opics in Arithmetic Geometry: 30/11/09

Some basics of Galois representations

Reference: Arno Kret's master thesis ← on homepage

or go directly to the long version of R. Taylor's Beijing ICM notes

(Linear) representations of a group G: $G \curvearrowright V$, ← k vector space, mostly fin. dim'l (a field)

Infinite Galois groups are topological groups, compact & totally disconnected

We will mostly be concerned w/ $Gal(\overline{\mathbb{Q}}/\mathbb{Q}) = \varprojlim_K Gal(K/\mathbb{Q})$

Consider an algebraic closure $\mathbb{Q} \longrightarrow \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$

$\overline{\mathbb{Q}} = \bigcup K$ where K finite (Galois) over $\mathbb{Q}$

$$Gal(\overline{\mathbb{Q}}/\mathbb{Q}) = \varprojlim_K Gal(K/\mathbb{Q}) \twoheadrightarrow \underset{\text{(discrete)}}{Gal(K/\mathbb{Q})}$$

$\exists$ basis of the topology consisting of open subgroups $Gal(\overline{\mathbb{Q}}/K)$

Because of this structure of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ or in general, infinite Galois groups, we should consider continuous representations

Now: give k some topology

Examples: $k = \mathbb{C}$.

$\rho: Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL_n(\mathbb{C}) \subset \mathbb{C}^{n^2}$

is continuous for the discrete topology on $\mathbb{C} \Leftrightarrow \rho$ is continuous for (usual) archimedean topology on $\mathbb{C}$.

Pf: $(\Rightarrow)$ is obvious; For $(\Leftarrow)$, consider small neighborhoods of the identity in $GL_n(\mathbb{C})$, and the map $M_n(\mathbb{C}) \xrightarrow{\exp} GL_n(\mathbb{C})$ $x \longmapsto 1 + x + \frac{1}{2}x^2 + \dots + \frac{x^n}{n!} + \dots$

$0 \longmapsto 1$

bounded $\longrightarrow U \underset{\log}{\overset{\sim}{\rightleftarrows}} V$ diffeomorphism

$$-\sum_{m \geq 1} \frac{x^m}{m} \longleftarrow 1 - x$$

~~Gal(Q/Q)~~. Note that $1 \in \rho^{-1}V \supset$ open subgroup of $Gal(\overline{\mathbb{Q}}/K)$. Let $\sigma \in Gal(\overline{\mathbb{Q}}/K)$.

Then $\forall m \in \mathbb{Z}$: $\underset{\rho(\sigma)^m}{\rho(\sigma^m)} \in V$. However, this implies $\forall m \in \mathbb{Z}$, $U \ni m \cdot \log(\rho(\sigma))$

Thus, $\log(\rho(\sigma)) = 0 \Rightarrow \rho(\sigma) = 1$.

We can write the representation as factoring through some K:

$$\begin{tikzcd} \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \arrow[rr, "\rho"] \arrow[dr, two heads] & & GL_n(\mathbb{C}) \\ & \mathrm{Gal}(K/\mathbb{Q}) \arrow[ur] & \end{tikzcd}$$

We can ask about faithful representations, and consider what ~~...~~ possible finite images are there in $GL_n(\mathbb{C})$.

or $n=1$, cyclic groups.

or $n=2$, consider instead $PGL_2(\mathbb{C})$:

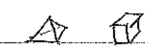
$$\begin{tikzcd} \mathbb{C}^\times \arrow[r, hook] & GL_2(\mathbb{C}) \arrow[r, two heads] & PGL_2(\mathbb{C}) = \mathrm{Aut}(\mathbb{P}^1(\mathbb{C})) \\ & \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \arrow[u, "\rho"] \arrow[ur, "\bar{\rho}"'] & \end{tikzcd}$$

$\bar{\rho}$ ← possible images:

D_n (dihedral)

A_4, A_5,

others related to symmetric bodies



xamples: $k = \mathbb{F}_q$, $GL_n(\mathbb{F}_q)$: discrete topology

$= \mathbb{Q}_\ell$ with ℓ-adic topology, or finite extension of $\mathbb{Q}_\ell$.

Ex1: $\chi_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}(\overline{\mathbb{Q}}^\times[\ell^\infty]) = \mathbb{Z}_\ell^\times \hookrightarrow \mathbb{Q}_\ell^\times$

"ℓ-adic cyclotomic character"

$\cong$ non-canonically

$\mathbb{Q}_\ell/\mathbb{Z}_\ell \cong \bigcup_{n\geq 1} (\ell^{-n}\mathbb{Z})/\mathbb{Z}$

$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \underset{\text{cont.}}{\curvearrowright} \overline{\mathbb{Q}}$ ← (discrete topology)

Ex2: $E/\mathbb{Q}$ elliptic curve. $E(\overline{\mathbb{Q}}) \subset E(\mathbb{C}) = \mathbb{C}/\Lambda \cong S^1 \times S^1$

$y^2 = x^3 + ax + b$, $a, b \in \mathbb{Q}$ where $\mathrm{disc}(E) = 4a^3 + 27b^2 \neq 0$

or $n \in \mathbb{Z}_{\geq 1}$: $E(\overline{\mathbb{Q}})[n] = E(\mathbb{C})[n] = \frac{1}{n}\Lambda/\Lambda$ ← free $(\mathbb{Z}/n\mathbb{Z})$-module of rank 2

o get to $\mathbb{Q}_\ell$, consider

$\rho_{E,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}(\underbrace{E(\overline{\mathbb{Q}})[\ell^\infty]}_{= \bigcup_{n\geq 1} E(\overline{\mathbb{Q}})[\ell^n]})$ ← free $(\mathbb{Z}/\ell^n\mathbb{Z})$-module of rank 2

$E(\overline{\mathbb{Q}})[\ell^n] = \frac{1}{\ell^n}\Lambda/\Lambda$ ← take a $\mathbb{Z}$-basis

Thus, we have $\mathrm{Aut}(E(\overline{\mathbb{Q}})[\ell^n]) \xrightarrow{\sim} GL_2(\mathbb{Z}/\ell^n\mathbb{Z})$, hence

$$\mathrm{Aut}(E(\overline{\mathbb{Q}})[\ell^\infty]) = \varprojlim_n GL_2(\mathbb{Z}/\ell^n\mathbb{Z}) = GL_2(\mathbb{Z}_\ell) \subset GL_2(\mathbb{Q}_\ell)$$

(:)

nother construction (Tate module): $T_\ell(E) :\overset{\text{def}}{=} \left(\varprojlim_n E(\overline{\mathbb{Q}})[\ell^n]\right)$ — ~~...~~, a free $\mathbb{Z}_\ell$-module of rank 2

ℓ-adic Tate module

↑ have transition maps: ℓ^{m-n}, $m \geq n$

(also gives continuous rep'n)

We get (from either construction): $\rho_{E,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL_2(\mathbb{Q}_\ell)$ cont.

$\rightsquigarrow$ L-functions (how to attach to Galois representations), maybe later.
(in relation to BSD-conjecture)

Prop: Let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL_n(\mathbb{Q}_\ell)$ be a continuous representation. Then after suitable conjugation, ρ has image in $GL_n(\mathbb{Z}_\ell)$

Pf: Up to conjugacy, $GL_n(\mathbb{Q}_\ell)$ has exactly 1 maximal compact subgroup, and it is $GL_n(\mathbb{Z}_\ell)$. [stronger statement], prove this instead.

Pf: Let K be a compact subgroup. Then $K' := K \cap GL_n(\mathbb{Z}_\ell)$ is open in K.
(recall $GL_n(\mathbb{Z}_\ell)$ is open in $GL_n(\mathbb{Q}_\ell)$)
So K/K' is finite because K = disjoint union of K' cosets, that are open.
K' stabilizes $\mathbb{Z}_\ell^n$. So: $\{k \cdot \mathbb{Z}_\ell^n : k \in K\}$ is finite. Take $M := \sum_{k \in K} k \cdot \mathbb{Z}_\ell^n$
M is a f.g. $\mathbb{Z}_\ell$-(sub)module of $\mathbb{Q}_\ell^n$; therefore, M is free as a $\mathbb{Z}_\ell$-module of rank n. Take a $\mathbb{Z}_\ell$-basis.
$M \supseteq \mathbb{Z}_\ell^n$
$K \hookrightarrow \mathrm{Aut}_{\mathbb{Z}_\ell}(M)$ $\leftarrow$ is a conj of $GL_n(\mathbb{Z}_\ell)$. $\square$

Exercise: Consider $PGL_2(\mathbb{Q}_\ell)$. How many max. compact subgroups up to conjugation?