# LECTURE 3 Local solutions to the endomorphism problem

joint with Gabrielle Scullard

Compute $\mathrm{End}(E)$ from a subring.

**Setup**: $E/\mathbb{F}_{p^2}$ supersingular

Given $\mathcal{O}_0 \subseteq \mathrm{End}(E)$ of finite index in $\mathrm{End}(E)$.

**Goal**: Enlarge $\mathcal{O}_0$ locally and compute $\mathrm{End}(E) \otimes \mathbb{Z}_q$ for all primes $q$. Compute $\mathrm{End}(E)$ from local data.

This is possible by local-global principle.

- An order $\mathcal{O} \subseteq B_{p,\infty}$ is maximal if and only if for all primes $q$ $\mathcal{O} \otimes \mathbb{Z}_q$ is maximal.
- Our input order $\mathcal{O}_0$ will be maximal at all primes $q$ that do not divide discrd(

**DEFN**: Given an order $\mathcal{O}_0 \subseteq B_{p,\infty}$ with $\mathbb{Z}$-basis $\alpha_1, \ldots, \alpha_4$ define the discriminant of $\mathcal{O}_0$ to be

$$\operatorname{disc}(\mathcal{O}_0) := \left| \det (\operatorname{Trd} \alpha_i \alpha_j)_{ij} \right|$$

$$\operatorname{Trd}(\alpha) = \alpha + \bar{\alpha}$$

$\operatorname{disc}(\mathcal{O}_0) > 0$; in fact, it is a square

the reduced discriminant, $\operatorname{discrd}(\mathcal{O})$ = pos. square root of $\operatorname{disc}(\mathcal{O})$.

- $\mathcal{O} \subseteq B_{p,\infty}$ is maximal $\iff \operatorname{discrd}(\mathcal{O}) = p$

**Fact**: $\mathcal{O} \subseteq B_{p,\infty}$ is not maximal at the primes dividing $\operatorname{discrd}(\mathcal{O})/p$.

So the input order $\mathcal{O}_0$ determines the primes $\ell$ where we have to enlarge it.

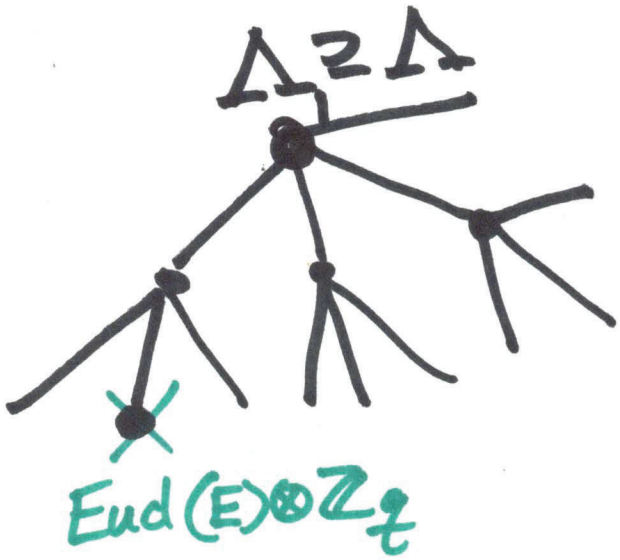
CASE 1: $q=p$

$B_{p,\infty} \otimes \mathbb{Q}_p$ is a division algebra
This has a unique maximal order,
which has to equal $\mathrm{End}(E) \otimes \mathbb{Z}_p$.
(can compute by work of Voight)

CASE 2: $q \neq p$ Here, $B_{p,\infty} \otimes \mathbb{Q}_q \simeq M_2(\mathbb{Q}_q)$

FACT: Every maximal order in $M_2(\mathbb{Q}_q)$
is conjugate to $M_2(\mathbb{Z}_q)$.
The maximal orders of $M_2(\mathbb{Q}_q)$
correspond to vertices in the
Bruhat-Tits tree $\mathcal{T}$ for $GL_2(\mathbb{Q}_q)$

Approach for CASE 2:
$\mathcal{O}_0 \subseteq \mathrm{End}(E) \Rightarrow \Lambda := \mathcal{O}_0 \otimes \mathbb{Z}_q \subseteq \mathrm{End}(E) \otimes$




If we find <u>one</u> max. order of $M_2(\mathbb{Q}_q)$, how far away from it could $End(E) \otimes \mathbb{Z}_q$ be?

At most distance $e = v_q(disrd(\mathcal{O}_0))$.

- Too expensive to check all of them.
- How would you even check that you have the right one?

$\hookrightarrow$ division test

The Bruhat-Tits tree $\mathcal{T}$

$\mathcal{T}$ is the undirected graph:

- vertices are rank 2 $\mathbb{Z}_q$-lattices in $\mathbb{Q}_q^2$ up to homothety.

$[L]$ and $[L']$ are connected by an edge $\Leftrightarrow \exists$ repres. lattices $L, L'$ s.t. $qL' \subsetneq L \subsetneq L'$.

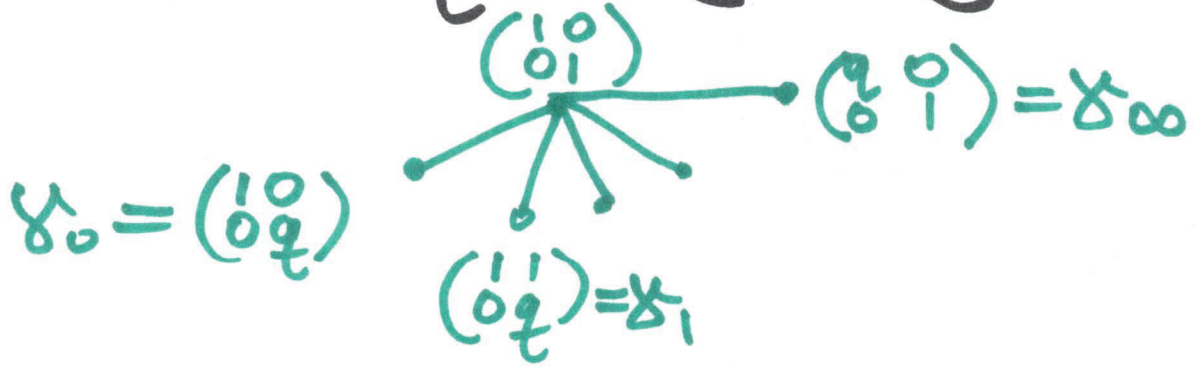
Equiv: vertices of $\mathcal{T}$ are max. orders of $M_2(\mathbb{Q}_q)$ via

$[L] \longrightarrow \mathrm{End}(L)$.

- maximal orders $\Lambda, \Lambda'$ are neighbors

$\Leftrightarrow [\Lambda : \Lambda \cap \Lambda'] = [\Lambda' : \Lambda \cap \Lambda'] = q$

- $\mathcal{T}$ is a $q+1$-regular graph




$q+1$ neighbors : can be repres. by $\Sigma = \{\gamma_c = \begin{pmatrix}1&c\\0&q\end{pmatrix} : 0 \le c \le q-1\} \cup \{\gamma_\infty\}$

Example $q=2$

$\begin{pmatrix}1&0\\0&1\end{pmatrix} \leftrightarrow M_2(\mathbb{Z}_q) = f(\mathcal{O}_q \otimes \mathbb{Z}_q)$

$\gamma_\infty = \begin{pmatrix}2&0\\0&1\end{pmatrix}$

$\leftrightarrow \gamma_\infty^{-1} M_2 \gamma_\infty$

$\gamma_0 = \begin{pmatrix}1&0\\0&2\end{pmatrix}$

$\leftrightarrow \gamma_0^{-1} M_2(\mathbb{Z}_q) \gamma_0$

$\gamma_1 = \begin{pmatrix}1&0\\0&\frac{1}{2}\end{pmatrix}$

$\updownarrow$

$\gamma_1^{-1} M_2(\mathbb{Z}_q) \gamma_1$

Step 1 : We enlarge $\mathcal{O}_0 \subseteq B_{p,\infty}$ to an order $\mathcal{O}_q \subseteq B_{p,\infty}$ s.t.

- $\mathcal{O}_0 \otimes \mathbb{Z}_{q'} = \mathcal{O}_q \otimes \mathbb{Z}_{q'}$, $q \neq q'$
- $\mathcal{O}_q \otimes \mathbb{Z}_q$ is maximal

Also choose $f: \mathcal{O}_q \otimes_{\mathbb{Z}} \mathbb{Q}_q \xrightarrow{\cong} M_2(\mathbb{Q}_q)$

s.t. $f(\mathcal{O}_q \otimes_{\mathbb{Z}} \mathbb{Z}_q) = M_2(\mathbb{Z}_q)$

Want to find : $\Lambda_E = f(\mathrm{End}(E) \otimes \mathbb{Z}_q)$

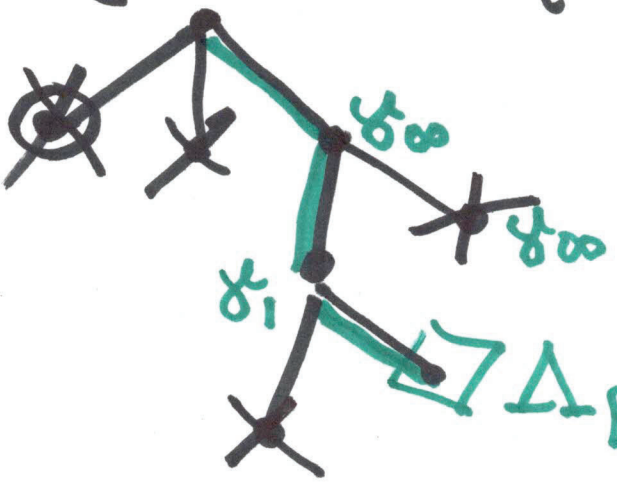
**PROPOSITION:** Let $r$ be the least integer $r$ s.t. $q^r \mathcal{O}_q \subseteq \mathrm{End}(E)$

Then $r = d(M_2(\mathbb{Z}_q), \Lambda_E)$.

**Example:** $q=2$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = f(\mathcal{O}_q \otimes \mathbb{Z}_q)$$

$r=3$




$$\gamma_0\gamma_\infty = \begin{pmatrix} 1 & 0 \\ 0 & q \end{pmatrix}\begin{pmatrix} q & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} q & 0 \\ 0 & q \end{pmatrix}$$

$\hookrightarrow$ backtracking