \mathfrak{l}\cdot\bar{\mathfrak{l}}$

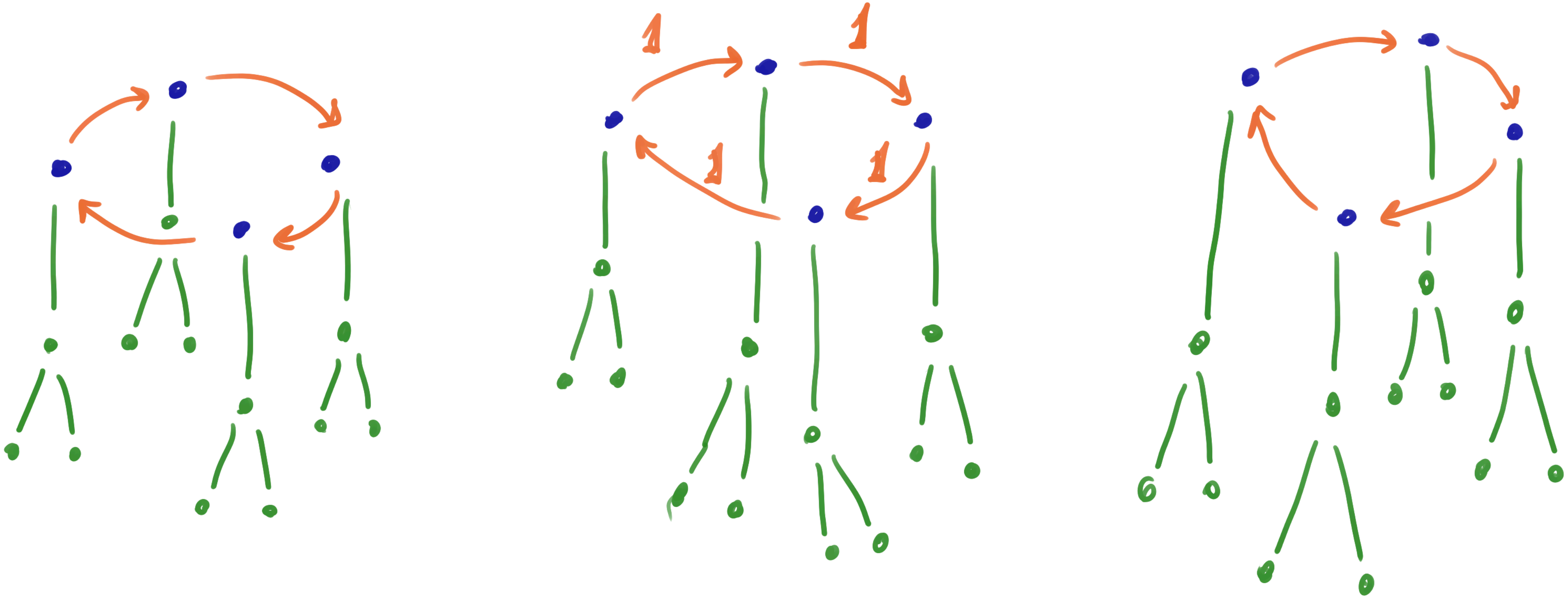
$\mathrm{Cl}(\mathcal{O})$ acts freely on $SS_{\mathcal{O}}^{pr}(p)$

$[\mathfrak{a}]\cdot E = E/E[\mathfrak{a}]$



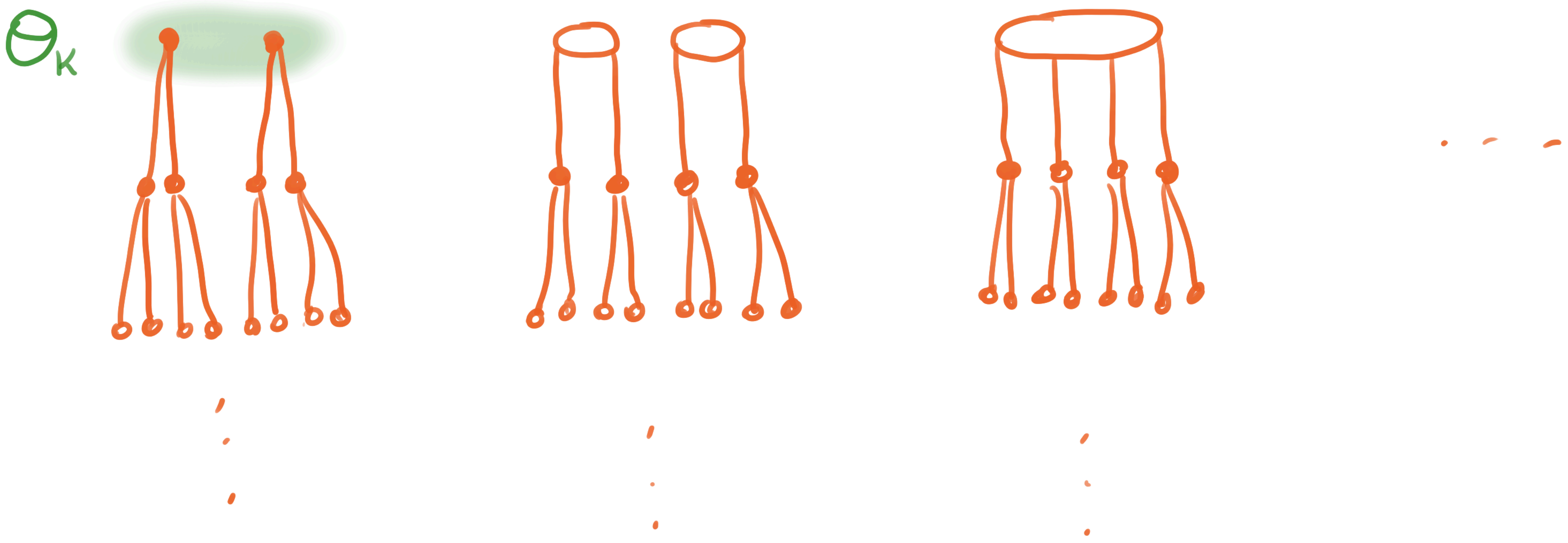
$Cl(\mathcal{O})$ acts freely on $SS^{pr}_{\mathcal{O}}(p)$

$[\mathfrak{a}]\cdot E = E/E[\mathfrak{a}]$

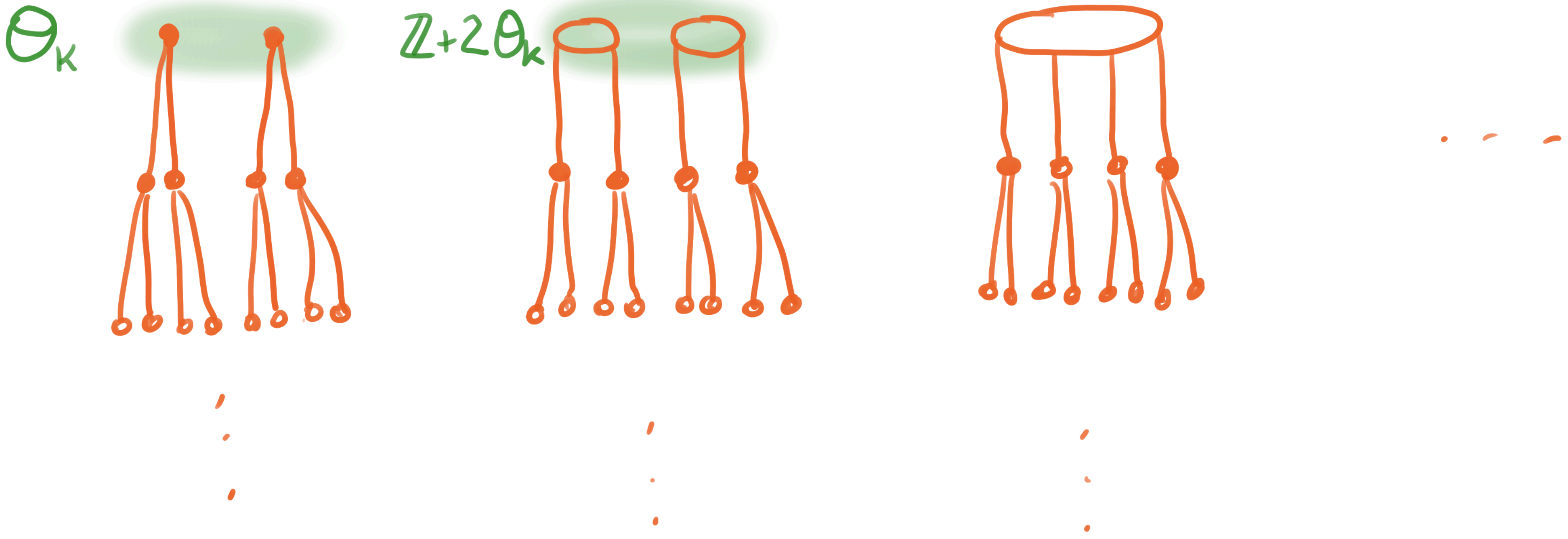


rim size = order of $[\mathbb{1}]$ in $Cl(\mathcal{O})$

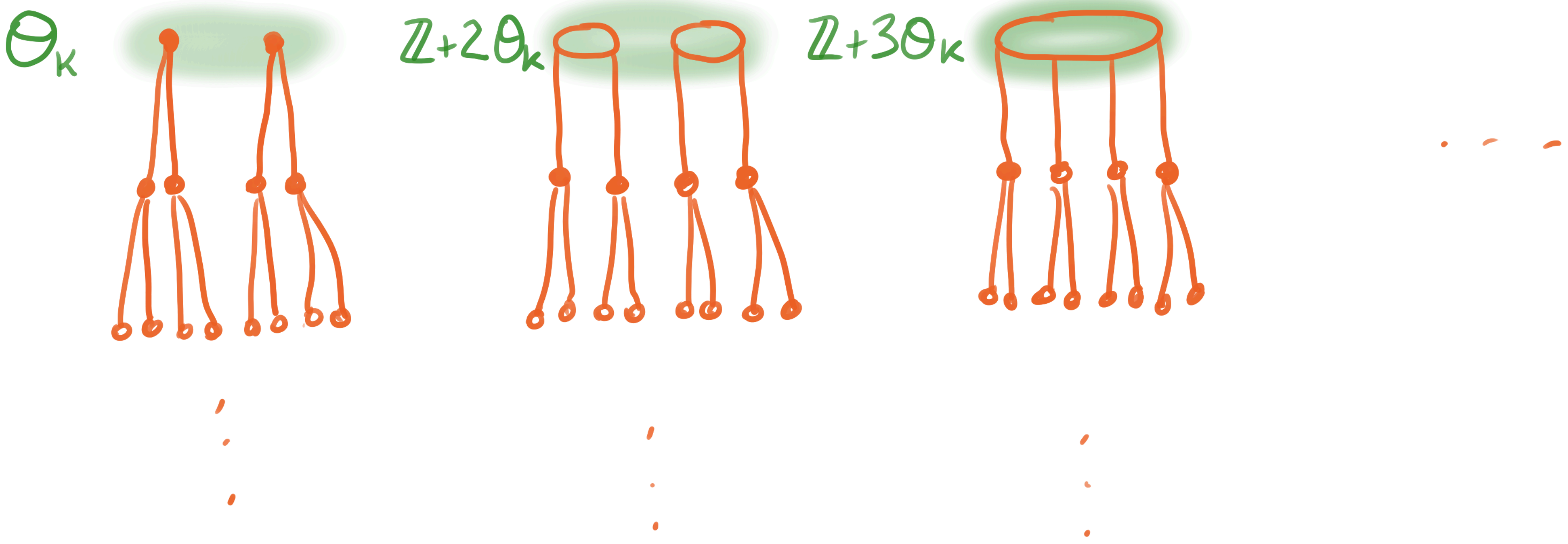
K-oriented ss. isog. graph



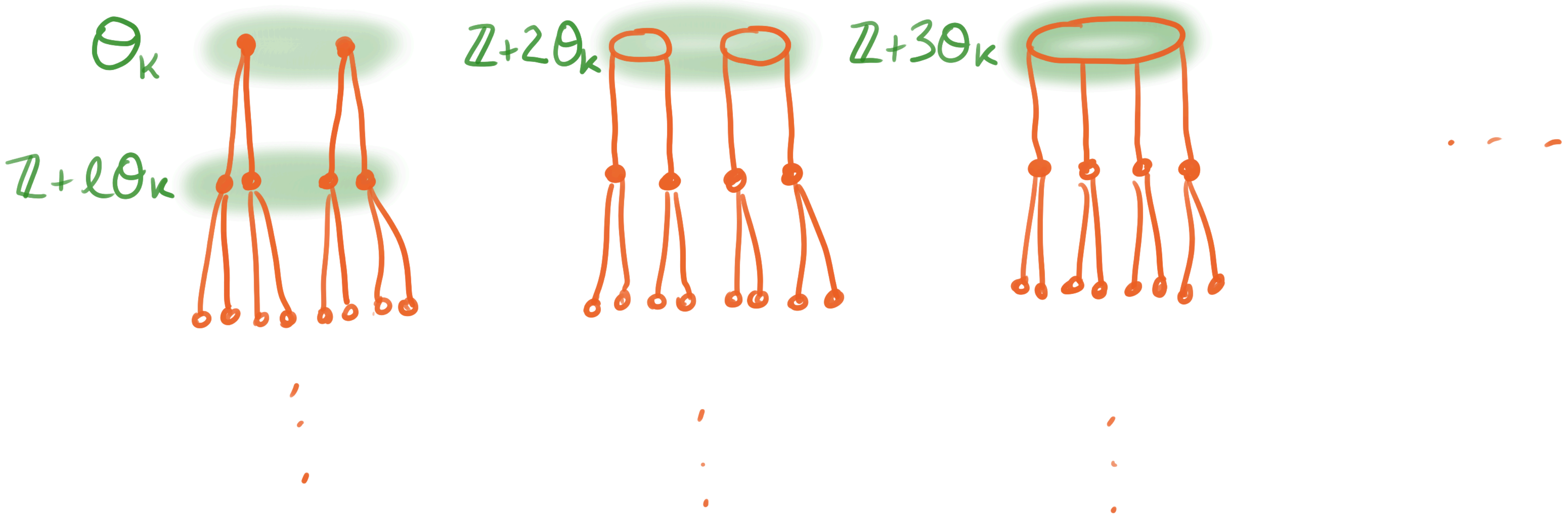
K-oriented ss. isog. graph



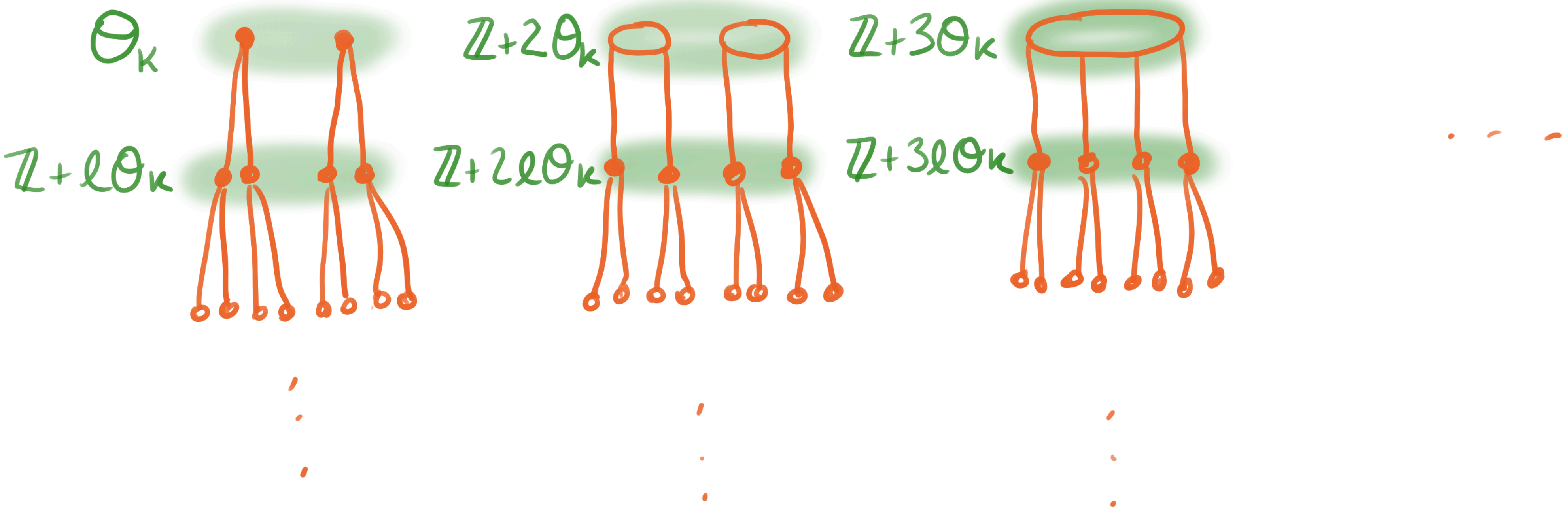
K-oriented ss. isog. graph



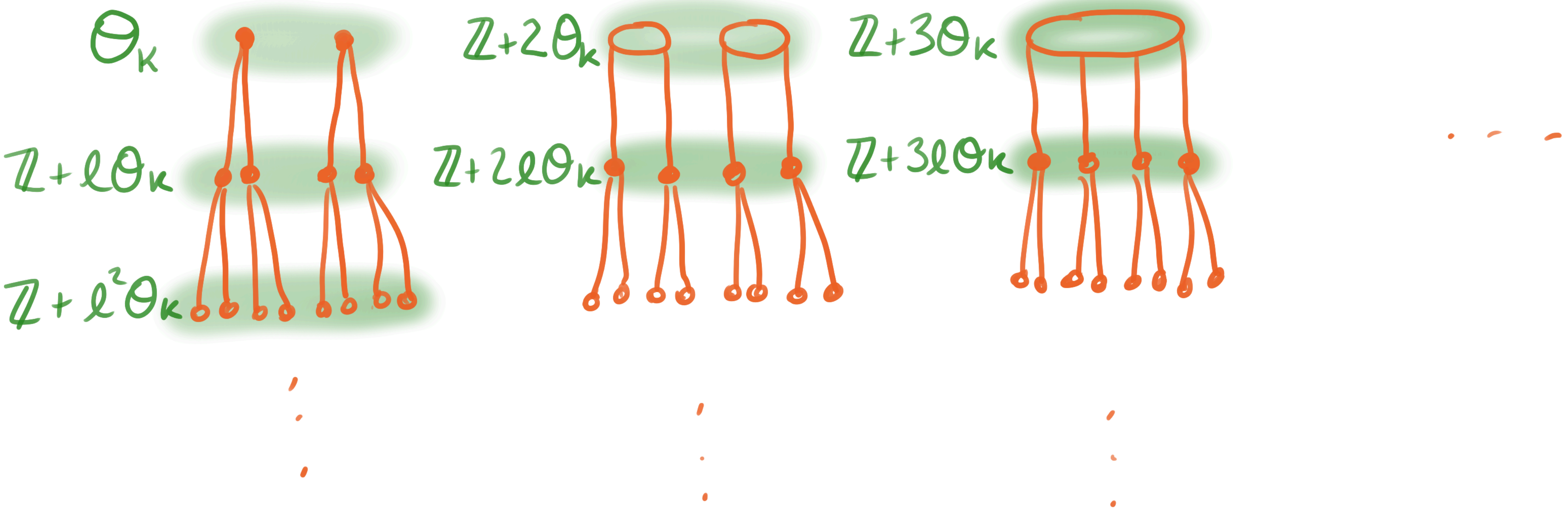
K-oriented ss. isog. graph



K-oriented ss. isog. graph



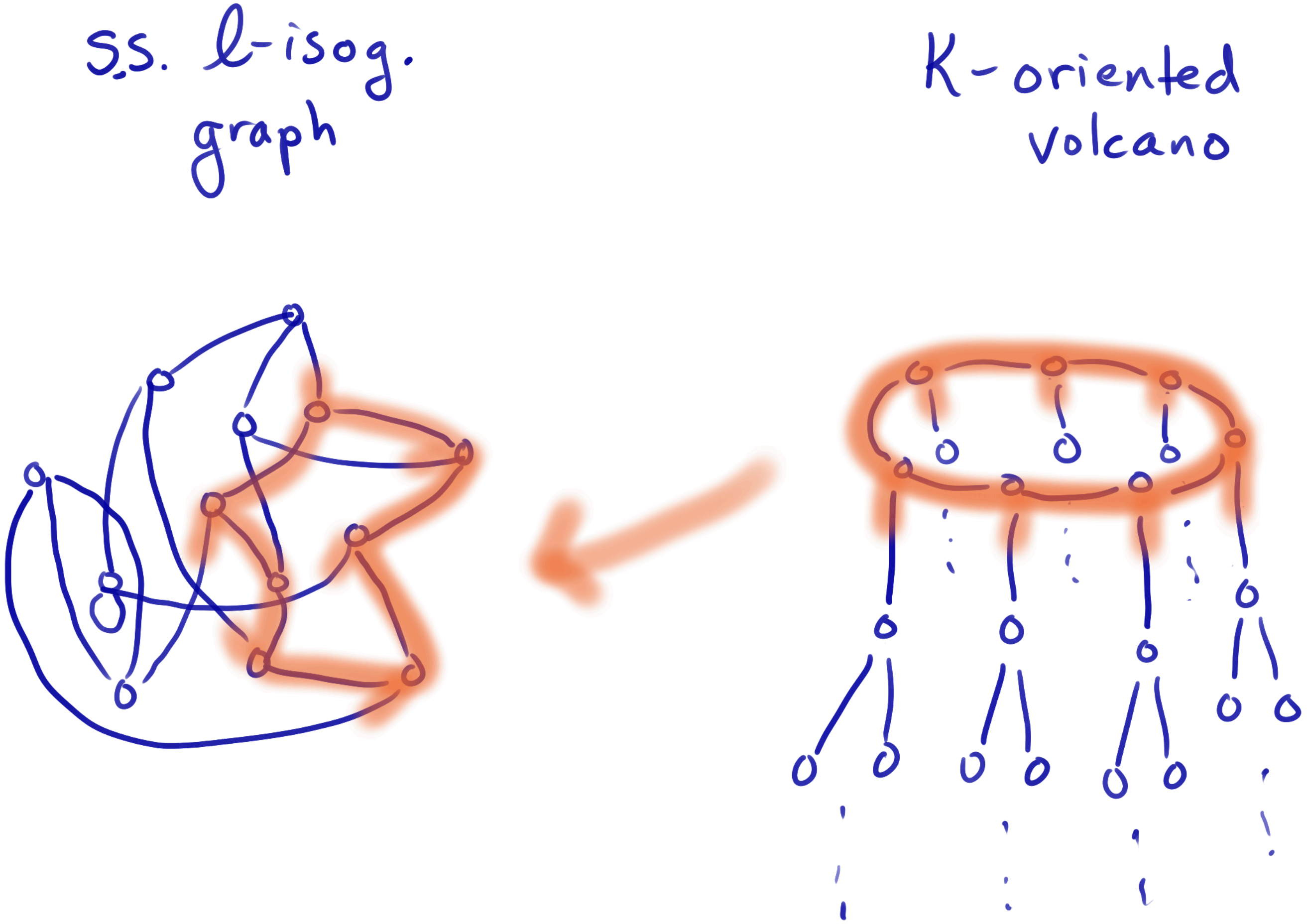
K-oriented ss. isog. graph

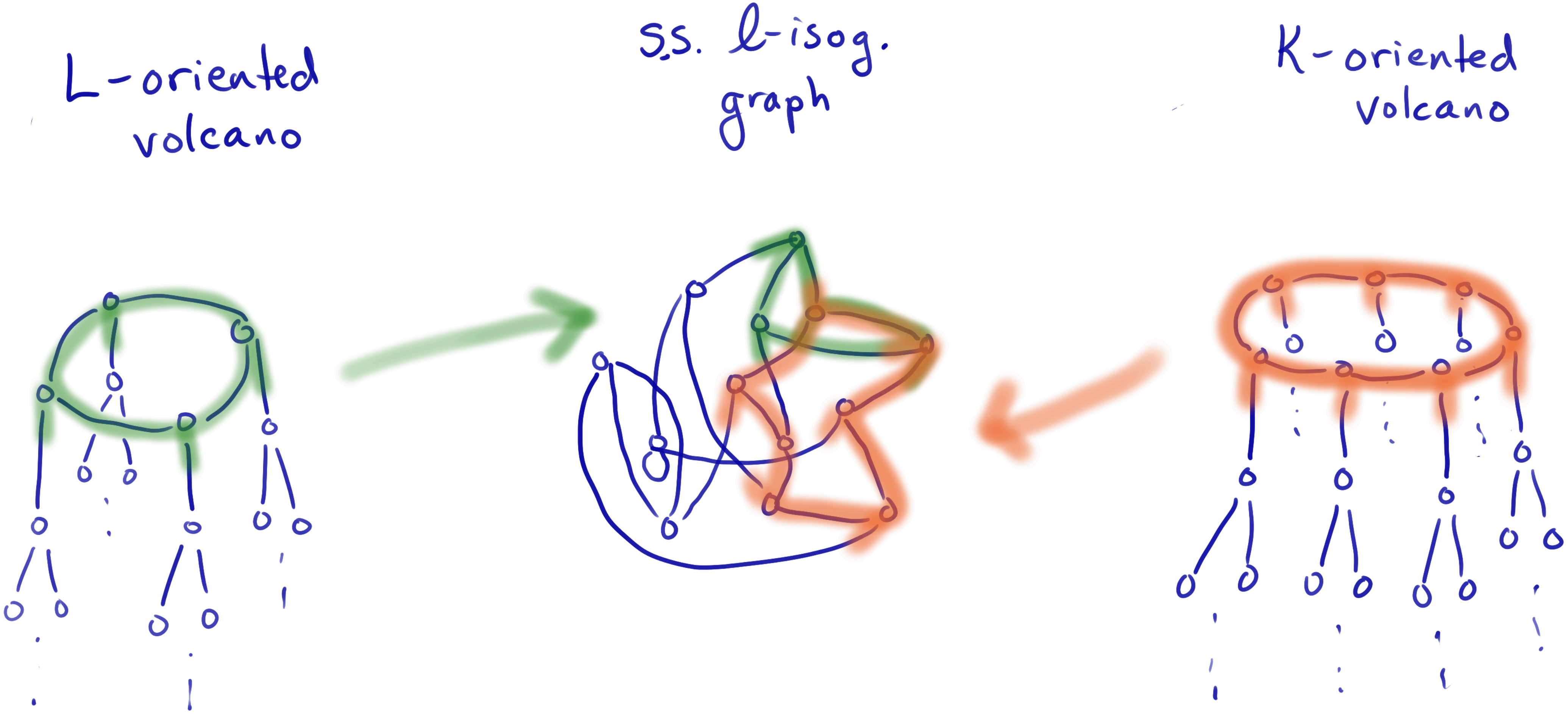


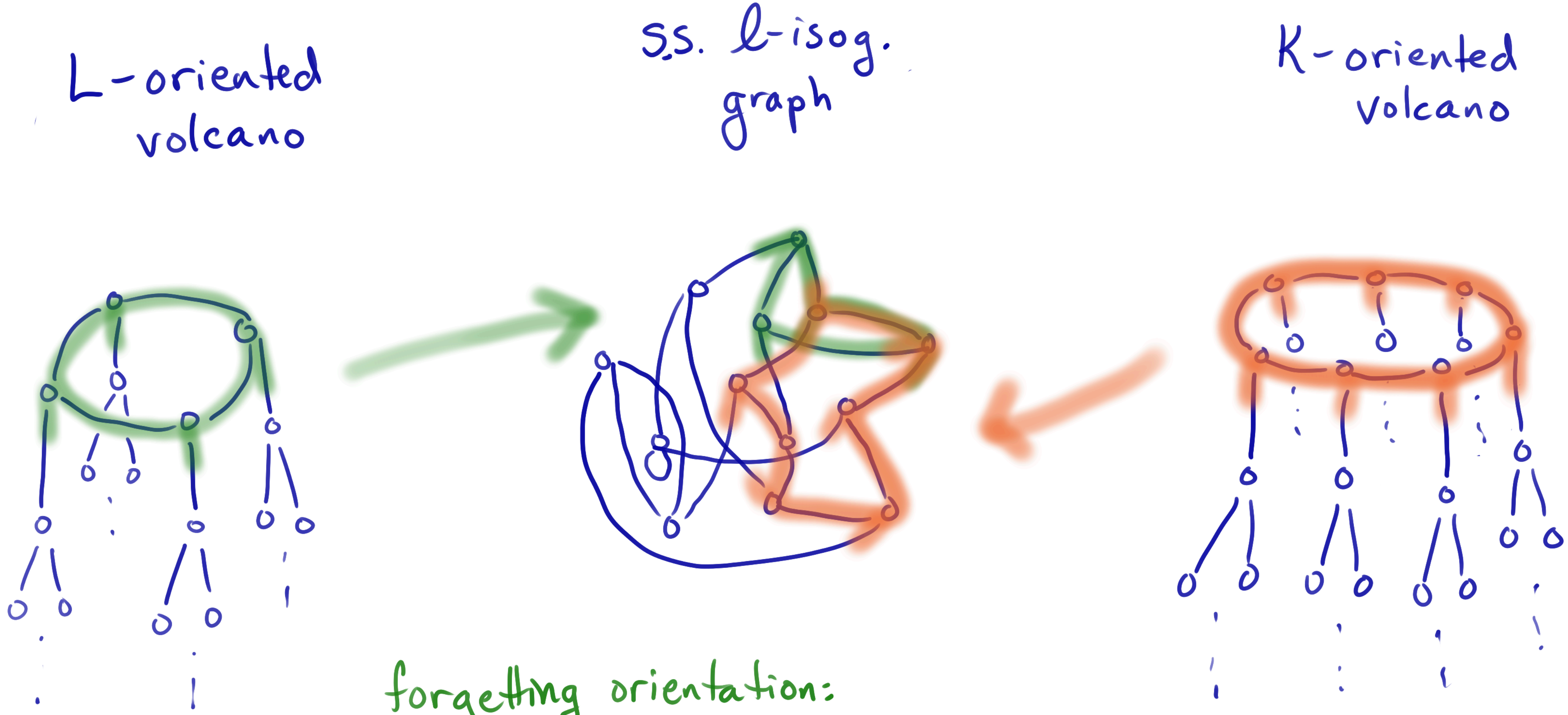
ascending → order gets bigger by index ℓ

descending → " " smaller " " "

horizontal → no change


s.s. ℓ-isog.
graph
K-oriented
volcano

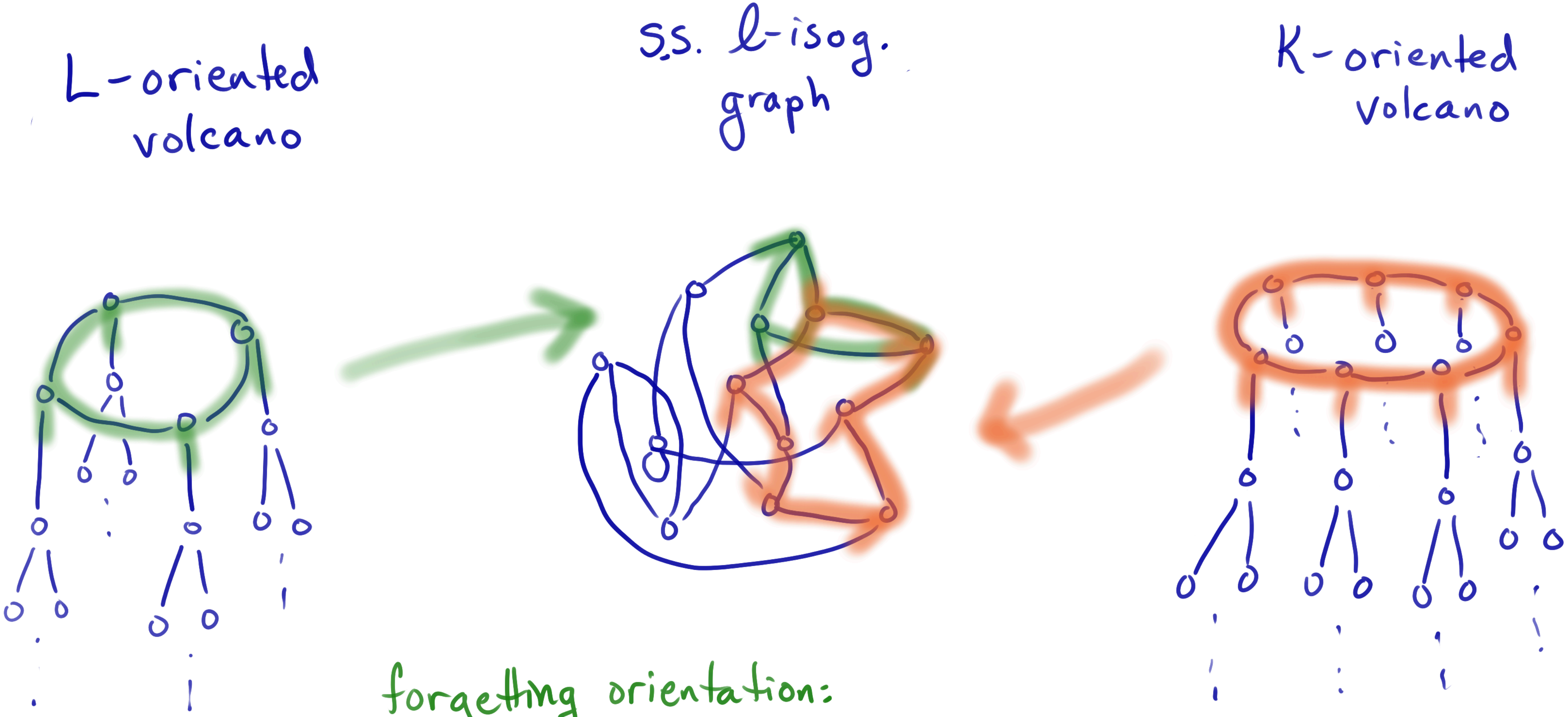

L-oriented volcano
s.s. ℓ-isog. graph
K-oriented volcano



forgetting orientation:

rim → closed walk, same length

- no backtracking
- not a repeat of a smaller cycle



forgetting orientation:

rim → closed walk, same length

- no backtracking
- not a repeat of a smaller cycle

"isogeny cycle"

Theorem (Arpin, Chen, Lauter, Scheidler, S. , Tran)

Primes $\ell < p$. Integer $r > 2$. $\mathcal{G}_\ell =$ s.s. ℓ-isog. graph

Theorem (Arpin, Chen, Lauter, Scheidler, S., Tran)

Primes $\ell < p$. Integer $r > 2$. $\mathcal{G}_\ell =$ s.s. ℓ-isog. graph

$$\left\{\begin{array}{c}\text{isogeny cycles of}\\ \text{length } r \text{ in } \mathcal{G}_\ell\end{array}\right\} \overset{\text{bij.}}{\longleftrightarrow} \left\{\begin{array}{c}\text{rims of size } r \text{ in}\\ \text{union of all oriented}\\ \text{s.s. } \ell\text{-isog. volcanoes}\end{array}\right\}$$

up to conjugation

$\iota \longrightarrow \bar{\iota}$

Theorem (Arpin, Chen, Lauter, Scheidler, S., Tran)

Primes $\ell < p$. Integer $r > 2$. $\mathcal{G}_\ell$ = s.s. ℓ-isog. graph

$$\left\{ \begin{array}{c} \text{isogeny cycles of} \\ \text{length } r \text{ in } \mathcal{G}_\ell \end{array} \right\} \xleftrightarrow{\text{bij.}} \left\{ \begin{array}{c} \text{rims of size } r \text{ in} \\ \text{union of all oriented} \\ \text{s.s. } \ell\text{-isog. volcanoes} \end{array} \right\}$$

$\xleftarrow[\text{orientation}]{\text{forget}}$

up to conjugation

$\iota \to \bar{\iota}$

Theorem (Arpin, Chen, Lauter, Scheidler, S., Tran)

Primes $\ell < p$. Integer $r > 2$. $\mathcal{G}_\ell$ = s.s. ℓ-isog. graph

$$\left\{ \begin{array}{c} \text{isogeny cycles of} \\ \text{length } r \text{ in } \mathcal{G}_\ell \end{array} \right\} \xleftrightarrow{\text{bij.}} \left\{ \begin{array}{c} \text{rims of size } r \text{ in} \\ \text{union of all oriented} \\ \text{s.s. } \ell\text{-isog. volcanoes} \end{array} \right\}$$

$$\xleftarrow[\text{orientation}]{\text{forget}}$$

up to conjugation

$\iota \to \bar{\iota}$

$$\longrightarrow$$

Theorem (Arpin, Chen, Lauter, Scheidler, S., Tran)

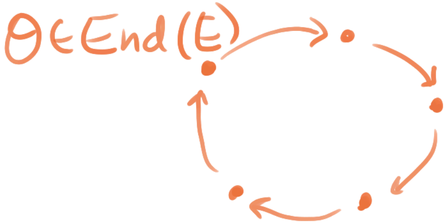
Primes $\ell < p$. Integer $r > 2$. $\mathcal{G}_\ell =$ s.s. ℓ-isog. graph

$$\left\{ \begin{array}{c}\text{isogeny cycles of}\\ \text{length } r \text{ in } \mathcal{G}_\ell\end{array}\right\} \xleftrightarrow{\text{bij.}} \left\{\begin{array}{c} \text{rims of size } r \text{ in} \\ \text{union of all oriented} \\ \text{s.s. } \ell\text{-isog. volcanoes}\end{array}\right\}$$

$\xleftarrow[\text{orientation}]{\text{forget}}$

up to conjugation

$\iota \rightarrow \bar{\iota}$



$\xrightarrow[\text{around cycle}]{\text{compose}}$

$\iota : \alpha \longmapsto \theta$

Theorem (Arpin, Chen, Lauter, Scheidler, S., Tran)

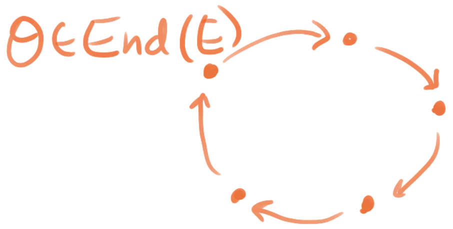
Primes $\ell < p$. Integer $r > 2$. $\mathcal{G}_\ell$ = s.s. ℓ-isog. graph

$$\left\{ \begin{array}{c} \text{isogeny cycles of} \\ \text{length } r \text{ in } \mathcal{G}_\ell \end{array} \right\} \xleftrightarrow{\text{bij.}} \left\{ \begin{array}{c} \text{rims of size } r \text{ in} \\ \text{union of all oriented} \\ \text{s.s. } \ell\text{-isog. volcanoes} \end{array} \right\}$$

$$\xleftarrow[\text{orientation}]{\text{forget}}$$

up to conjugation

$\iota \rightarrow \bar{\iota}$



$$\xrightarrow[\text{around cycle}]{\text{compose}}$$

$\iota : \alpha \longmapsto \theta$

Corollary: Counting Isogeny Cycles

Corollary: Counting Isogeny Cycles

\# isogeny
cycles of
length r

Corollary: Counting Isogeny Cycles

$$\frac{\ell^r}{2r} \underset{\text{Ramanujan graphs}}{\overset{r\to\infty}{\sim}} \#\text{ isogeny cycles of length } r$$

Corollary: Counting Isogeny Cycles

$$\frac{\ell^r}{2r} \underset{\text{Ramanujan graphs}}{\overset{r\to\infty}{\sim}} \#\text{ isogeny cycles of length } r = \frac{1}{r}\sum \varepsilon_{\theta,\ell}\, h_\theta$$

Corollary: Counting Isogeny Cycles

$$\frac{\ell^r}{2r} \underset{\text{Ramanujan graphs}}{\overset{r\to\infty}{\sim}} \#\text{ isogeny cycles of length } r = \frac{1}{r}\sum_{\theta} \overset{\text{1 or 2}}{\varepsilon_{\theta,\ell}}\, \overset{\text{class \#}}{h_\theta}$$

θ :

- p not split
- $p \nmid$ conductor
- Δ_θ is ℓ-fund.
- $[\mathfrak{l}]$ has order r

Corollary: Counting Isogeny Cycles

1 or 2

class #

$$\frac{\ell^r}{2r} \overset{r\to\infty}{\sim} \#\text{ isogeny cycles of length } r = \frac{1}{r}\sum_{\theta} \varepsilon_{\theta,\ell}\, h_\theta \le \text{explicit bd}$$

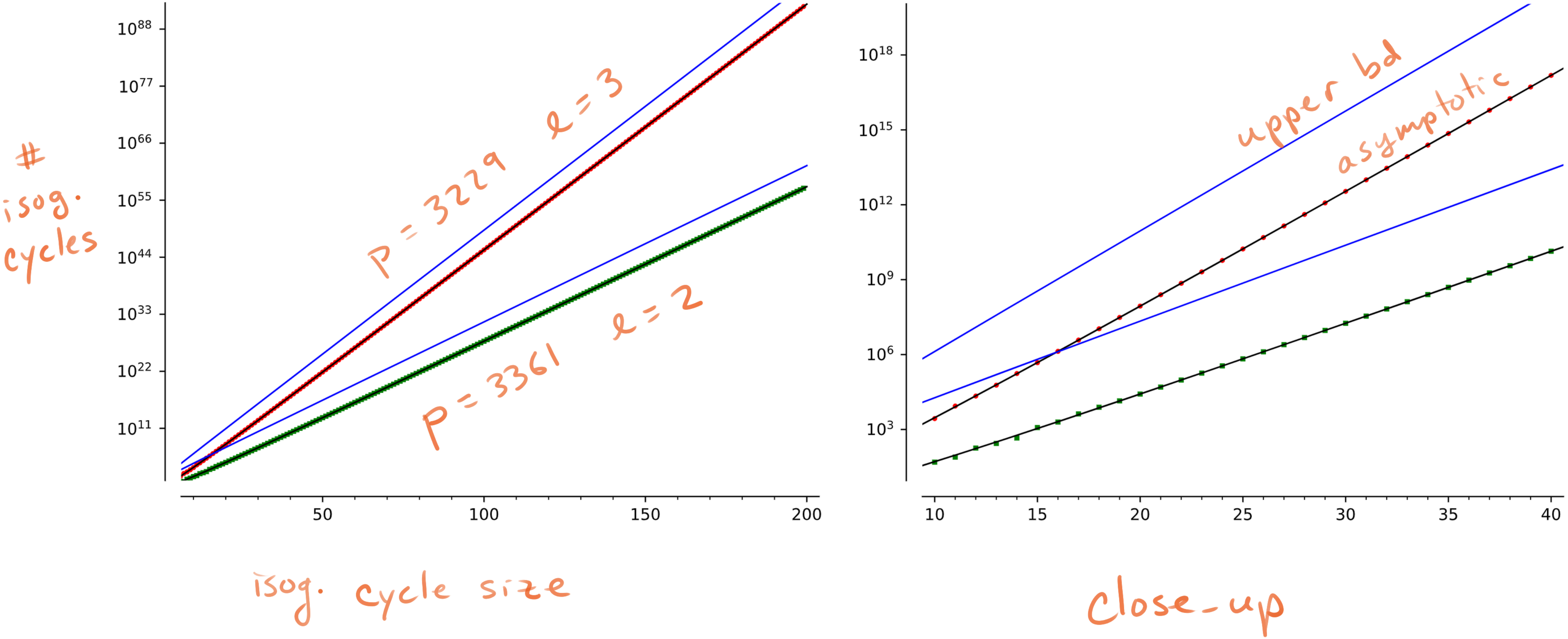
Ramanujan graphs

θ :
- p not split
- $p \nmid$ conductor
- Δ_θ is ℓ-fund.
- $[1]$ has order r

class # bds,

Möbius inversion

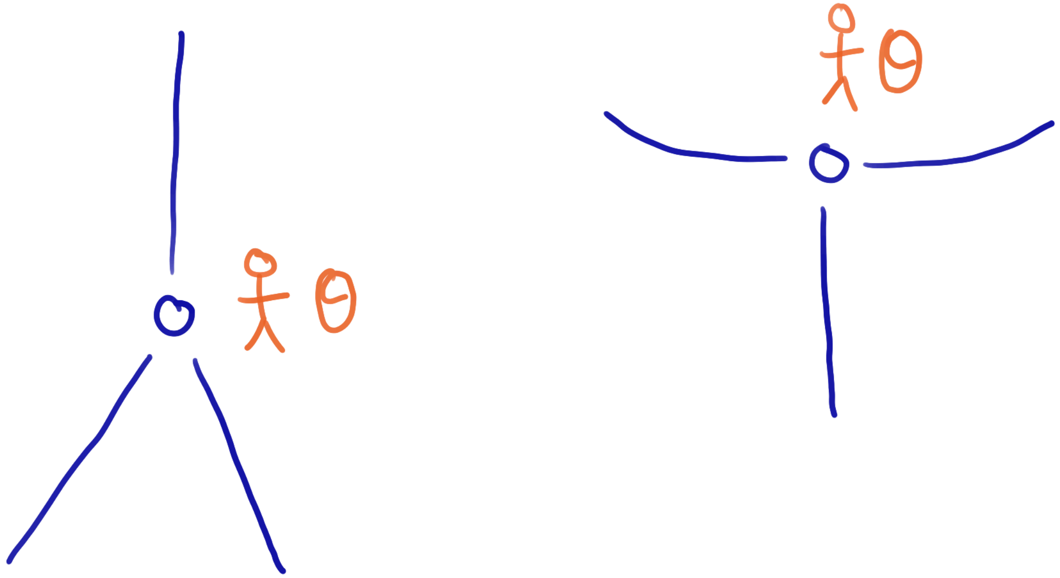
approx. $\ell^r \log^r$



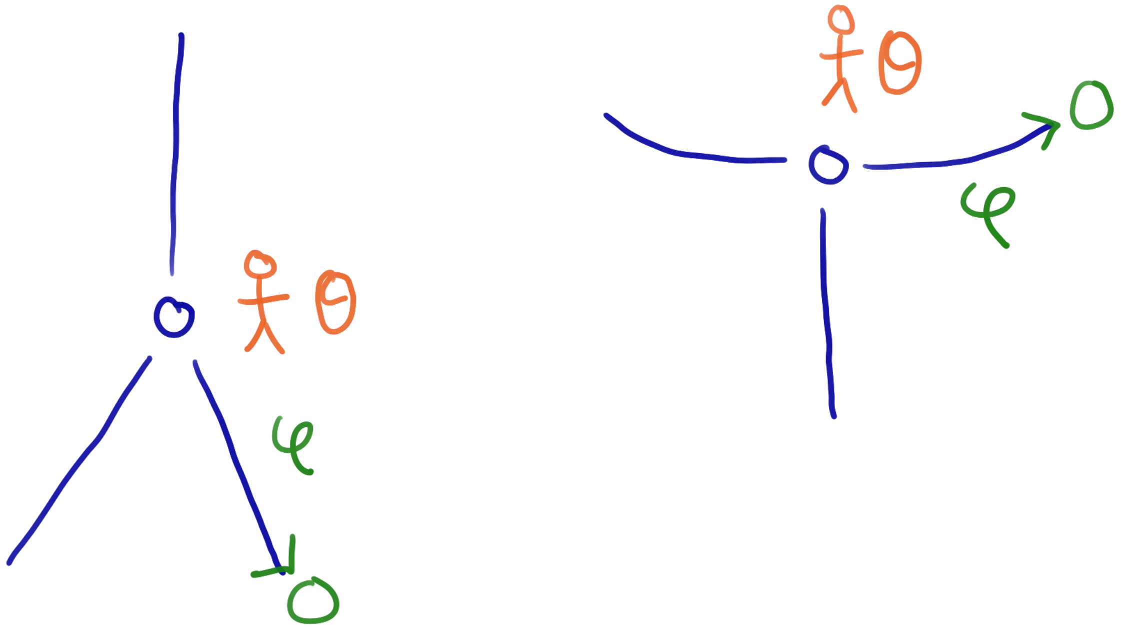
isog. cycles
10^88
10^77
10^66
10^55
10^44
10^33
10^22
10^11
p = 3229 ℓ = 3
p = 3361 ℓ = 2
50
100
150
200
isog. cycle size
10^18
10^15
10^12
10^9
10^6
10^3
upper bd
asymptotic
10
15
20
25
30
35
40
close-up

Can you use this to navigate in the ℓ-isogeny graph?

Can you use this to navigate in the ℓ-isogeny graph?

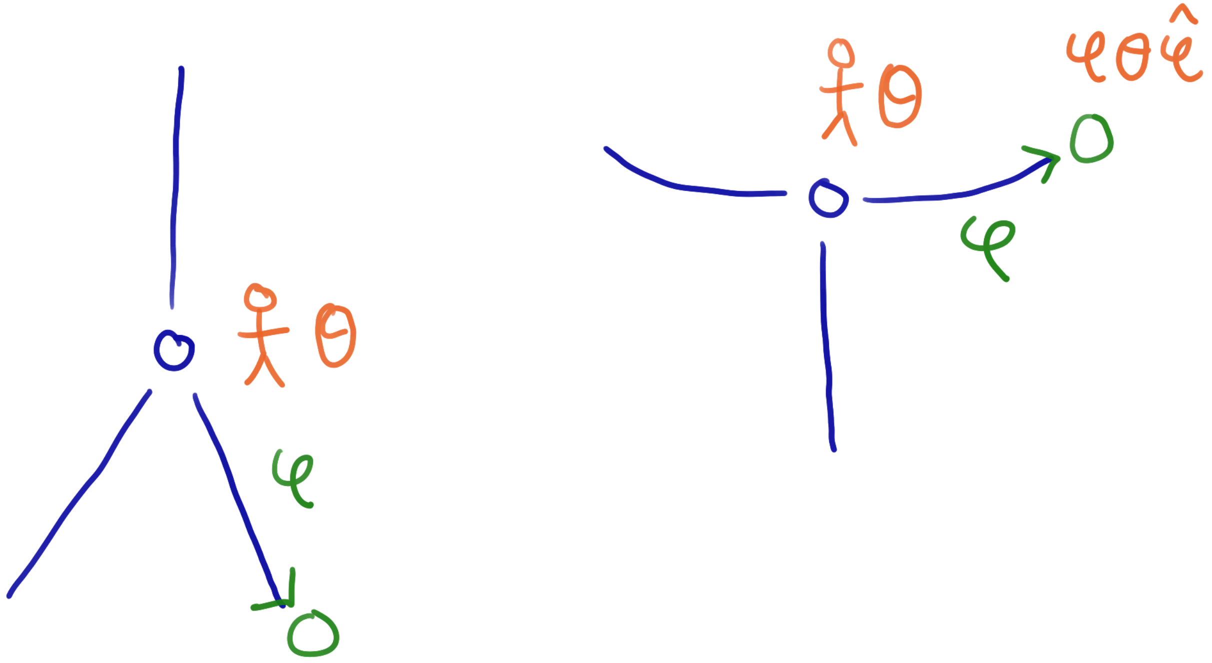


Can you use this to navigate in the ℓ-isogeny graph?



try one direction φ:

Can you use this to navigate in the ℓ-isogeny graph?

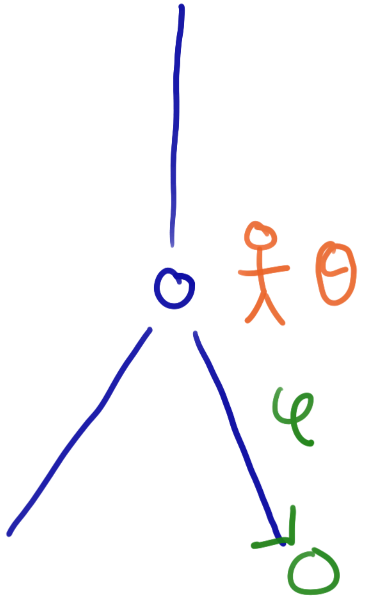


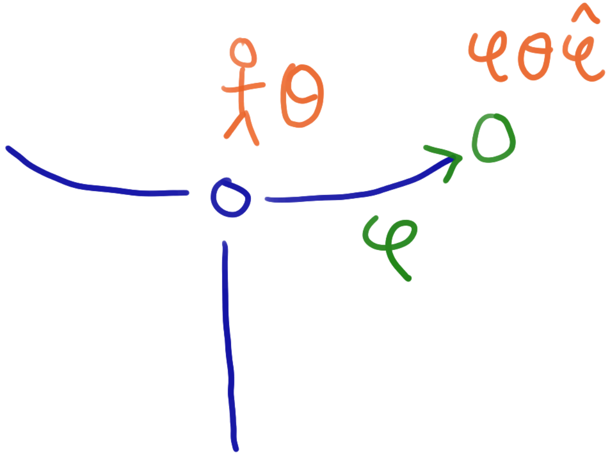
try one direction φ:

- the new orientation is

$$\varphi\,\theta\,\hat{\varphi}$$

Can you use this to navigate in the ℓ-isogeny graph?





try one direction φ:

- the new orientation is

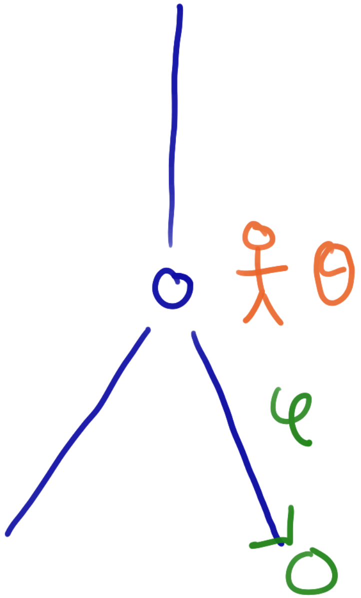
$$\varphi\theta\hat{\varphi}$$

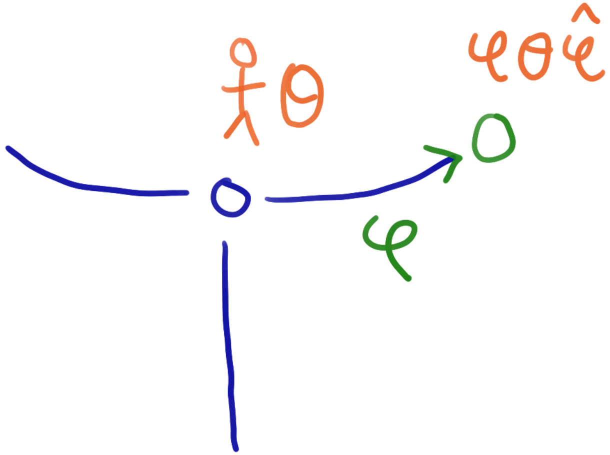
$\ell^2 \,\|\, \varphi\theta\hat{\varphi} \Leftrightarrow$ ascending

$\ell \,\|\, \varphi\theta\hat{\varphi} \Leftrightarrow$ horizontal

$\ell \nmid \varphi\theta\hat{\varphi} \Leftrightarrow$ descending

Can you use this to navigate in the ℓ-isogeny graph?





try one direction φ:

- the new orientation is $\varphi\theta\hat{\varphi}$

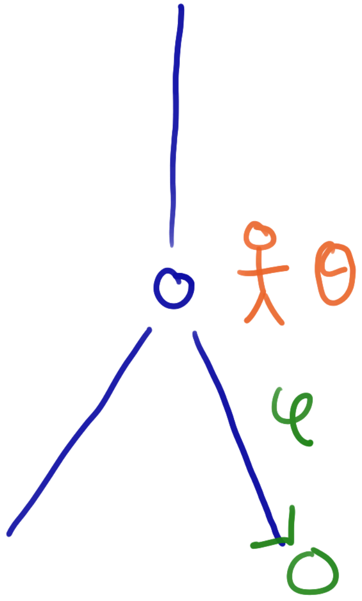
$\ell^2 \| \varphi\theta\hat{\varphi} \Leftrightarrow$ ascending

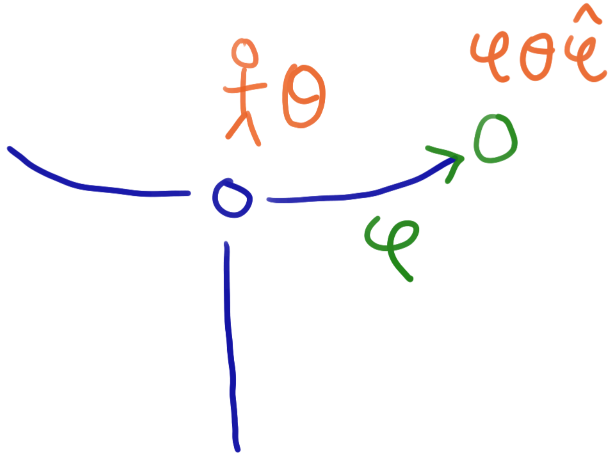
$\ell \| \varphi\theta\hat{\varphi} \Leftrightarrow$ horizontal

$\ell \nmid \varphi\theta\hat{\varphi} \Leftrightarrow$ descending

* This works if θ is ℓ-primitive & ℓ-suitable

Can you use this to navigate in the ℓ-isogeny graph?





try one direction φ:

- the new orientation is $\varphi\theta\hat{\varphi}$

$\ell^2 \| \varphi\theta\hat{\varphi} \Leftrightarrow$ ascending

$\ell \| \varphi\theta\hat{\varphi} \Leftrightarrow$ horizontal

$\ell \nmid \varphi\theta\hat{\varphi} \Leftrightarrow$ descending

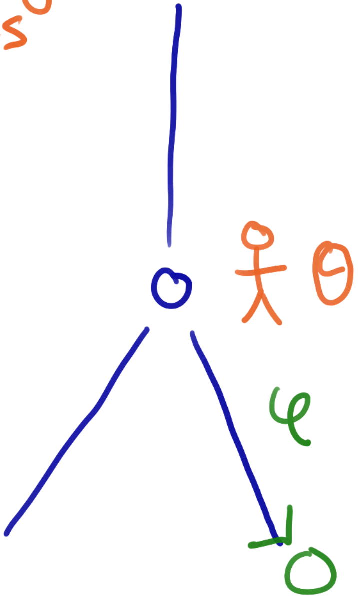
☆ This works if θ is ℓ-primitive & ℓ-suitable

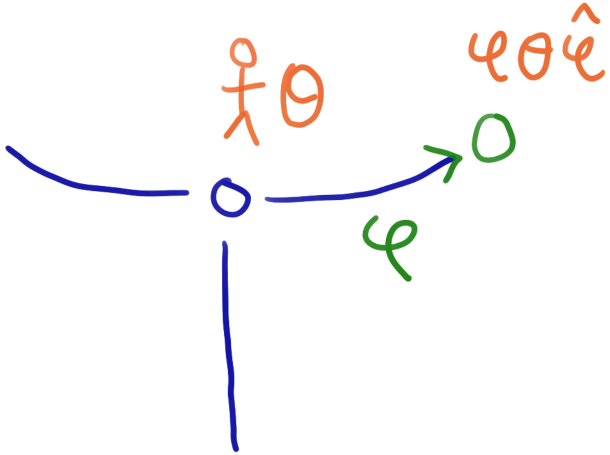
not div. by ℓ

fix by translation $\theta \mapsto \theta + n$

Can you use this to navigate in the ℓ-isogeny graph?

∃ another method using eigenvalues of θ





try one direction φ:

- the new orientation is $\varphi\theta\hat{\varphi}$

$\ell^2 \parallel \varphi\theta\hat{\varphi} \Leftrightarrow$ ascending

$\ell \parallel \varphi\theta\hat{\varphi} \Leftrightarrow$ horizontal

$\ell \nmid \varphi\theta\hat{\varphi} \Leftrightarrow$ descending

⚠ This works if θ is <u>ℓ-primitive</u> & <u>ℓ-suitable</u>

not div. by ℓ

fix by translation $\theta \mapsto \theta + n$

(ACLSST)

Thm There exists a classical algorithm:

Input: $\underset{\in \mathrm{End}(E)}{\Theta}$ with $|\Delta'| \leq p^2$, can be efficiently evaluated on pts.

Output: ℓ-isog. path of length $O(\log p + h_{\Delta'})$ from E to $j=1728$.

Runtime: $h_{\Delta'} L_d(\frac{1}{2})\,\mathrm{poly}(\log p)$

(ACLSST)

Thm There exists a classical algorithm:

ℓ-fundamental part of Δ_θ

Input: $\underset{\in \mathrm{End}(E)}{\theta}$ with $|\Delta'| \leq p^2$, can be efficiently evaluated on pts.

Output: ℓ-isog. path of length $O(\log p + h_{\Delta'})$ from E to $j=1728$.

Runtime: $h_{\Delta'} L_d(\frac{1}{2}) \,\mathrm{poly}(\log p)$

class #

$e^{O((\log d)^{1/2} (\log\log d)^{1/2})}$

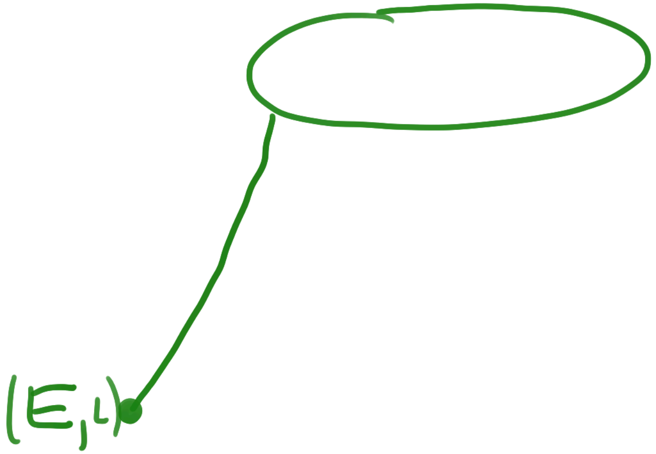
(ACLSST)

Thm There exists a classical algorithm:

Input: $\underset{\in \mathrm{End}(E)}{\theta}$ with $|\Delta'| \leq p^2$, can be efficiently evaluated on pts.

Output: ℓ-isog. path of length $O(\log p + h_{\Delta'})$ from E to $j=1728$.

Runtime: $h_{\Delta'} L_d(\tfrac{1}{2}) \operatorname{poly}(\log p)$



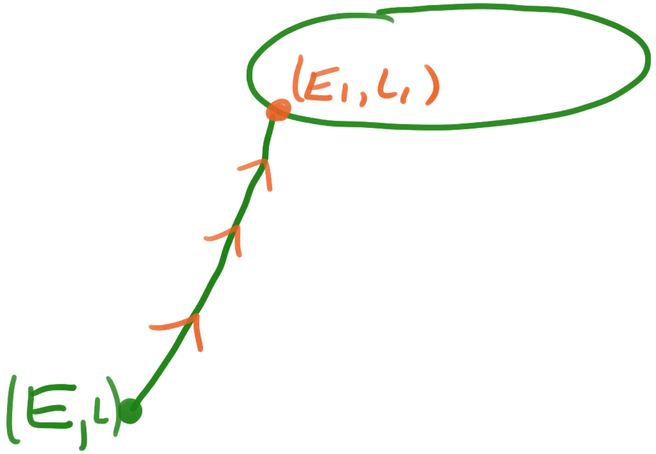
(ACLSST)

Thm There exists a classical algorithm:

Input: $\underset{\in \mathrm{End}(E)}{\theta}$ with $|\Delta'| \leq p^2$, can be efficiently evaluated on pts.

Output: ℓ-isog. path of length $O(\log p + h_{\Delta'})$ from E to $j=1728$.

Runtime: $h_{\Delta'} L_d(\frac{1}{2}) \mathrm{poly}(\log p)$



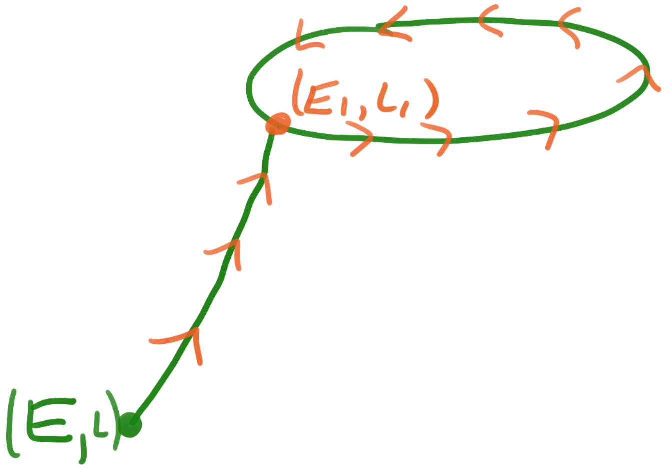
(ACLSST)

Thm There exists a classical algorithm:

Input: $\underset{\in \mathrm{End}(E)}{\theta}$ with $|\Delta'| \leq p^2$, can be efficiently evaluated on pts.

Output: ℓ-isog. path of length $O(\log p + h_{\Delta'})$ from E to $j=1728$.

Runtime: $h_{\Delta'} L_d(\frac{1}{2})\,\mathrm{poly}(\log p)$



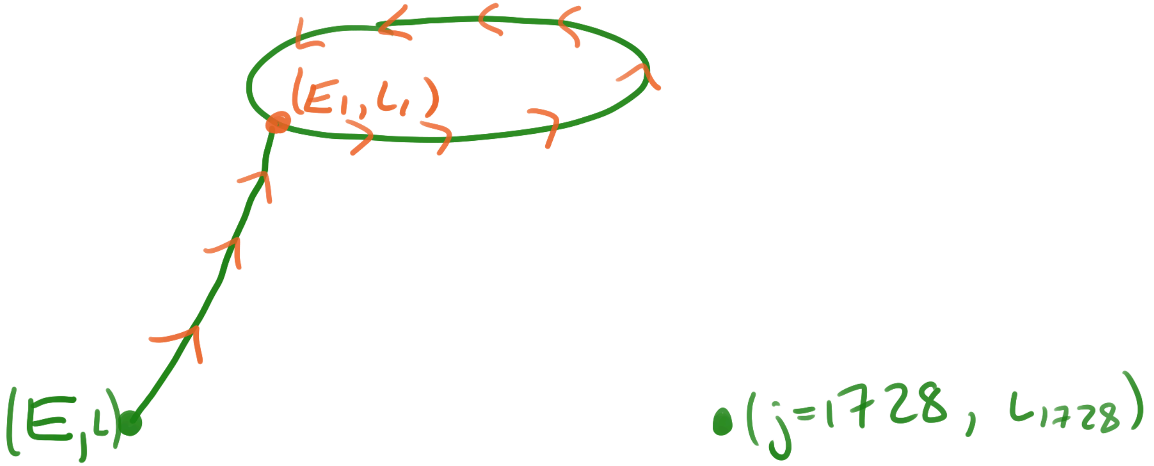
(ACLSST)

Thm There exists a classical algorithm:

Input: $\underset{\in \mathrm{End}(E)}{\theta}$ with $|\Delta'| \leq p^2$, can be efficiently evaluated on pts.

Output: ℓ-isog. path of length $O(\log p + h_{\Delta'})$ from E to $j=1728$.

Runtime: $h_{\Delta'} L_d(\frac{1}{2}) \operatorname{poly}(\log p)$



} <u>Subalgorithm:</u> orient 1728 by a given field

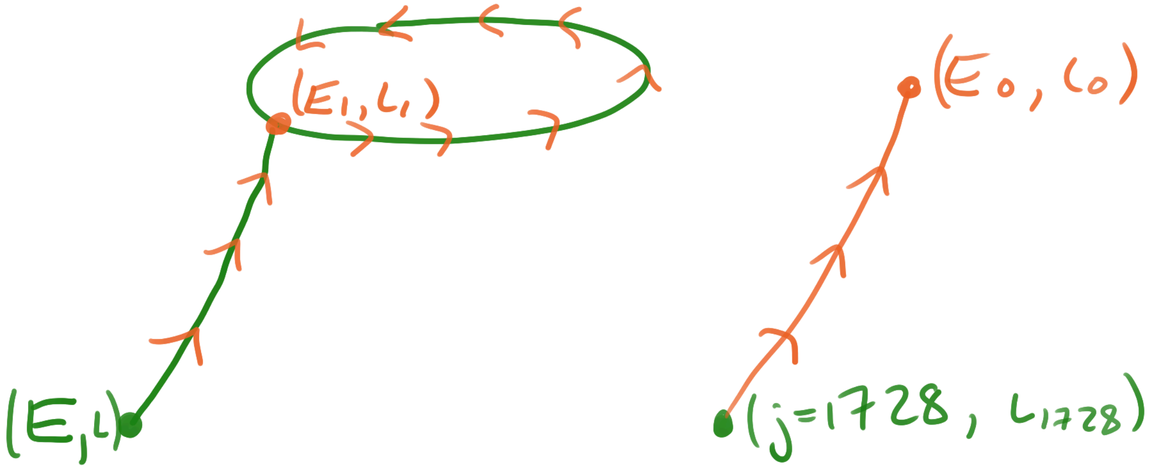
(ACLSST)

Thm There exists a classical algorithm:

Input: $\underset{\in \mathrm{End}(E)}{\theta}$ with $|\Delta'| \leq p^2$, can be efficiently evaluated on pts.

Output: ℓ-isog. path of length $O(\log p + h_{\Delta'})$ from E to $j=1728$.

Runtime: $h_{\Delta'} L_d\left(\frac{1}{2}\right) \mathrm{poly}(\log p)$



} **Subalgorithm:** orient 1728 by a given field

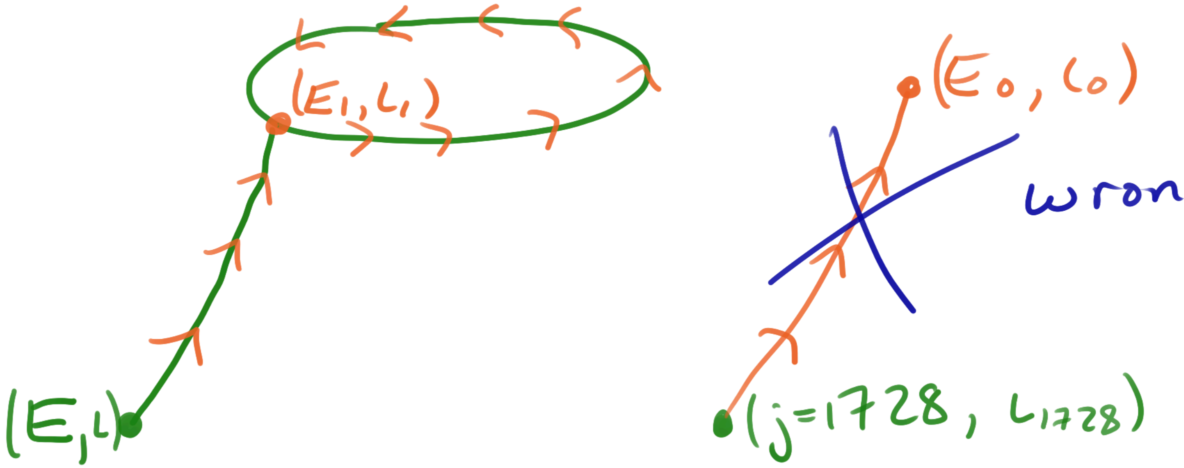
(ACLSST)

Thm There exists a classical algorithm:

Input: $\underset{\in \mathrm{End}(E)}{\theta}$ with $|\Delta'| \leq p^2$, can be efficiently evaluated on pts.

Output: ℓ-isog. path of length $O(\log p + h_{\Delta'})$ from E to $j=1728$.

Runtime: $h_{\Delta'} L_d(\frac{1}{2}) \, \mathrm{poly}(\log p)$



wrong volcano

} **Subalgorithm:**
orient 1728
by a given
field

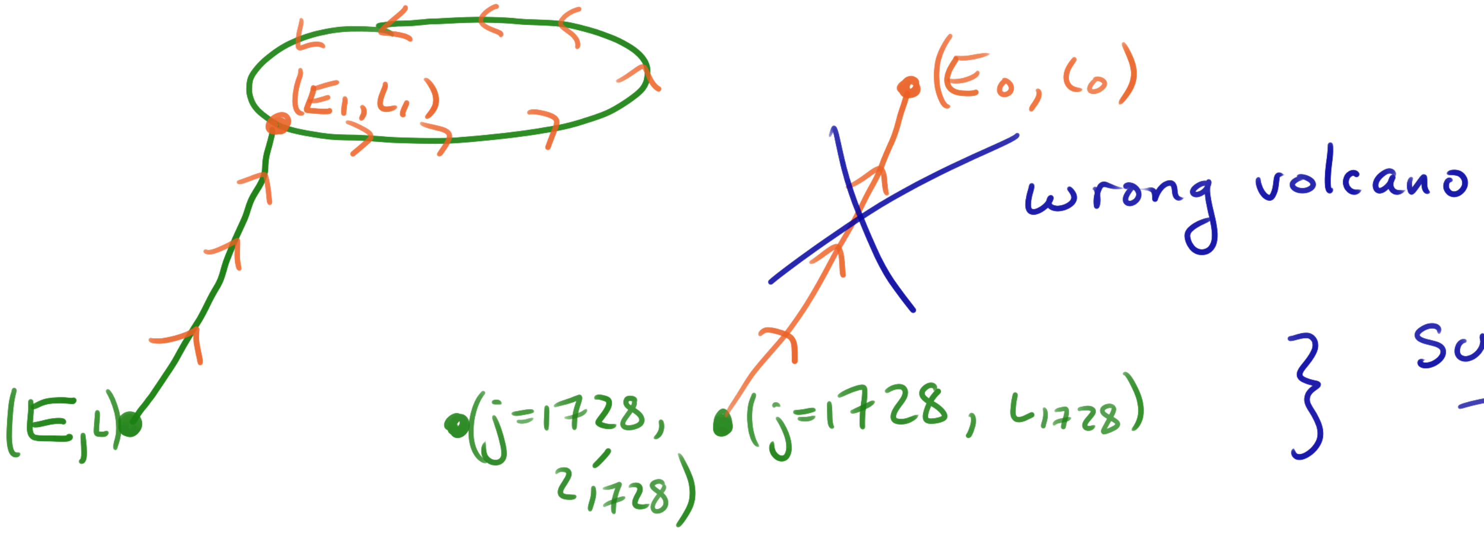
(ACLSST)

Thm There exists a classical algorithm:

Input: $\underset{\in \mathrm{End}(E)}{\theta}$ with $|\Delta'| \leq p^2$, can be efficiently evaluated on pts.

Output: ℓ-isog. path of length $O(\log p + h_{\Delta'})$ from E to $j=1728$.

Runtime: $h_{\Delta'} L_d(\frac{1}{2}) \mathrm{poly}(\log p)$



} subalgorithm: orient 1728 by a given field

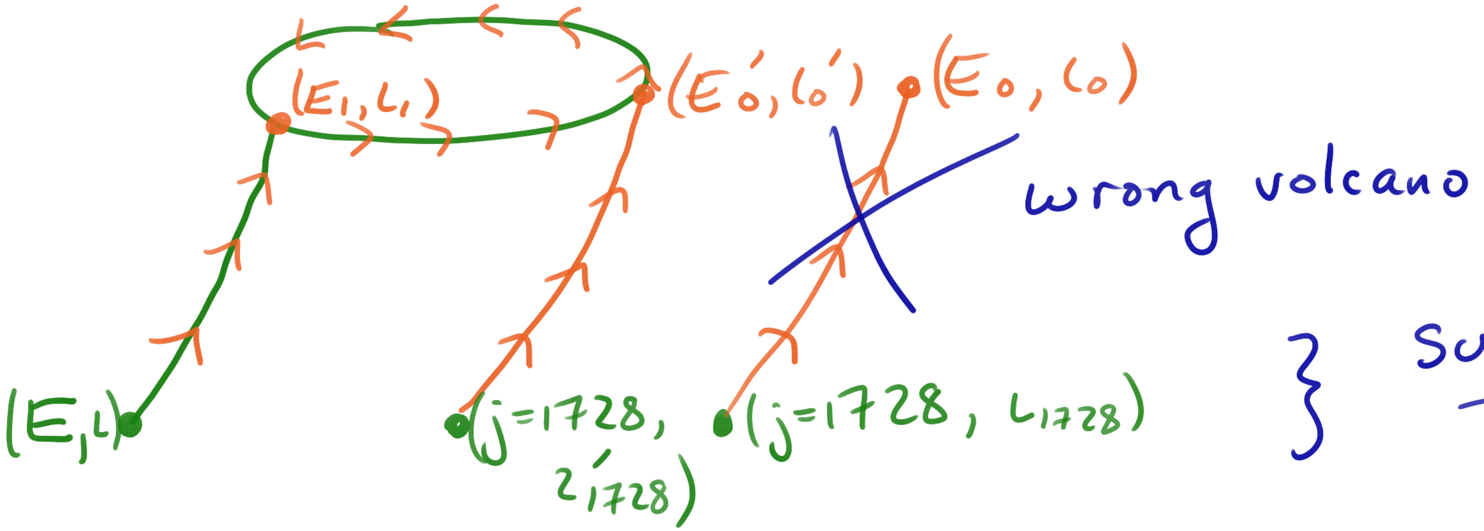
(ACLSST)

Thm There exists a classical algorithm:

Input: $\underset{\in \mathrm{End}(E)}{\theta}$ with $|\Delta'| \leq p^2$, can be efficiently evaluated on pts.

Output: ℓ-isog. path of length $O(\log p + h_{\Delta'})$ from E to $j=1728$.

Runtime: $h_{\Delta'} L_d(\tfrac{1}{2})\, \mathrm{poly}(\log p)$



} Subalgorithm: orient 1728 by a given field

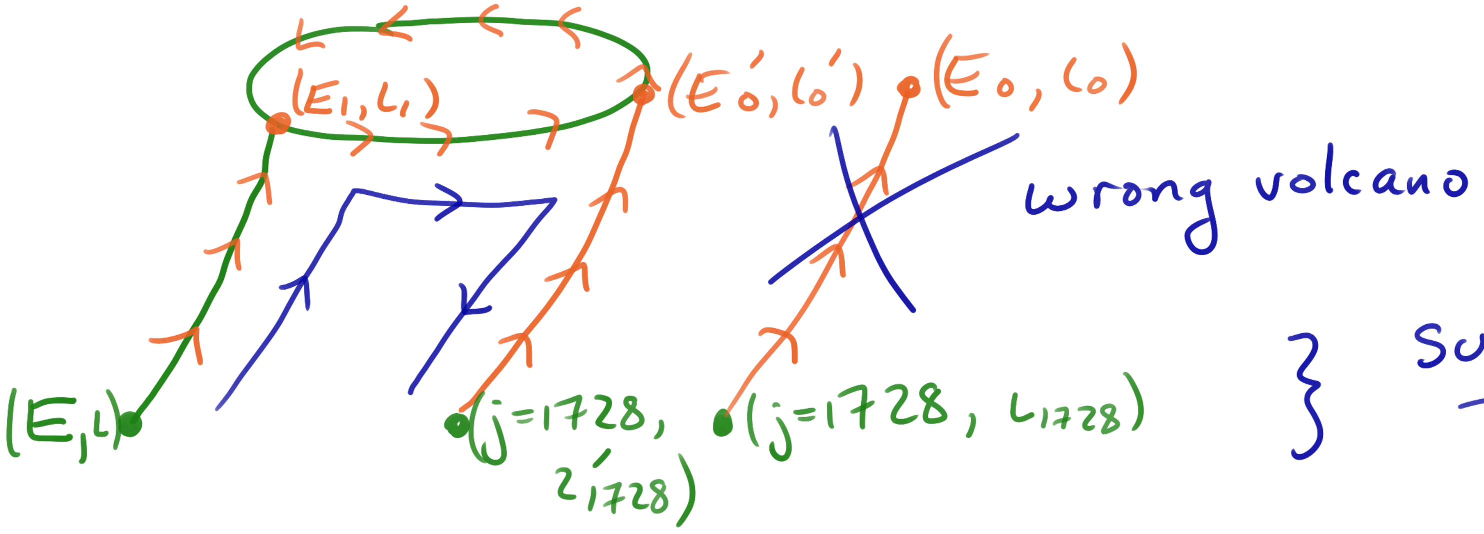
(ACLSST)

Thm There exists a classical algorithm:

Input: Θ with $|\Delta'| \leq p^2$, can be efficiently evaluated on pts.

Output: ℓ-isog. path of length $O(\log p + h_{\Delta'})$ from E to $j=1728$.

Runtime: $h_{\Delta'} L_d\left(\frac{1}{2}\right) \operatorname{poly}(\log p)$



} subalgorithm: orient 1728 by a given field

(ACLSST)

Thm There exists a classical algorithm:

Input: Θ with $|\Delta'| \le p^2$, can be efficiently evaluated on pts.

Output: ℓ-isog. path of length $O(\log p + h_{\Delta'})$ from E to $j=1728$.

Runtime: $h_{\Delta'} L_d(\frac{1}{2}) \,\mathrm{poly}(\log p)$

walking the rim

(expected size $h_{\Delta'}$)

(ACLSST)

Thm There exists a classical algorithm:

Input: θ with $|\Delta'| \leq p^2$, can be efficiently evaluated on pts.

Output: ℓ-isog. path of length $O(\log p + h_{\Delta'})$ from E to $j=1728$.

Runtime: $h_{\Delta'} L_d(\frac{1}{2})\,\mathrm{poly}(\log p)$

walking the rim

(expected size $h_{\Delta'}$)

at each step, need to translate

$$\theta \mapsto \theta + n$$

that is
- ℓ-suitable
- powersmooth degree

(ACLSST)

Thm There exists a classical algorithm:

Input: Θ with $|\Delta'| \leq p^2$, can be efficiently evaluated on pts.

Output: ℓ-isog. path of length $O(\log p + h_{\Delta'})$ from E to $j=1728$.

Runtime: $h_{\Delta'} L_d(\frac{1}{2}) \operatorname{poly}(\log p)$

walking the rim

(expected size $h_{\Delta'}$)

at each step, need to translate

$$\Theta \mapsto \Theta + n$$

that is
- ℓ-suitable
- powersmooth degree

solution: sieving (subexp.)

(ACLSST)

Thm. There exists a quantum algorithm:

Input: $\underset{\text{degree } d}{\theta} \in \mathrm{End}(E)$ with $d \ll |\Delta| \leq p^2$, efficient to evaluate

(ACLSST)

Thm. There exists a quantum algorithm:

Input: $\theta \in \mathrm{End}(E)$ with $d \ll |\Delta| \leq p^2$, efficient to evaluate
degree d

Output: An $L_{|\Delta|}(\frac{1}{2})$-smooth isogeny of norm $O(\sqrt{|\Delta|})$ to $j=1728$

Runtime: $L_{|\Delta|}(\frac{1}{2})\,\mathrm{poly}(\log p)$

(ACLSST)

Thm. There exists a quantum algorithm:

Input: $\theta \in \mathrm{End}(E)$ with $d \ll |\Delta| \leq p^2$, efficient to evaluate
degree d

Output: An $L_{|\Delta|}(\frac{1}{2})$-smooth isogeny of norm $O(\sqrt{|\Delta|})$ to $j=1728$

Runtime: $L_{|\Delta|}(\frac{1}{2})\,\mathrm{poly}(\log p)$

1) Find Δ' s.t. (E,θ) is $\mathcal{O}_{\Delta'}$-primitive (quantum HSP)

2) Repeat:
- orient 1728
- walk to rim (E_1, ι_1)
- check rim is $\mathcal{O}_{\Delta'}$-primitive (quantum HSP)

3) Find $[\mathfrak{a}] \in \mathcal{Cl}(\mathcal{O}_{\Delta'})$ s.t. $[\mathfrak{a}] \cdot (E, \iota_\theta) = (E_1, \iota_1)$

(quantum, adaptation of Childs-Jao-Soukharev)

(ACLSST)

Thm. There exists a quantum algorithm:

Input: $\theta \in \mathrm{End}(E)$ with $d << |\Delta| \leq p^2$, efficient to evaluate
degree d

Output: An $L_{|\Delta|}(\frac{1}{2})$-smooth isogeny of norm $O(\sqrt{|\Delta|})$ to $j=1728$

Runtime: $L_{|\Delta|}(\frac{1}{2})\,\mathrm{poly}(\log p)$

1) Find Δ' s.t. (E,θ) is $\mathcal{O}_{\Delta'}$-primitive (quantum HSP)

2) Repeat:
- orient 1728
- walk to rim (E_1, ι_1)
- check rim is $\mathcal{O}_{\Delta'}$-primitive (quantum HSP)

3) Find $[\mathfrak{a}] \in \mathcal{Cl}(\mathcal{O}_{\Delta'})$ s.t. $[\mathfrak{a}] \cdot (E, \iota_\theta) = (E_1, \iota_1)$

(quantum, adaptation of Childs-Jao-Soukharev)