

Explicitly Computing

$$\begin{array}{c} \mathbb{Z} \hookrightarrow \mathbb{Z} \\ \mathbb{Q} \\ \mathbb{D} \subseteq \mathbb{E} \end{array}$$

$$GL_2(\mathbb{F}_\ell)$$

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \\ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\rho_{E,\ell} : G_{\mathbb{Q}} \rightarrow \text{Aut}(E[\ell])$$

E/\mathbb{Q} elliptic curve
 ℓ any prime

Theorem: $\cong \text{char poly}(\rho_{E,\ell}(\text{Frob}_p))$
 $\mathbb{F}_\ell[x]$

$$X^2 - a_p(E)X + p$$

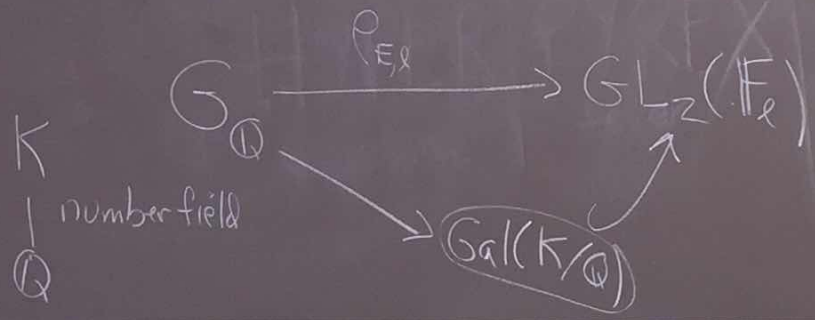
$$a_p(E) = p + 1 - \#E(\mathbb{F}_p)$$

$$\sigma \in G_{\mathbb{Q}} = \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$$

$$K = \mathbb{Q}(x(P), y(P); P \in E(\mathbb{Q})[\ell])$$

Galois extension

$$|a_p| \leq 2\sqrt{p}$$



K
 \mathbb{Q} number field

$p=2$.

$$\rho_{E,l}(\text{Frob}_p)$$

$$R_p = \mathbb{Z} \quad (\text{other primes})$$

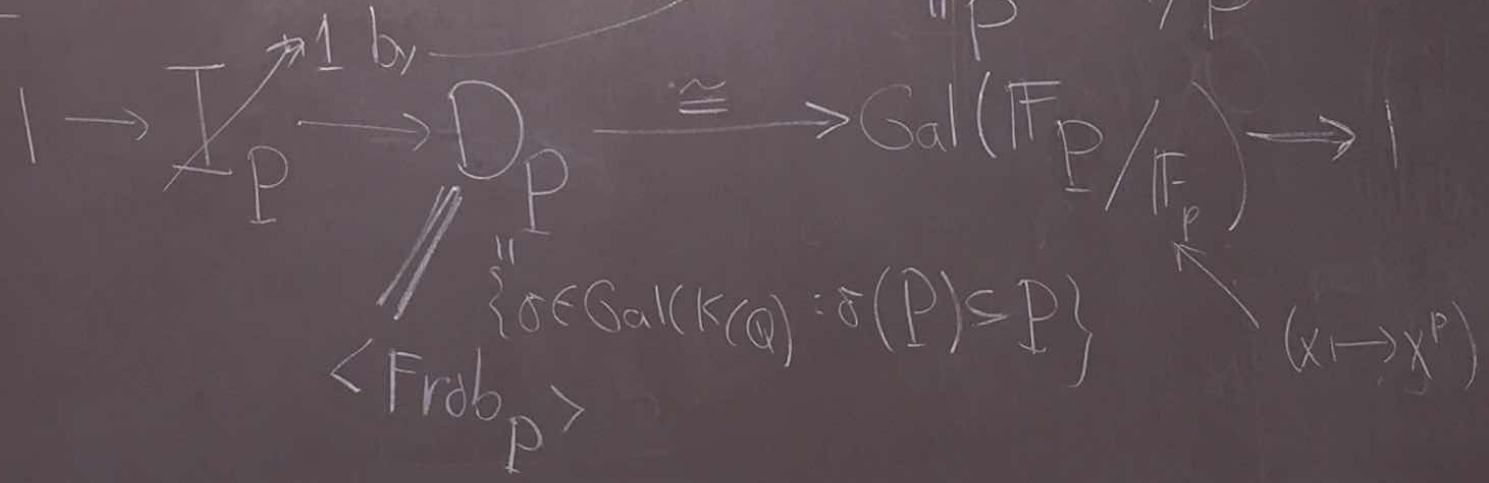
$$P \in \mathbb{Z}$$

$$\text{Frob}_p \in \text{Gal}(K/\mathbb{Q})$$

$p \in \mathbb{Z}$ prime unramified in K . (if $p \nmid l \cdot \Delta_E$ then $p \nmid \Delta_K$)

$$\text{Frob}_p \leftrightarrow P \in R = \mathcal{O}_K$$

$$\mathbb{F}_p = R/p$$



Explicitly Computing

$$\begin{array}{c} \mathbb{Z} \rightarrow \mathbb{Z} \\ \mathbb{Q} \\ \mathbb{0} \subseteq \mathbb{C} \end{array}$$

$$\text{Aut}(E[\ell]) \cong GL_2(\mathbb{F}_\ell)$$

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$\bar{\rho}_{E,\ell}$

$\ell = 5$

$E = 11a$

$\rho_{E,\ell}$

$G_{\mathbb{Q}}$

$\# E[5] = 25 = 1 + 12 + 12$

$\mathbb{Q}(\zeta_5) \subseteq \mathbb{Q}(E[5])$

conj. finitely often

$E[5] =$

$E_{\mathbb{Q}}$

$K = \mathbb{Q}(E[5])$

$\Delta = 5^3$

$K = \mathbb{Q}[x] / (x^4 - x^3 + x^2 - x + 1)$

$E_K(K)_{\text{tor}} \cong \mathbb{Z}/5 \oplus \mathbb{Z}/5$

$\Delta_K = 5^3$

$\mathbb{Q}(\zeta_5)$

\mathbb{Q}

C_4

4

solos

(14)

$p=2$

$$p \in \mathbb{Z} \text{ (Frob}_p)$$

$$R_p = \mathbb{Z} \text{ (other primes)}$$

$$P \in \mathbb{Z}$$

$$\text{Frob}_p \in \text{Gal}(K/\mathbb{Q})$$

$2, p \in \mathbb{Z}$ prime

unramified in K . (if $p \nmid l \cdot \Delta_E$ then $p \mid \Delta_K$)

$$\text{Frob}_p \leftrightarrow P \in R = \mathcal{O}_K$$

$$\mathbb{F}_p = R/p$$

$$1 \rightarrow I_p \rightarrow D_p \xrightarrow{\cong} \text{Gal}(\mathbb{F}_p/\mathbb{F}_p) \rightarrow 1$$

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

$$\{ \sigma \in \text{Gal}(K/\mathbb{Q}) : \sigma(P) = P \}$$

 $\langle \text{Frob}_p \rangle$

$$(x \mapsto x^p)$$