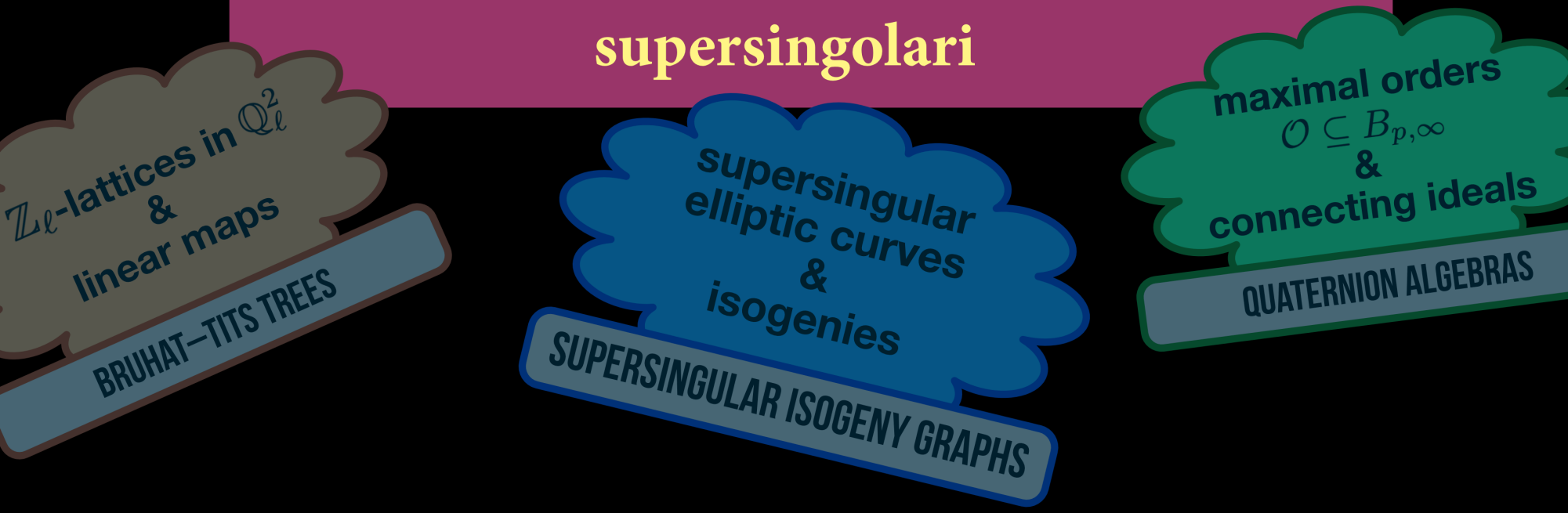
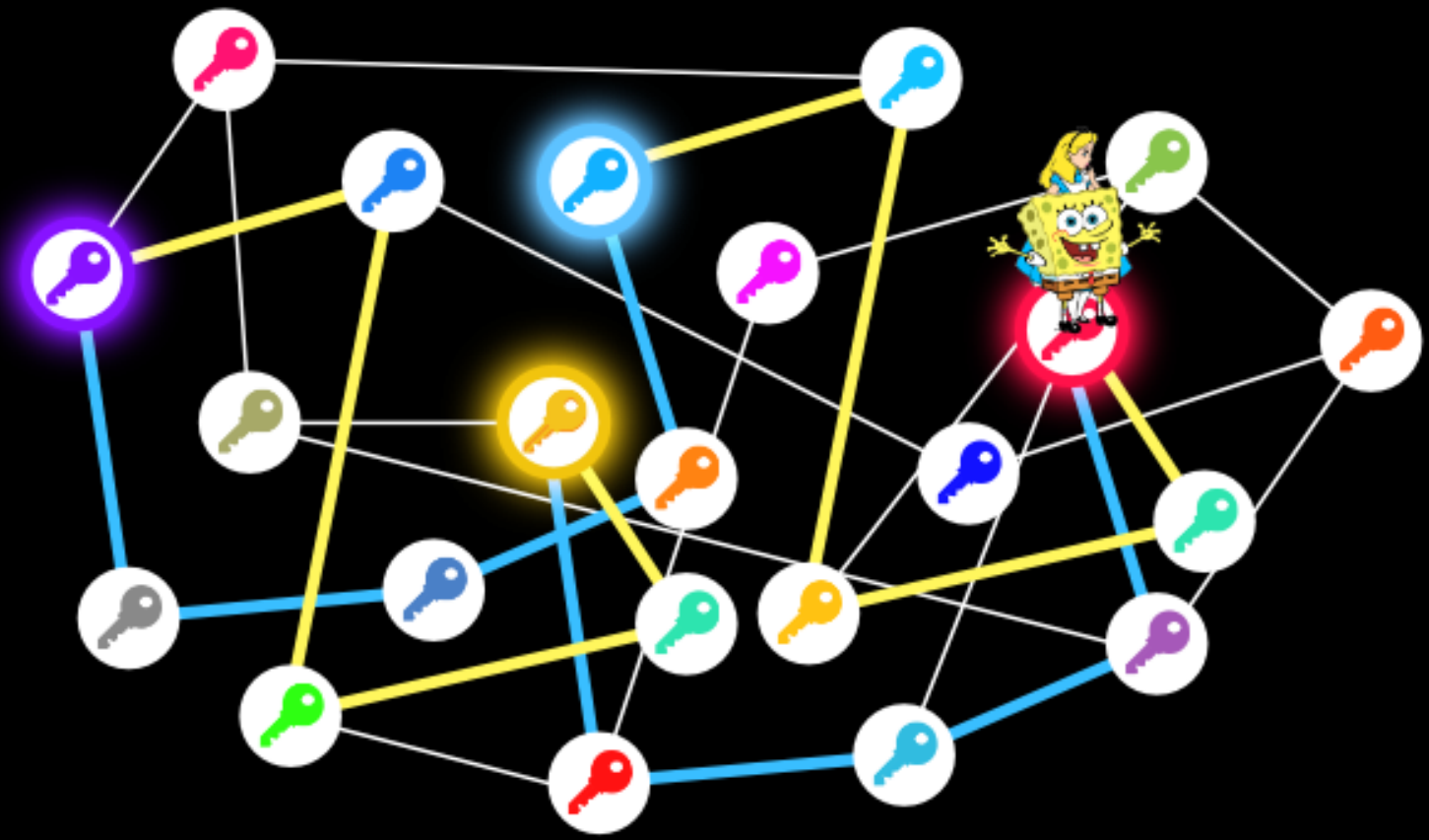
Strumenti per fare crittoanalisi nei grafi di isogenie supersingolari

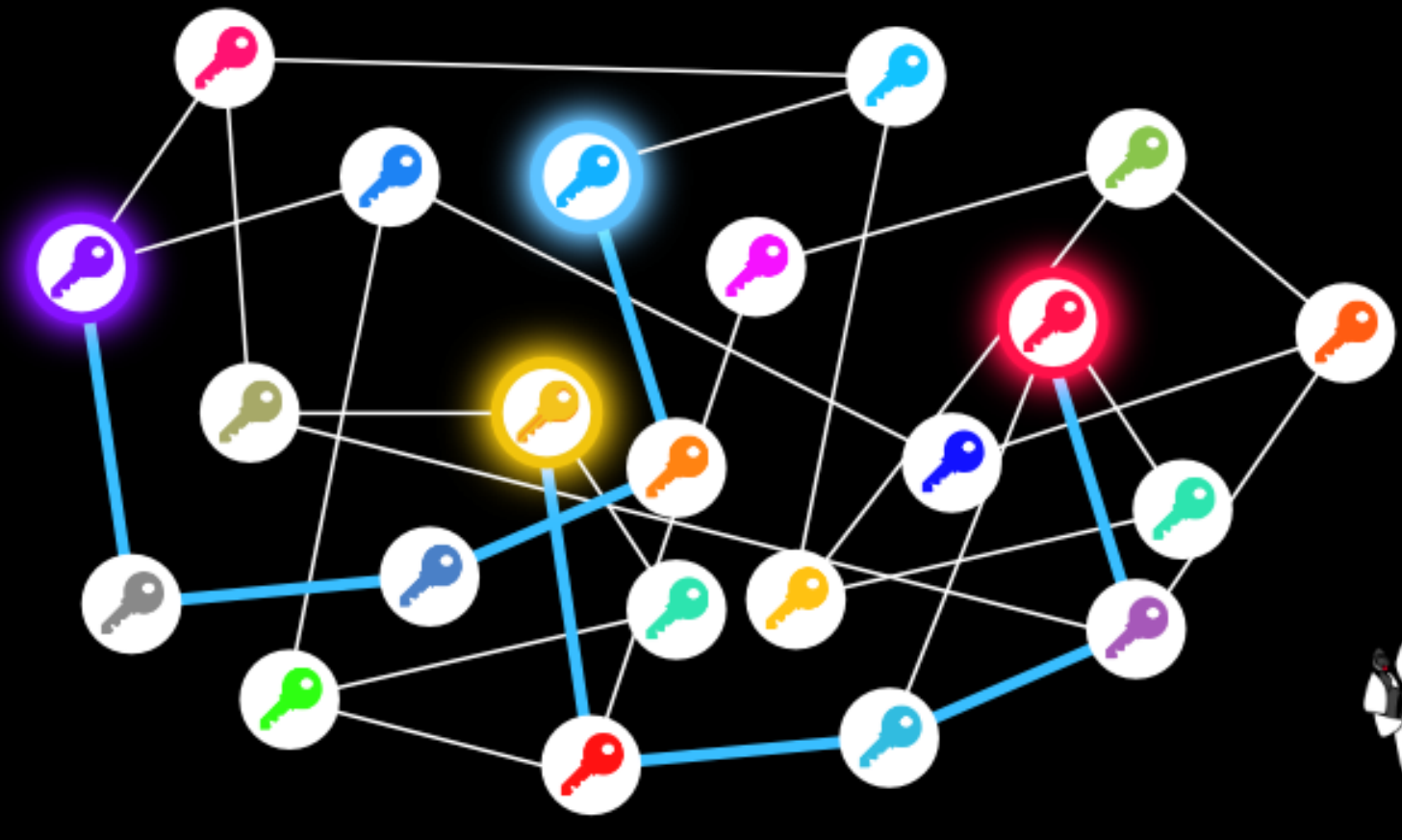


ANNAMARIA IEZZI

Université de la Polynésie Française

DE CIFRIS ATHESIS - 20 maggio, 2021





ROUTING FINDING PROBLEM

ISOGENY GRAPH

ISOGENY FINDING PROBLEM

Isogeny-based cryptography...

Elliptic curves

If $p := \mathrm{char}(\mathbb{F}_q) \neq 2, 3$, any **elliptic curve** defined over $\mathbb{F}_q$ is isomorphic to an elliptic curve E in Weierstrass affine form:

$$E : y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{F}_q, \quad 4A^3 + 27B^2 \neq 0.$$

$$E(\overline{\mathbb{F}}_q) = \{(x, y) \in (\overline{\mathbb{F}}_q)^2 : y^2 = x^3 + Ax + B\} \cup \{\infty\}.$$

To an elliptic curve in Weierstrass form we associate an element $j_E \in \mathbb{F}_q$, called j-invariant and defined as:

$$j_E := 1728 \cdot \frac{4A^3}{4A^3 + 27B^2} \in \mathbb{F}_q.$$

E_1 and E_2 are $\overline{\mathbb{F}}_q$-isomorphic $\Leftrightarrow j_{E_1} = j_{E_2}$

$$\left\{ \begin{array}{c} \overline{\mathbb{F}}_q\text{-isomorphism classes of} \\ \text{elliptic curves} \\ \text{defined over } \mathbb{F}_q \end{array} \right\} \overset{\text{bijection}}{\longleftrightarrow} \{j\text{-invariants in } \mathbb{F}_q\} = \mathbb{F}_q$$

Supersingular elliptic curves

Let $E/\mathbb{F}_q$ be an elliptic curve with $\mathrm{char}(\mathbb{F}_q) = p$. For n a positive integer, the n-torsion subgroup

$$E[n] := \{P \in E(\overline{\mathbb{F}}_q) : nP = O_E\} \leq E(\overline{\mathbb{F}}_q),$$

satisfies:

- $E[n] \cong \dfrac{\mathbb{Z}}{n\mathbb{Z}} \times \dfrac{\mathbb{Z}}{n\mathbb{Z}}$ if $(n, p) = 1$.
- $E[p^r] \cong \begin{cases} \frac{\mathbb{Z}}{p^r\mathbb{Z}} & \text{ordinary} \\ \{0\} & \text{supersingular} \end{cases}$

If $E/\overline{\mathbb{F}}_p$ is a supersingular elliptic curve, then $j_E \in \mathbb{F}_{p^2}$.

An element of $\mathbb{F}_{p^2}$ which is the j-invariant of a supersingular elliptic curve is called a supersingular j-invariant.

$$\sharp\left\{\begin{array}{c}\overline{\mathbb{F}}_p\text{-isomorphism classes of}\\ \text{supersingular elliptic curves}\\ \text{defined over } \overline{\mathbb{F}}_p\end{array}\right\} = \sharp\left\{\begin{array}{c}\text{supersingular}\\ j\text{-invariants in } \mathbb{F}_{p^2}\end{array}\right\} = \left[\frac{p}{12}\right] + \left\{\begin{array}{ll} 0 \text{ if } p \equiv 1 & (\mathrm{mod}\ 12)\\ 1 \text{ if } p \equiv 5, 7 & (\mathrm{mod}\ 12)\\ 2 \text{ if } p \equiv 11 & (\mathrm{mod}\ 12)\end{array}\right.$$

Isogenies

An **isogeny** $\varphi : E_1 \to E_2$ is a non-constant rational map which is also a group homomorphism. In particular an isogeny is surjective with finite kernel.

If E_1 and E_2 are in Weierstrass form, then φ can be written in standard affine form:

$$\begin{array}{rccc} \varphi : & E_1 & \longrightarrow & E_2 \\ & (x, y) & \mapsto & \left(\frac{f_1(x)}{g_1(x)}, \frac{f_2(x)}{g_2(x)} y\right) \end{array}$$

where $f_1, g_1, f_2, g_2 \in \overline{\mathbb{F}}_q[x]$ and $\gcd(f_1, g_1) = \gcd(f_2, g_2) = 1$.

- The **degree** of φ is $\deg(\varphi) = \max\{\deg(f_1), \deg(g_1)\}$.
- If φ is separable, i.e. if $\left(\frac{f_1}{g_1}\right)' \neq 0$, then $\deg(\varphi) = \sharp \ker(\varphi)$.

Isogenies will be our connections between j-invariants.

Supersingular ℓ-isogeny graphs

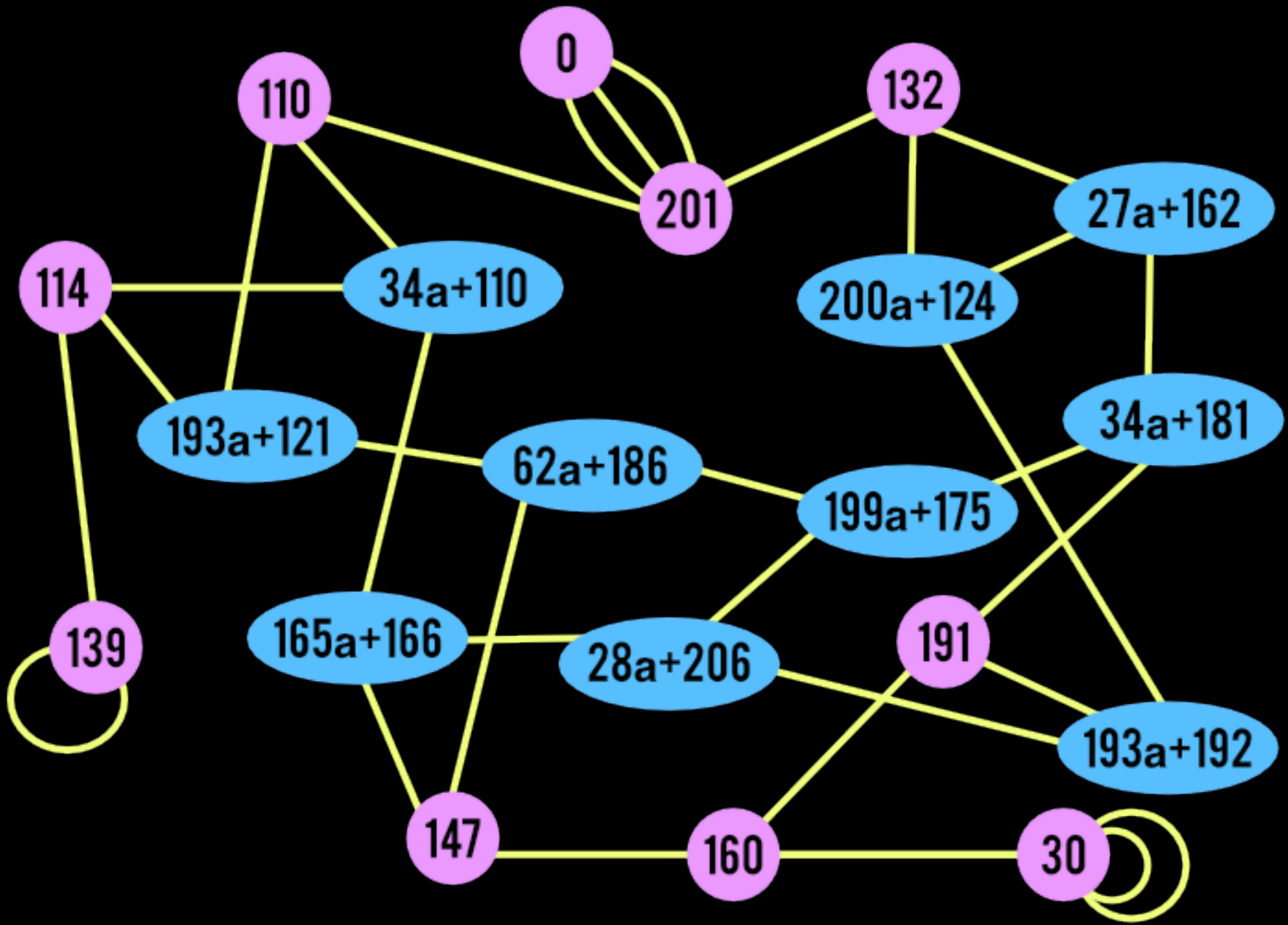
Let $p > 3$ and ℓ be primes such that $p \neq \ell$. We denote $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ the supersingular ℓ-isogeny graph over $\overline{\mathbb{F}}_p$ with:

- **Vertices:** supersingular j-invariants in $\mathbb{F}_{p^2}$.
- **Edges:** isogenies of degree ℓ (up to a certain equivalence. We also identify dual isogenies).

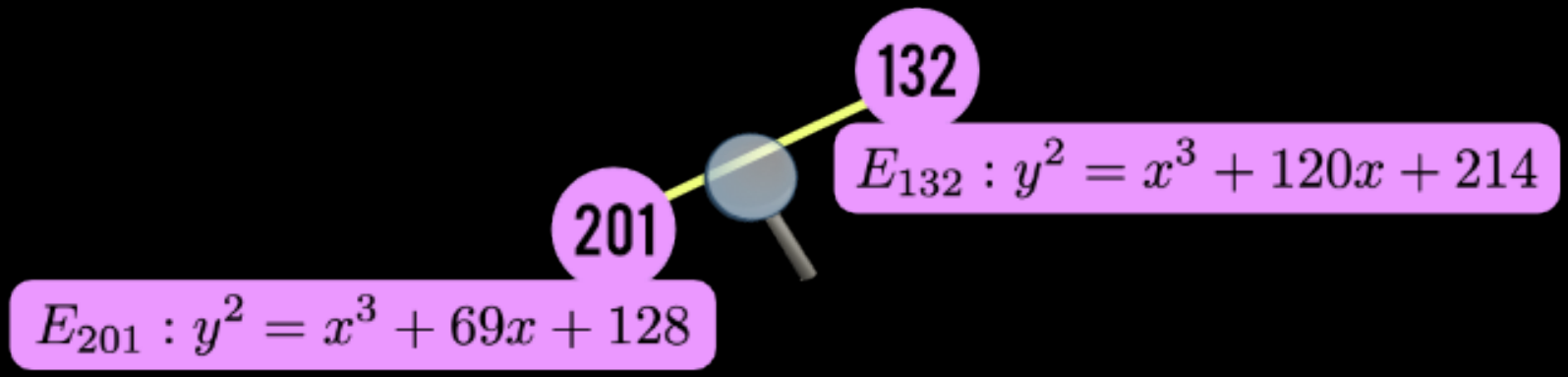
In practice (e.g. SIKE):

- p is a large prime number (> 400 bits)
- ℓ is a small prime number ($\ell = 2$ or 3)

$\mathcal{G}_2(\overline{\mathbb{F}}_{227})$



$\mathcal{G}_2(\overline{\mathbb{F}}_{227})$



$$\begin{array}{rccc} \varphi : & E_{201} & \to & E_{132} \\ & (x, y) & \mapsto & \left(\frac{x^2+84x-101}{x+84}, y\frac{x^2-59x-107}{x^2-59x+19} \right) \end{array}$$

Properties of supersingular isogeny graphs

A supersingular ℓ-isogeny graph over $\overline{\mathbb{F}}_p$ is:

- Exponentially large

  Approximately $\frac{p}{12}$ vertices

- Connected with diameter $O(\log(p))$

- $\ell + 1$-regular

  Except possibly at $j = 0$ or $j = 1728$ (because of the extra automorphisms).

- Ramanujan graph (i.e. optimal expander graphs)

  Relatively short walks on the graph approximate the uniform distribution.

Isogenies from kernels

Recall that if $\varphi : E_1 \to E_2$ is an isogeny, then $\ker(\varphi)$ is a finite subgroup of $E_1(\overline{\mathbb{F}}_p)$.

Let $E_1/\overline{\mathbb{F}}_p$ be an elliptic curve and let G be a finite subgroup of $E_1(\overline{\mathbb{F}}_p)$. Then, up to isomorphism, there exists a unique elliptic curve E_2 and a unique separable isogeny $\varphi : E_1 \to E_2$ with $\ker(\varphi) = G$.

We can build isogenies from their kernels using Vélu's formulas.

$$\begin{array}{c}\text{Separable isogeny from } E \\ \text{of prime degree } \ell \neq p\end{array} \longrightarrow G \leq E(\overline{\mathbb{F}}_p) \text{ cyclic subgroup of order } \ell$$

$$\forall P \in G, \ell P = O_E \Rightarrow G \subsetneq E[\ell] := \{P \in E(\overline{\mathbb{F}}_p) : \ell P = O_E\} \cong \frac{\mathbb{Z}}{\ell\mathbb{Z}} \times \frac{\mathbb{Z}}{\ell\mathbb{Z}}.$$

There are $\ell + 1$ cyclic subgroups of order ℓ in $E[\ell]$.

SIKE (see [3] and [4])

Public parameters:

- Prime $p = 2^{e_A}3^{e_B} - 1$.
- Supersingular elliptic curve $E_0/\mathbb{F}_{p^2}$ of order $(p+1)^2$.
- A basis $\{P_A, Q_A\}$ for $E[2^{e_A}]$ and a basis $\{P_B, Q_B\}$ for $E[3^{e_B}]$.

$0 \leq n_A < 2^{e_A}$

$0 \leq n_B < 3^{e_B}$

$E_A, \varphi_A(P_B), \varphi_A(Q_B)$

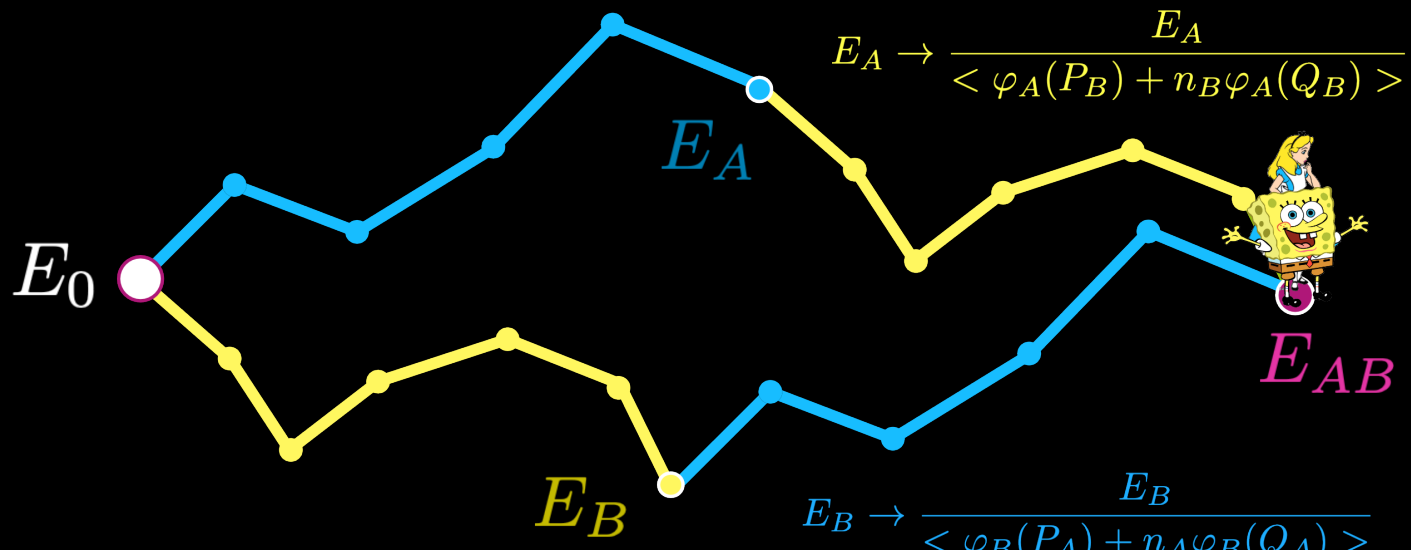
$E_B, \varphi_B(P_A), \varphi_B(Q_A)$

$$\varphi_A : E_0 \to \frac{E_0}{< P_A + n_A Q_A >} \cong E_A$$

$$E_A \to \frac{E_A}{< \varphi_A(P_B) + n_B \varphi_A(Q_B) >}$$

$$\varphi_B : E_0 \to \frac{E_0}{< P_B + n_B Q_B >} \cong E_B$$

$$E_B \to \frac{E_B}{< \varphi_B(P_A) + n_A \varphi_B(Q_A) >}$$

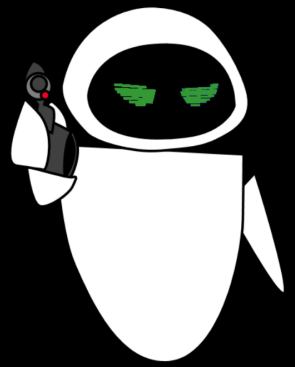


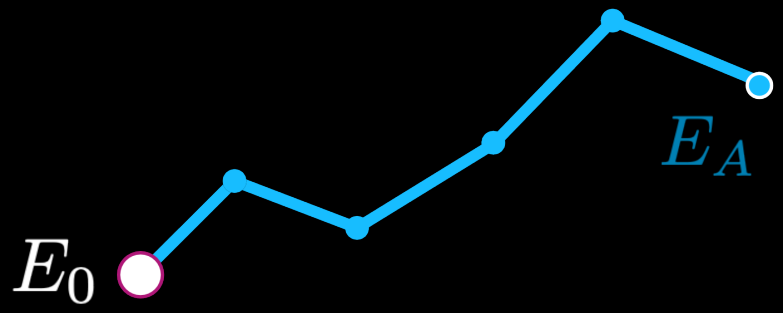
What Eve sees...

Isogeny finding problem

Given two ℓ^k-isogenous supersingular elliptic curves E_1 and E_2 defined over $\overline{\mathbb{F}}_p$, compute an isogeny

$$\varphi : E_1 \to E_2.$$



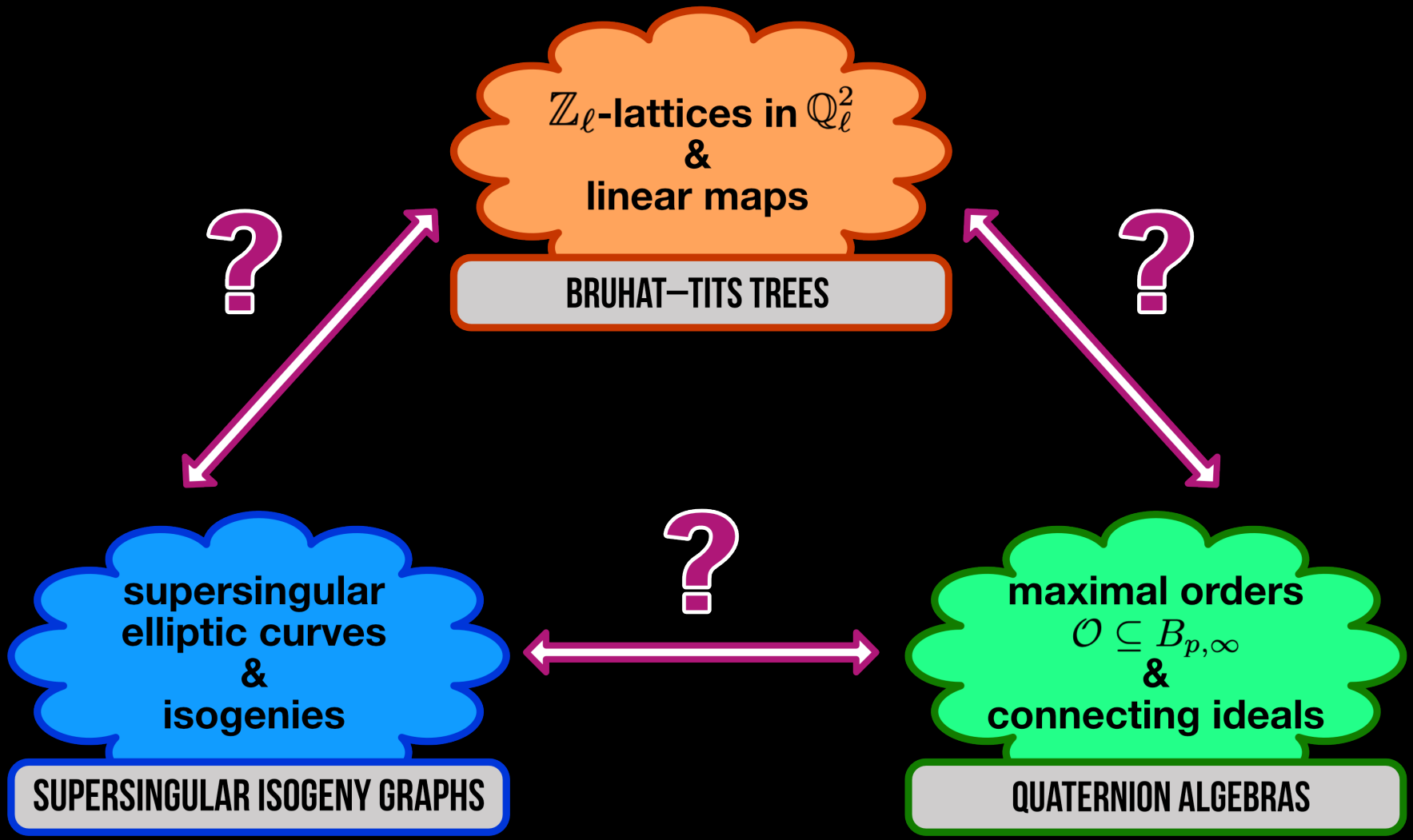


$E_A, \varphi_A(P_B), \varphi_A(Q_B)$

$E_B, \varphi_B(P_A), \varphi_B(Q_A)$

E_B

Three apparently different worlds



The quaternion algebras $B_{p,\infty}$

$B_{p,\infty}$: quaternion algebra ramified in p and ∞.

Example for $p \equiv 3 \pmod 4$:

$$B_{p,\infty} = \left(\frac{-1,-p}{\mathbb{Q}}\right) = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$$

such that

$$i^2 = -1,\ j^2 = -p,\ ij = -ji = k.$$

- For $\ell \neq p$, $B_{p,\infty} \otimes \mathbb{Q}_\ell \cong M_2(\mathbb{Q}_\ell)$.
- An ideal I of $B_{p,\infty}$: a $\mathbb{Z}$-lattice of rank 4.

$$I = \mathbb{Z}\alpha + \mathbb{Z}\beta + \mathbb{Z}\gamma + \mathbb{Z}\delta, \qquad \alpha, \beta, \gamma, \delta \in B_{p,\infty}.$$

- An order $\mathcal{O}$ of $B_{p,\infty}$: an ideal which is also a subring.

Given two maximal orders $\mathcal{O}_1$ and $\mathcal{O}_2$, I is a connecting ideal for $\mathcal{O}_1$ and $\mathcal{O}_2$

$$\mathcal{O}_1 \overset{I}{\longleftrightarrow} \mathcal{O}_2$$

if $\mathcal{O}_L(I) := \{\alpha \in B_{p,\infty} : \alpha I \subseteq I\} = \mathcal{O}_1$ and $\mathcal{O}_R(I) := \{\alpha \in B_{p,\infty} : I\alpha \subseteq I\} = \mathcal{O}_2$.

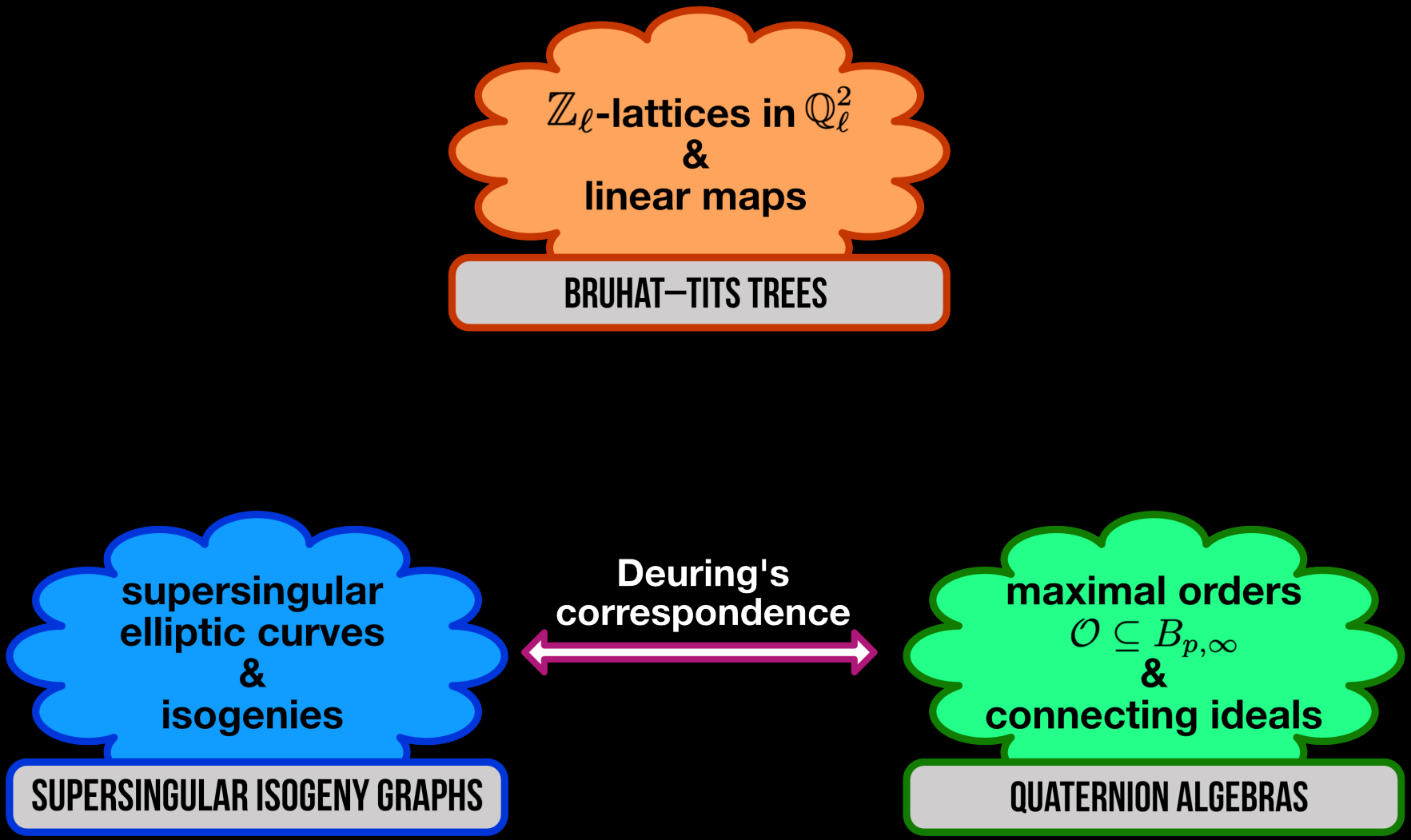
Deuring's correspondence

$$\mathrm{End}(E) = \{\text{isogenies } \varphi : E \to E\} \cup \{\text{zero morphism}\}$$

Elliptic curves	**Quaternion algebras**
$E/\overline{\mathbb{F}}_p$ supersingular elliptic curves up to Galois conjugacy	$\mathcal{O} \cong \mathrm{End}(E)$ maximal orders in $B_{p,\infty}$ up to isomorphism
$\varphi : E \to E'$ isogeny of $\deg(\varphi) = n$	I_φ left $\mathcal{O}$-ideal and right $\mathcal{O}'$-ideal of norm n

The isogeny finding problem can be reduced to the endomorphism ring computation problem (see [1] and [2]).

Connections



Bruhat-Tits trees

For each prime ℓ, we can define the Bruhat–Tits tree associated to $\mathrm{PGL}_2(\mathbb{Q}_\ell)$. Its vertices can be described as:

- classes of homothetic $\mathbb{Z}_\ell$-lattices in $\mathbb{Q}_\ell^2$;
- classes of equivalent norms on these lattices;
- classes of matrices in $\mathrm{PGL}_2(\mathbb{Q}_\ell)/\mathrm{PGL}_2(\mathbb{Z}_\ell)$;
- maximal orders in the quaternion algebra $\mathrm{M}_2(\mathbb{Q}_\ell)$.

Note that we use the notation $\mathbb{Q}_\ell$ for matching the notation from supersingular isogeny graphs.

Bruhat-Tits trees

For each prime ℓ, we can define the Bruhat–Tits tree associated to $\mathrm{PGL}_2(\mathbb{Q}_\ell)$. Its vertices can be described as:

- classes of homothetic $\mathbb{Z}_\ell$-lattices in $\mathbb{Q}_\ell^2$;
- classes of equivalent norms on these lattices;
- classes of matrices in $\mathrm{PGL}_2(\mathbb{Q}_\ell)/\mathrm{PGL}_2(\mathbb{Z}_\ell)$;
- maximal orders in the quaternion algebra $\mathrm{M}_2(\mathbb{Q}_\ell)$.

Note that we use the notation $\mathbb{Q}_\ell$ for matching the notation from supersingular isogeny graphs.

Homotetic lattices of $\mathbb{Q}_\ell^2$

A lattice L of $\mathbb{Q}_\ell^2$ is a free $\mathbb{Z}_\ell$-module of rank 2 of $\mathbb{Q}_\ell^2$. If L is a lattice of $\mathbb{Q}_\ell^2$, then there exists two independent vectors $\mathbf{u}, \mathbf{v} \in \mathbb{Q}_\ell^2$ such that

$$\begin{aligned} L &= \langle \mathbf{u}, \mathbf{v} \rangle_{\mathbb{Z}_\ell} = \\ &= \mathbb{Z}_\ell \mathbf{u} + \mathbb{Z}_\ell \mathbf{v} \\ &= \{x\mathbf{u} + y\mathbf{v} : x, y \in \mathbb{Z}_\ell\} \end{aligned}$$

Example:

- For $\mathbf{u} = (1, 0)$ and $\mathbf{v} = (0, 1)$ we obtain $L = \mathbb{Z}_\ell^2$.

We say that two lattices L_1 and L_2 are homothetic if there exists $\lambda \in \mathbb{Q}_\ell^\times$ such that $L_1 = \lambda L_2$. We denote $[L]$ the homothety class of a lattice L.

For instance $L = \langle \mathbf{u}, \mathbf{v} \rangle$ and $\ell L = \langle \ell\mathbf{u}, \ell\mathbf{v} \rangle$ are homothetic lattices.

Adjacent homothety classes

Two homothety classes $[L_1]$ and $[L_2]$ are said to be adjacent if their representatives L_1 and L_2 can be chosen so that

$$\ell L_1 \subsetneq L_2 \subsetneq L_1.$$

Remarks:

- This is a symmetric relation since if $\ell L_1 \subsetneq L_2 \subsetneq L_1$ then $\ell L_2 \subsetneq \ell L_1 \subsetneq L_2$ and $\ell L_1 \in [L_1]$.
- $\ell L_1 \subsetneq L_2 \subsetneq L_1$ if and only if L_2 is a cyclic sublattice of index ℓ in L_1.

Example:

- Given $L = \langle (1,0), (0,1) \rangle_{\mathbb{Z}_\ell}$ there are $\ell + 1$-lattices L_i such that $\ell L \subsetneq L_i \subsetneq L$:

$$L_i = \langle (1,i), (0,\ell) \rangle_{\mathbb{Z}_\ell}, \text{ for } i = 0, \ldots, \ell - 1$$
$$L_\infty = \langle (\ell,0), (0,1) \rangle_{\mathbb{Z}_\ell}$$

The Bruhat-Tits tree for $\mathrm{PGL}_2(\mathbb{Q}_\ell)$

The Bruhat–Tits tree associated to $\mathrm{PGL}_2(\mathbb{Q}_\ell)$ is the graph $\mathcal{T}_\ell$ with

- $\mathrm{Ver}(\mathcal{T}_\ell)$: homothety classes of lattices of $\mathbb{Q}_\ell^2$.
- $\mathrm{Ed}(\mathcal{T}_\ell)$: set of pairs of adjacent homothety classes.

The (undirected) graph $\mathcal{T}_\ell$ is a $(\ell+1)$-regular infinite tree.

Note that we can represent each vertex as a class of matrices of $\mathrm{PGL}_2(\mathbb{Q}_\ell)$:

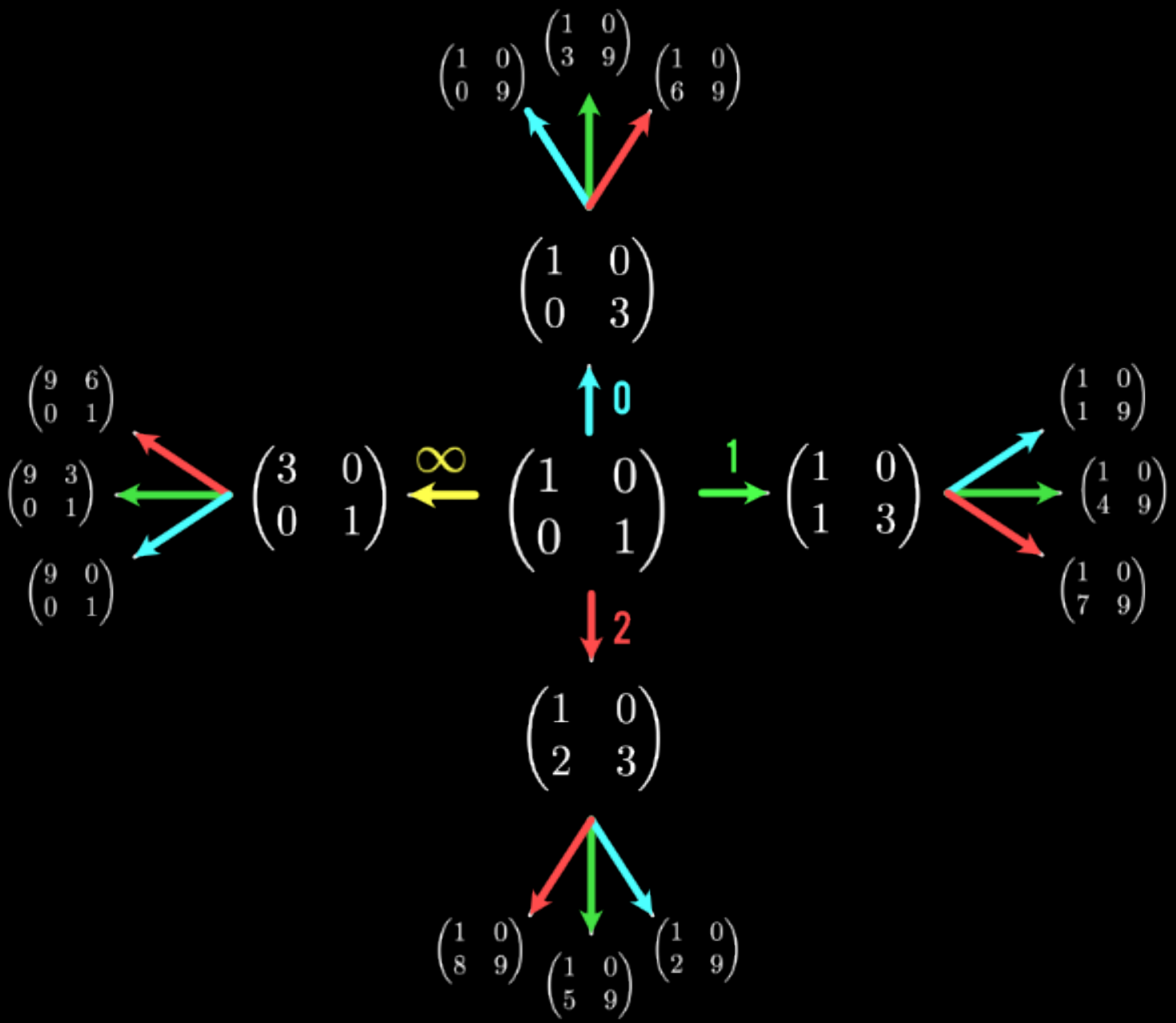
$$\{\text{homothety classes of lattices of } \mathbb{Q}_\ell^2\} \longrightarrow \mathrm{PGL}_2(\mathbb{Q}_\ell)$$

$$[L] = [\langle \mathbf{u}, \mathbf{v} \rangle_{\mathbb{Z}_\ell}] \mapsto [(\mathbf{u}|\mathbf{v})]$$

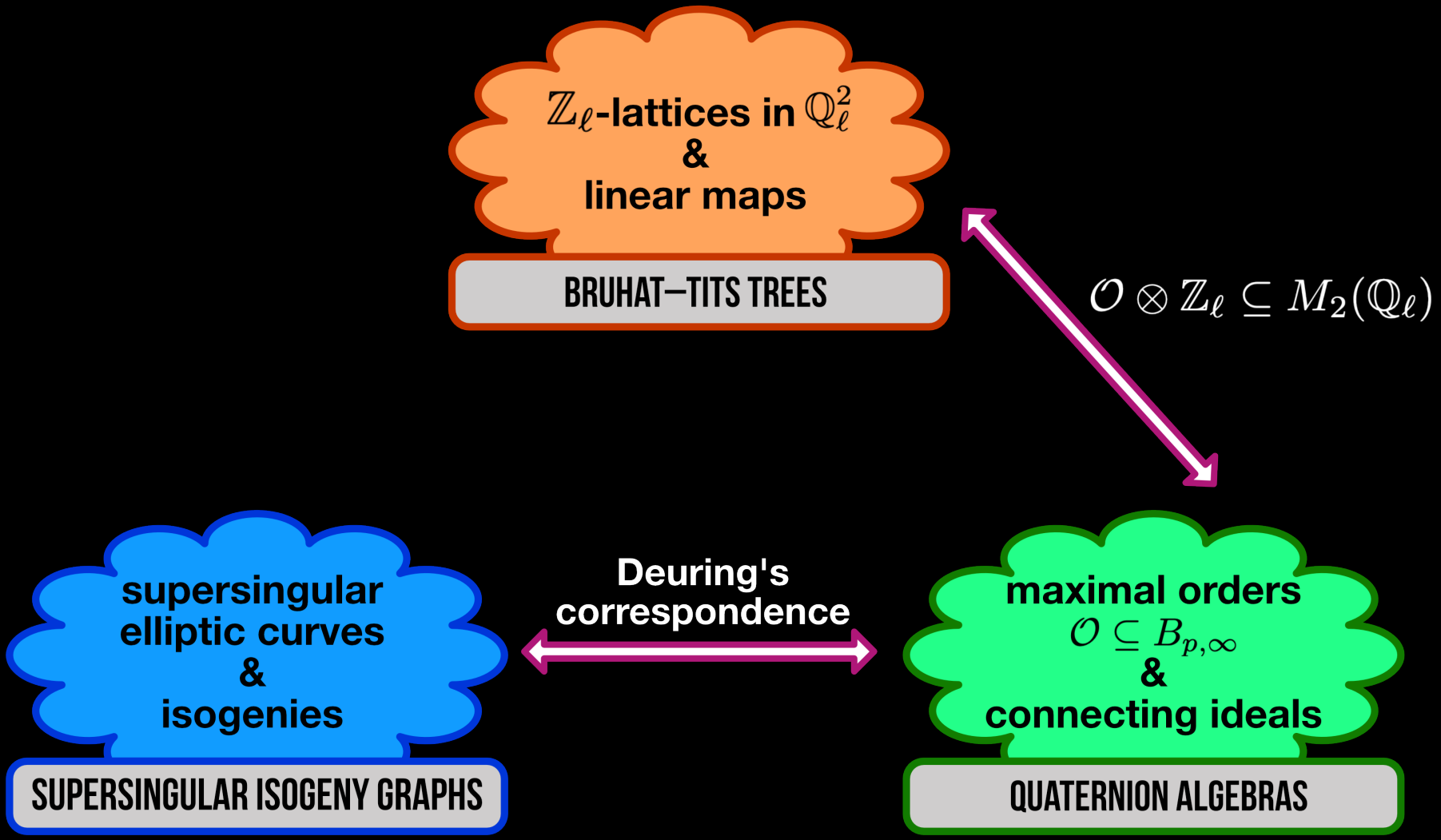
We have bijections:

$$\mathrm{Ver}(\mathcal{T}_\ell) \leftrightarrow \{\text{homothety classes of lattices of } \mathbb{Q}_\ell^2\} \leftrightarrow \mathrm{PGL}_2(\mathbb{Q}_\ell)/\mathrm{PGL}_2(\mathbb{Z}_\ell)$$

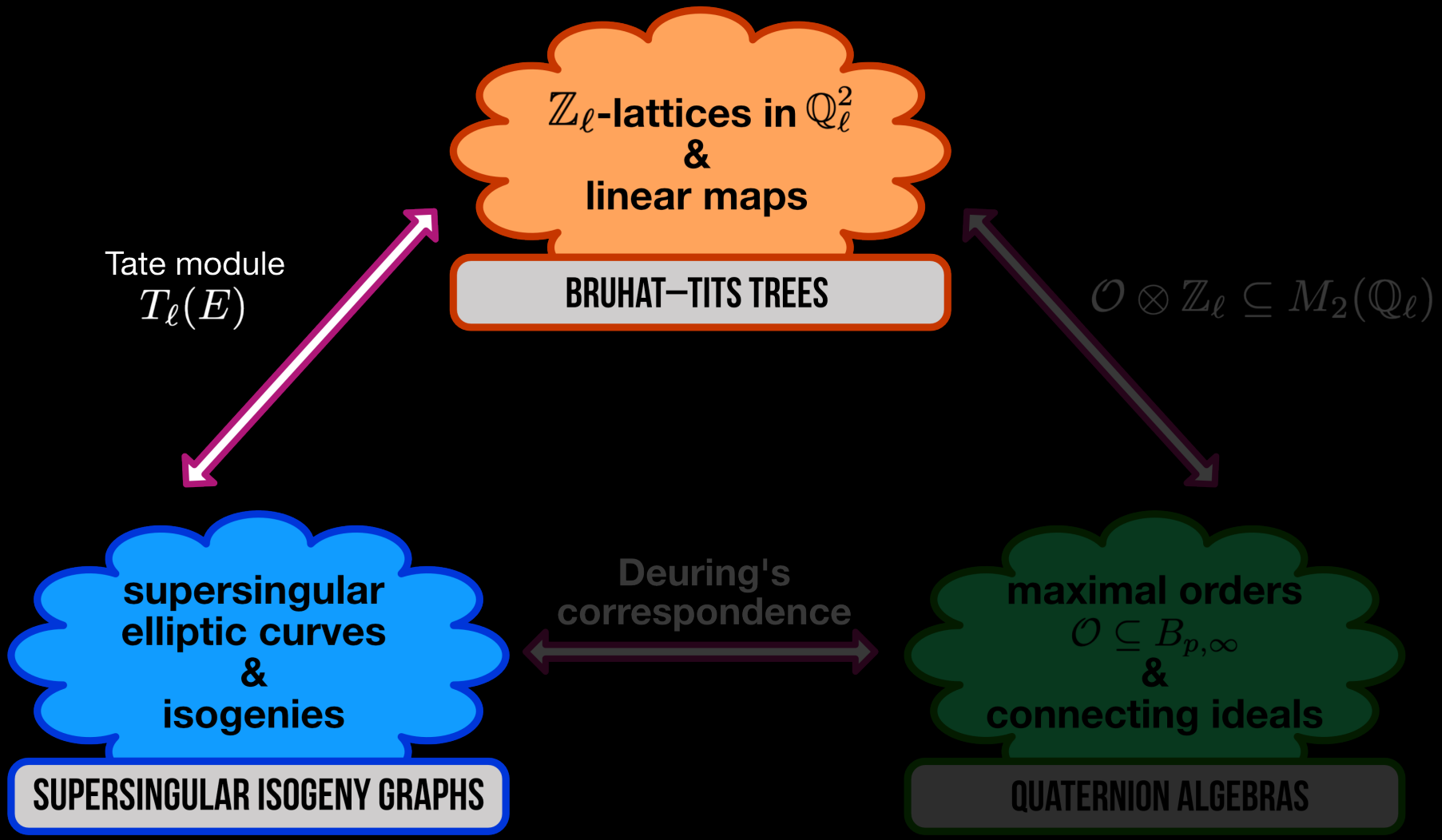
An example: $\mathcal{T}_3$



Connections



Connections



The ℓ-adic Tate module

Let $E/\overline{\mathbb{F}}_p$ be an elliptic curve and let $\ell \neq p$ be a prime. We have

$$E[\ell^n] \cong \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z},$$

as abelian groups. Moreover we have connecting maps

$$\begin{array}{rccc} [\ell]: & E[\ell^{n+1}] & \to & E[\ell^n] \\ & P & \mapsto & \ell P. \end{array}$$

The Tate module is defined to be the inverse limit of $E[\ell^n]$ with respect to these connecting maps:

$$T_\ell(E) = \varprojlim E[\ell^n] \cong \varprojlim \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z}.$$

There exists an isomorphism as $\mathbb{Z}_\ell$-modules

$$T_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell.$$

Note that an isogeny $\phi : E_1 \to E_2$ induces a $\mathbb{Z}_\ell$-linear map $\phi_\ell : T_\ell(E_1) \to T_\ell(E_2)$.

The Bruhat–Tits tree for the Tate module

Fix $\{P, Q\} = \{(P_n)_{n=1}^{\infty}, (Q_n)_{n=1}^{\infty}\}$, a basis of $T_\ell(E)$.

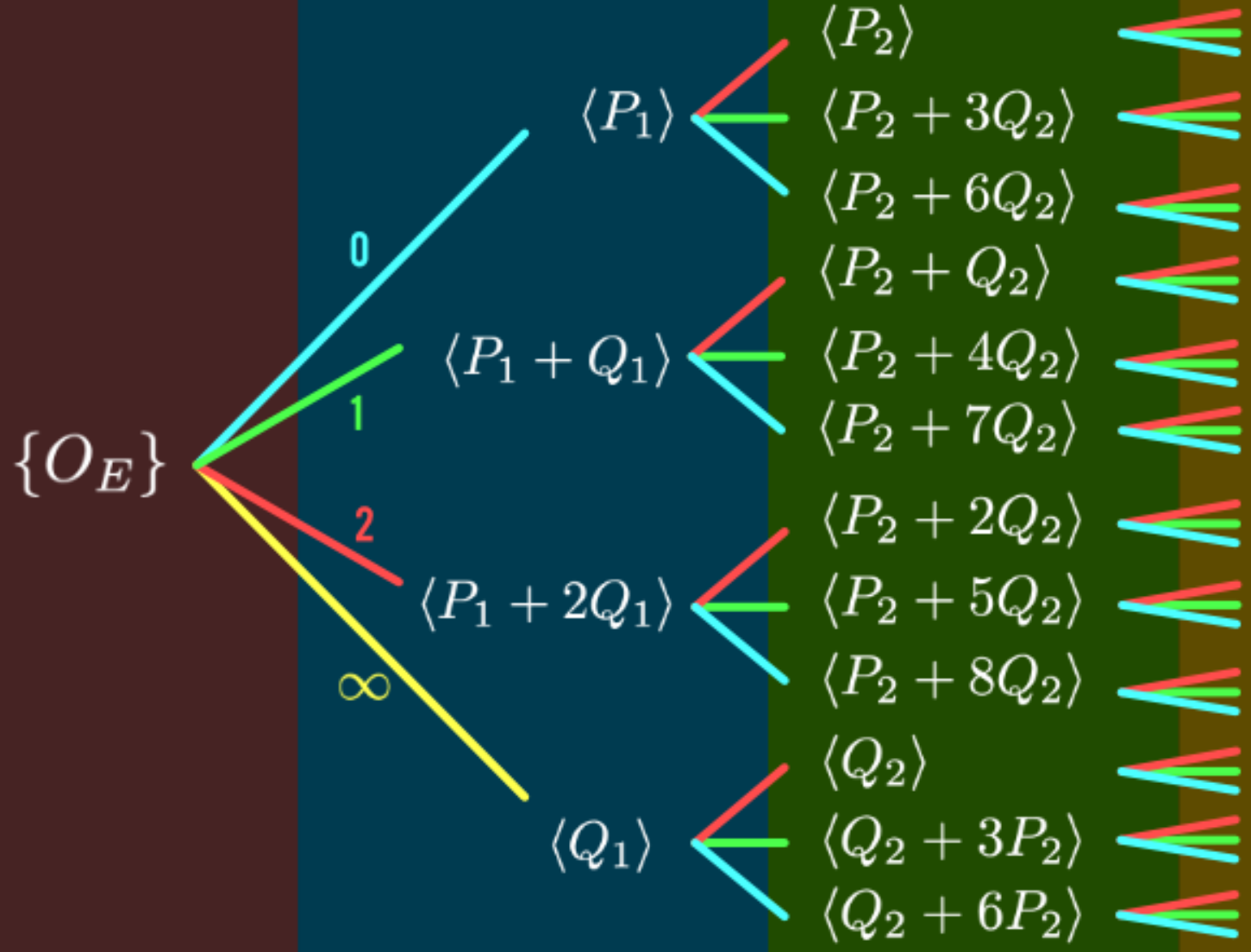
In particular $\{P_n, Q_n\}_{n=1}^{\infty}$ is a system of *compatible bases* of $E[\ell^n]$:

- $\{P_n, Q_n\}$ is a basis of $E[\ell^n]$, for all $n \geq 1$,
- $\ell P_{n+1} = P_n$, $\ell Q_{n+1} = Q_n$, for all $n \geq 1$.

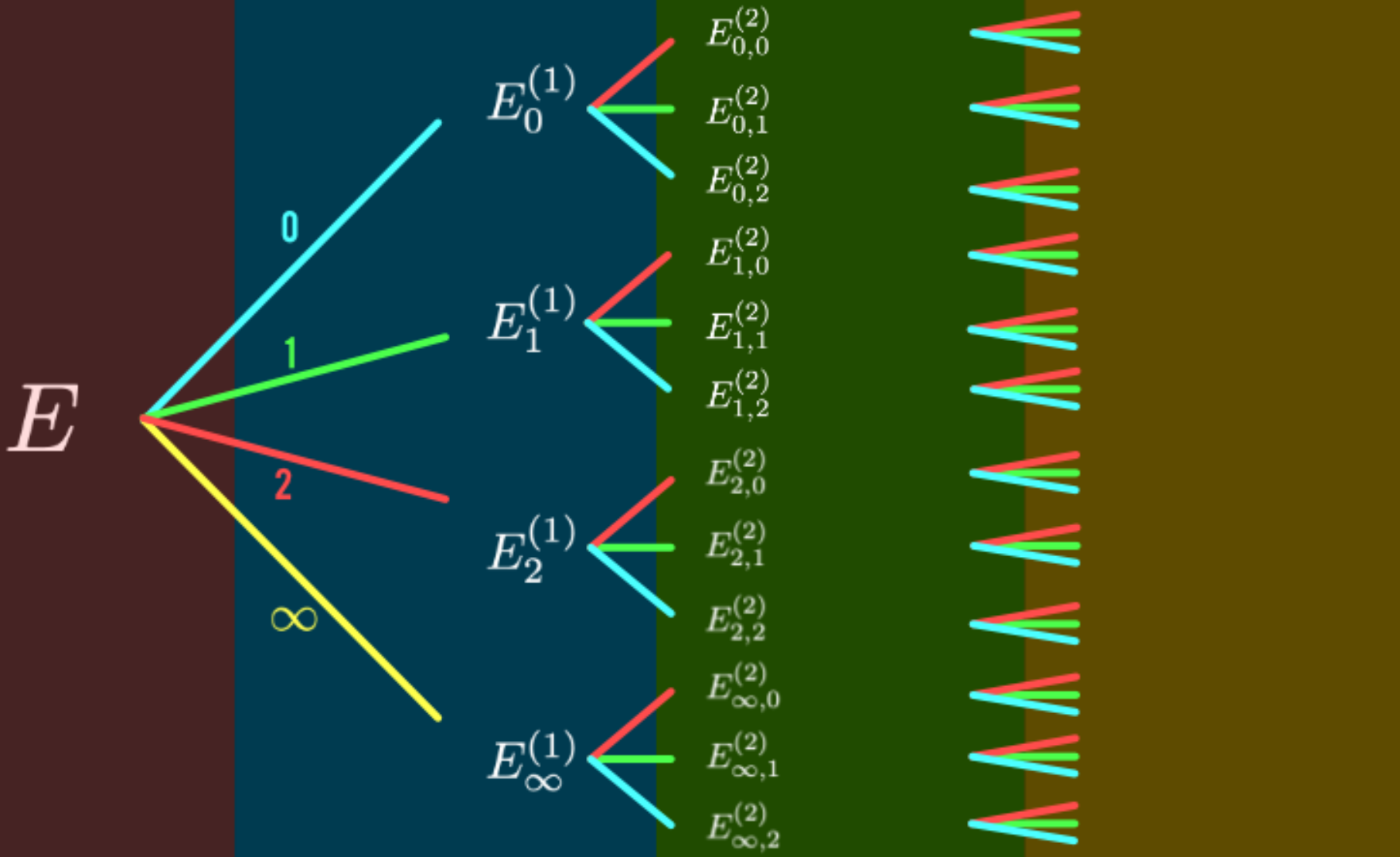
$$v^{(0)} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \longleftrightarrow T_\ell(E) = \langle P, Q \rangle$$

$$v^{(k)} \longleftrightarrow \text{a cyclic sublattice } L^{(k)} \text{ of } T_\ell(E) \text{ of index } \ell^k$$

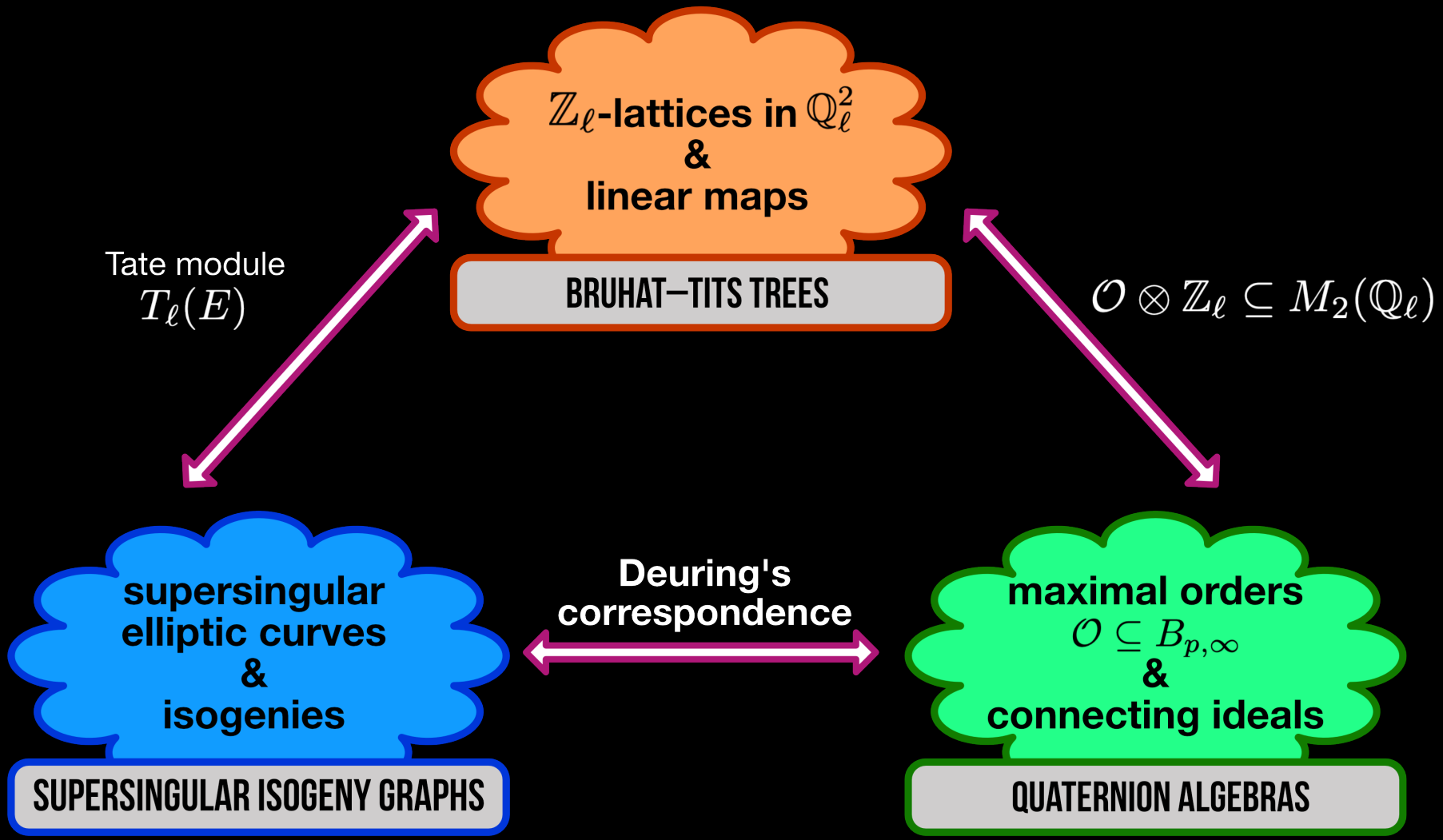
$$\begin{array}{ccc} L^{(k)} & & G^{(k)} \\ \text{cyclic sublattice of} & \to & \text{cyclic subgroup of} \\ T_\ell(E) \text{ of index } \ell^k & & E[\ell^k] \text{ of order } \ell^k \end{array} \quad \to \quad \begin{array}{c} E^{(k)} \cong \frac{E}{G^{(k)}}, \\ \text{elliptic curve} \\ \ell^k \text{ isogenous to } E \end{array}$$



$E[\ell^0] = \{O_E\}$ $E[\ell] = \langle P_1, Q_1 \rangle$ $E[\ell^2] = \langle P_2, Q_2 \rangle$ $E[\ell^k] = \langle P_k, Q_k \rangle$


E
0
1
2
∞
$E_0^{(1)}$
$E_1^{(1)}$
$E_2^{(1)}$
$E_\infty^{(1)}$
$E_{0,0}^{(2)}$
$E_{0,1}^{(2)}$
$E_{0,2}^{(2)}$
$E_{1,0}^{(2)}$
$E_{1,1}^{(2)}$
$E_{1,2}^{(2)}$
$E_{2,0}^{(2)}$
$E_{2,1}^{(2)}$
$E_{2,2}^{(2)}$
$E_{\infty,0}^{(2)}$
$E_{\infty,1}^{(2)}$
$E_{\infty,2}^{(2)}$
ℓ-isogenous to E
ℓ^2-isogenous to E
ℓ^k-isogenous to E

Conclusions



References

Explicit connections between supersingular isogeny graphs and Bruhat-Tits trees

Laia Amorós, Annamaria Iezzi, Kristin Lauter, Chloe Martindale, Jana Sotáková. (2021)

https://eprint.iacr.org/2021/372

Other references:

[1] Kirsten Eisenträger, Sean Hallgren, Kristin Lauter, Travis Morrison, and Christophe Petit. *Supersingular isogeny graphs and endomorphism rings : reductions and solutions*. In Advances in cryptology – EUROCRYPT 2018. Part III, volume 10822 of Lecture Notes in Comput. Sci., pages 329–368. Springer, Cham, 2018.

[2] David Kohel, Kristin Lauter, Christophe Petit, and Jean-Pierre Tignol. *On the quaternion ℓ-isogeny path problem*. LMS J. Comput. Math., 17(suppl. A):418–432, 2014.

[3] David Jao and Luca De Feo. *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies*. In Post-quantum cryptography, volume 7071 of Lecture Notes in Comput. Sci., pages 19–34. Springer, Heidelberg, 2011.

[4] SIKE, http://sike.org.