Stevenhagen

8-18-16

pg 1

Galois representations and adelic point groups.

E elliptic curve defined over a number field K.

$$\begin{array}{l} E(K) \longrightarrow E(K_{\mathfrak{p}}) \leftarrow \text{top. group} \\ \quad \searrow \\ \qquad \overline{E}(k_{\mathfrak{p}}) \end{array} \Bigg\} \text{ easier to study.}$$

$\nwarrow$ finite group $\mathfrak{p}$ good reduction.

Mordell-Weil: $E(K) \cong E(K)^{tor} \times \mathbb{Z}^r$.

$E(K)^{tor}$ finite

Today: adelic point group $E(\mathbb{A}_K)$

$$\mathbb{A}_K = \prod_{\mathfrak{p} \leq \infty}{}' K_{\mathfrak{p}}$$

$$E(\mathbb{A}_K) = \prod_{\mathfrak{p} \leq \infty} E(K_{\mathfrak{p}})$$

This is a topological group.

① What types of top. grps do we obtain?

② Is there a distribution, generic group?

Thm 1: Fix K of degree n. Then for "almost all" E/K we have

$$E(\mathbb{A}_K) \underset{\text{as top grps.}}{\cong} \mathcal{E}_n := (\mathbb{R}/\mathbb{Z})^n \times \hat{\mathbb{Z}}^n \times \prod_{k \geq 1} \mathbb{Z}/k\mathbb{Z}.$$

Steven hagen

8-18-16

pg 2

<u>$\mathcal{E}_n$:</u> ① $\mathcal{E}_n^{(0)}$ = connected component of $0 \in \mathcal{E}_n$.

$$\cong (\mathbb{R}/\mathbb{Z})^n$$

②

$$1 \longrightarrow \underset{\substack{\text{closure of} \\ \text{torsion}}}{T_E} \longrightarrow \mathcal{E}_n/\mathcal{E}_n^{(0)} \longrightarrow \hat{\mathbb{Z}}^n \longrightarrow 0$$

③ $T_E \cong \prod_{k \geq 1} \mathbb{Z}/k\mathbb{Z}$ almost always

<u>Exercise:</u> $\prod_{k \geq 1} \mathbb{Z}/k\mathbb{Z} \cong \prod_{k \geq 2016} \mathbb{Z}/k\mathbb{Z} \cong \prod_{p \text{ prime}} \mathbb{F}_p^\times$.

as topological groups.

<u>Thm 2:</u> Given K a number field of degree n, there exists a non-isotrivial family E_t/K s.t.

$$E_t(\mathbb{A}_K) \not\cong \mathcal{E}_n$$

$\forall\ t \in K \setminus \{\text{finite set}\}$.

$E_{A,B}: Y^2 = X^3 + AX + B \qquad (A,B) \in \mathcal{O}_K^2 \hookrightarrow (\mathcal{O}_K \otimes \mathbb{R})^2$

$$\cong \mathbb{R}^{2n}$$

Pick a $\|\cdot\|$ on $\mathbb{R}^{2n}$

Then by "almost all" E have a property P, ~~$E_{A,B}$ s.t. $\|(A,B)\| < X$ ... $E_{A,B}$ has property P~~

$$\lim_{X \to \infty} \frac{\#\{E_{A,B} : \|(A,B)\| < X \ \&\ E_{A,B} \text{ has property } P\}}{\#\{E_{A,B} : \|(A,B)\| < X\}} = 1.$$

$$\mathbb{A}_K = \mathbb{A}_K^{\infty} \times \mathbb{A}_K^{fin}$$

$$\prod_{p|\infty} K_p \qquad \prod_{p\nmid\infty}{}' K_p$$

<u>p infinite:</u>

$$E(K_p) = \begin{cases} (\mathbb{R}/\mathbb{Z})^2 & p \text{ complex} \\ (\mathbb{R}/\mathbb{Z}) \times \mathbb{Z}/2\mathbb{Z} & p \text{ real}, \ \Delta_{E_p} >_p 0 \\ \mathbb{R}/\mathbb{Z} & p \text{ real}, \ \Delta_E <_p 0. \end{cases}$$

$\therefore$

$$E(\mathbb{A}_K^{\infty}) = (\mathbb{R}/\mathbb{Z})^n \times (\mathbb{Z}/2\mathbb{Z})^r$$

$$r = \#\{p \text{ real}, \ \Delta_E >_p 0\}$$

<u>p finite:</u>

$$\begin{array}{ccccc} \left(\text{finite } p\text{-power}\right) & E(K_p) & \xrightarrow{\text{red}_p} & \overline{E}(k_p) & \text{finite set} \\ \downarrow & \cup\!\mid & & \cup\!\mid & \\ 1 \to E^1(K_p) & \to & E^0(K_p) & \longrightarrow & \overline{E}^{NS}(k_p) \quad \text{finite group.} \\ \downarrow \log_p & & & & \\ \mathcal{O}_p & \supseteq \mathbb{Z}_p^{[K_p:\mathbb{Q}_p]}. & & & \end{array}$$

$$\therefore \quad E(K_p) \cong \underset{\text{fin. tor-subgrp.}}{T_p} \times \mathbb{Z}_p^{[K_p:\mathbb{Q}_p]}$$

$$\therefore \quad E(\mathbb{A}_K^{fin}) \cong \hat{\mathbb{Z}}^n \times \prod_{p<\infty} T_p$$

$$E(\mathbb{A}_K) \cong (\mathbb{R}/\mathbb{Z})^n \times \hat{\mathbb{Z}}^n \times T_E$$

$$T = \prod_{p \le \infty} T_p$$

$$T_p = \begin{cases} E(K_p)^{tor} & \text{if } p < \infty \\ \mathbb{Z}/2\mathbb{Z} & \text{if } p \text{ real}, \ \Delta_E >_p 0 \\ 1 & \text{o/w} \end{cases}$$

T any countable product of ~~finite~~ cyclic abelian groups "standard rep."

$$\cong \prod_{\ell \text{ prime}} \prod_{m \ge 1} (\mathbb{Z}/\ell^m\mathbb{Z})^{e(\ell^m)} \qquad e(\ell^m) \in \mathbb{Z}_{\ge 0} \cup \{\infty\}$$

$$e(\ell^m) = \dim_{\mathbb{F}_\ell}\left(T[\ell^m] \big/ T[\ell^{m-1}] + \ell T[\ell^{m+1}] \right).$$

$T \cong \prod_{k \ge 1} \mathbb{Z}/k\mathbb{Z}$ iff $e(\ell^m) = \infty$ for all $\ell^m > 1$

$$E(K_p)[\ell^m] \cong (\mathbb{Z}/\ell^m\mathbb{Z})^2 \iff p \text{ splits completely in } K(E[\ell^m](\bar{K})) = Z_E(\ell^m)$$

<u>Lemma:</u> For $\ell^m > 1$

If $Z_E(\ell^m) \subsetneq Z_E(\ell^{m+1})$,

then T_E has $e(\ell^m) = \infty$

<u>Pf:</u> pick p that splits completely in $Z_E(\ell^m)$, but not in $Z_E(\ell^{m+1})$.

$$\rho_E : G_K \longrightarrow \mathrm{Aut}(E(\bar{K})^{tors}) \cong GL_2(\hat{\mathbb{Z}})$$

<u>Serre:</u>
- If E is without CM, then $\mathrm{Im}\,\rho_E \overset{<\infty}{\subset} GL_2(\hat{\mathbb{Z}})$
- $K = \mathbb{Q}$, then $\mathrm{im}\,\rho_E$ has even index in $GL_2(\hat{\mathbb{Z}})$.

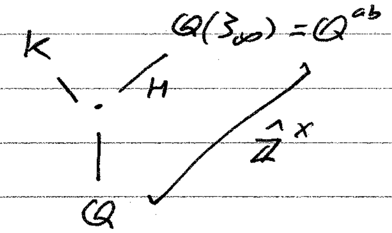
$$\begin{tikzcd}
GL_2(\hat{\mathbb{Z}}) \arrow[r] \arrow[d, "\det"'] \arrow[rr, bend left, "\varepsilon"] \arrow[drr, bend right, "\chi"'] & GL_2(\mathbb{Z}/2\mathbb{Z}) \arrow[r] & \{\pm 1\} \\
& \hat{\mathbb{Z}}^\times \arrow[r, "\chi_{\Delta_E}", "\mathrm{Dir.}"'] & \{\pm 1\}
\end{tikzcd}$$

$\mathrm{im}(\rho_E) \subseteq \ker(\varepsilon\chi)$. ← equality is called Serre curve.

<u>Thm (Jones '10):</u> Almost all $E/\mathbb{Q}$ are Serre curves.

<u>Cor:</u> Thm 1 for $K = \mathbb{Q}$.

<u>Thm: (Zywina '10):</u> If $K \neq \mathbb{Q}$, then almost all E/K have "maximal" Galois image



$$\begin{array}{ccc}
GL_2(\hat{\mathbb{Z}}) & \xrightarrow{\det} & \hat{\mathbb{Z}}^* \\
\cup_{<\infty} & & \cup| \\
\det^{-1}[H] & \subset & H
\end{array}$$

$\mathrm{im}\,\rho_{E,K} \subset \det^{-1}[H]$

= means maximal

Stevenhagen
8-18-16
pg 6

This gives the rest of Thm 2.

<u>Easy:</u> $E/\mathbb{Q}$ $\quad K = \mathbb{Z}_{E,\mathbb{Q}}(\ell^{k+1})$

$\rightsquigarrow$

$E/A_k)$ has $e(\ell^k) = 0$ for $m < k+1$.

$K = \mathbb{Q}$ $\quad E/\mathbb{Q}$ has $e(\ell^k) = \infty$ for ℓ odd, $k \in \mathbb{Z}_{\geq 1}$.

Can find $E/\mathbb{Q}$ w/ $\mathbb{Z}_E(2) = \mathbb{Z}_E(4)$

$\Rightarrow e(2) = 0$.

Pick E s.t.

$\mathbb{Z}_E(4) = \mathbb{Q}(i)$: $\quad y^2 = x(x-\alpha)(x-\bar{\alpha})$

$\alpha \in \mathbb{Q}(i) \setminus \mathbb{Q}$.

$$\text{if } \begin{cases} \alpha = \square & \text{in } \mathbb{Q}(i) \\ \alpha - \bar{\alpha} = \square & \text{in } \mathbb{Q}(i) \end{cases} \quad \text{then } \mathbb{Z}_E(2) = \mathbb{Z}_E(4) = \mathbb{Q}(i)$$

$$\alpha = (1+qi)^2$$

$$\alpha - \bar{\alpha} = 4qi = (2+2i)^2 \cdot \frac{q}{2}.$$

Take $q = 2r^2$