GALOIS REPRESENTATIONS

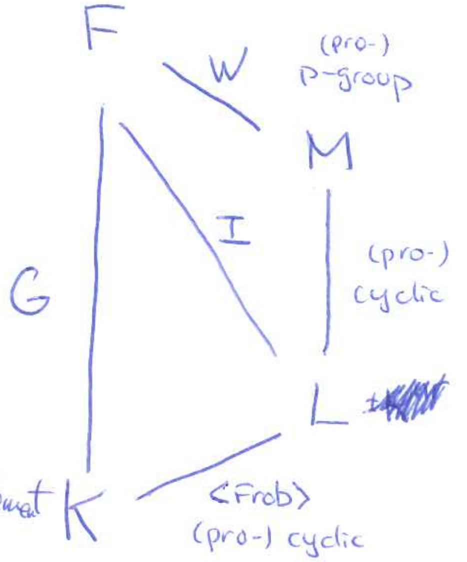
§1 ℓ-adic representations

K = non-archimedean local field, res. char. p (e.g. $\mathbb{Q}_p$)

$\mathbb{F}_K = \mathbb{F}_q$ ($= k_K$) = residue field

Recall: if F/K Galois then

- $I = I_{F/K}$ = inertia subgroup of $G = \mathrm{Gal}(F/K)$; acts trivially on $\mathbb{F}_F$
- $W = \mathrm{Syl}_p I$ = wild inertia (a p-group)
- I/W = tame inertia (cyclic)
- $\mathrm{Gal}(L/K)$ generated by Frob_K = frobenius element; Frob_K acts as $x \mapsto x^q$ on $\mathbb{F}_K$.



- L/K unramified, F/L totally ramified.
- We allow infinite algebraic extensions, e.g. $K = \mathbb{Q}_p$, $F = \bar{\mathbb{Q}}_p$.

Definition

A <u>continuous l-adic representation</u> over K is a continuous homomorphism
$$\rho : \mathrm{Gal}(\bar{K}/K) \to GL_d(\bar{\mathbb{Q}})$$
for some d.

Remark

An l-adic representation $\rho : \mathrm{Gal}(\bar{K}/K) \to GL_d(\bar{\mathbb{Q}})$ is continuous if and only if $\forall n \geq 1$ $\exists F_n/K$ finite Galois s.t.
$$\mathrm{Gal}(\bar{K}/F_n) \xrightarrow{\rho} Id \bmod l^n$$

$$\begin{array}{c} \bar{K} \\ | \\ F_n \\ | \\ K \end{array}$$

Example

Take $F = \mathbb{Q}_5(\sqrt[3]{5}, \zeta_3)$ $K = \mathbb{Q}_5$

$$\langle s,t \mid t^2 = s^3 = 1,\ tst = s^{-1} \rangle = S_3$$

$$\begin{array}{ccc} F & & \\ | & \diagdown & \\ \mathbb{Q}_5 & - & \mathbb{Q}_5(\zeta_3) \end{array}$$

Take $\rho_0 : S_3 \to GL_2(\bar{\mathbb{Q}})$

$$\rho_0(t) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \rho_0(s) = \begin{pmatrix} \zeta_3 & 0 \\ 0 & \zeta_3^{-1} \end{pmatrix}$$

usual 2-dimensional representation (symmetries of a triangle)

Take
$$\rho : \mathrm{Gal}(\bar{\mathbb{Q}}_5/\mathbb{Q}_5) \to \mathrm{Gal}(F/\mathbb{Q}_5) = S_3 \xrightarrow{\rho_0} GL_2(\bar{\mathbb{Q}}) \subseteq GL_2(\bar{\mathbb{Q}}_l)$$

Then ρ is continuous : take $F_n = F$, so
$$\mathrm{Gal}(\bar{\mathbb{Q}}_5/F) \xrightarrow{\rho} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod l^n \ \forall n.$$

Generally, all representations of finite Galois groups are continuous l-adic representations.

Example:

Let ζ_{ℓ^n} be a primitive ℓ^n-th roots of unity in $\bar{k}$ with $\zeta_{\ell^{n+1}}^{\ell} = \zeta_{\ell^n}$. For $g \in Gal(\bar{k}/k)$ define $0 \le a_i < \ell$ by

$$g(\zeta_\ell) = \zeta_\ell^{a_1}$$
$$g(\zeta_{\ell^2}) = \zeta_{\ell^2}^{a_1 + \ell a_2}$$
$$\vdots$$
$$g(\zeta_{\ell^n}) = \zeta_{\ell^n}^{a_1 + \ell a_2 + \dots + \ell^{n-1} a_n}$$

Define the <u>ℓ-adic cyclotomic character</u> χ_{cyc} by

$$\chi_{cyc}(g) = a_1 + \ell a_2 + \dots + \ell^{n-1} a_n + \dots \in \mathbb{Z}_\ell$$

Note that $\chi_{cyc}(g) \bmod \ell^n$ says what g does to ζ_{ℓ^n}.

- $\chi_{cyc}(gh) = \chi_{cyc}(g)\,\chi_{cyc}(h)$
- $\chi_{cyc}(g) \equiv 1 \bmod \ell^n \quad \forall g \in Gal(\bar{k}/k(\zeta_{\ell^n}))$

$\Rightarrow$ $\chi_{cyc}: Gal(\bar{k}/k) \to GL_1(\bar{\mathbb{Q}}_\ell)$ is a continuous ℓ-adic representation.

Example ~~...~~)

E/K elliptic curve

Let P_n, Q_n be a basis for $E[\ell^n]$

with $\ell P_n = P_{n-1}$ $\ell Q_n = Q_{n-1}$

For $g \in Gal(\bar{K}/K)$ define $0 \le a_i, b_i, c_i, d_i < \ell$

by $g(P_1) = a_1 P_1 + b_1 Q_1$ $g(Q_1) = c_1 P_1 + d_1 Q_1$

and

$$g P_n = (a_1 + a_2 \ell + \ldots + a_n \ell^{n-1}) P_n + (b_1 + b_2 \ell + \ldots + b_n \ell^{n-1}) Q_n$$

$$g Q_n = (c_1 + c_2 \ell + \ldots + c_n \ell^{n-1}) P_n + (d_1 + d_2 \ell + \ldots + d_n \ell^{n-1}) Q_n.$$

Then

$$\rho(g) = \begin{pmatrix} a_1 + \ldots + \ell^{n-1} a_n + \ldots & c_1 + \ldots \\ b_1 + \ldots + \ell^{n-1} b_n + \ldots & d_1 + \ldots \end{pmatrix} \in GL_2(\mathbb{Z}_\ell) \subseteq GL_2(\mathbb{Q}_\ell)$$

is the representation on the <u>ℓ-adic Tate module of E</u>.

Here take $F_n = K(E[\ell^n])$ to see ρ is continuous;

$\rho(g) \bmod \ell^n$ says what ρ does to $E[\ell^n]$.

Definition:

ρ is <u>unramified</u> $\Leftrightarrow$ $\rho(I_{\bar{K}/K}) = Id$

(These are determined by $\rho(Frob_K)$.)

Example: $K = \mathbb{Q}_p$, $p \neq \ell$

Then $\mathbb{Q}_p(\zeta_{\ell^n})/\mathbb{Q}_p$ is unramified $\forall n$,

so $I_{\bar{K}/K}$ acts trivially on ζ_{ℓ^n} $\forall n$ and

$Frob_{\mathbb{Q}_p}(\zeta_{\ell^n}) = \zeta_{\ell^n}^p$.

Hence $\chi_{cyc}(I_K) = 1$ $\quad \chi_{cyc}(Frob_{\mathbb{Q}_p}) = p$

χ_{cyc} is unramified.

Definition (for $\ell \neq p$).

The <u>local polynomial</u> of ρ is

$$P(\rho, T) = \det(1 - T\, Frob_K^{-1} \mid \rho^{I}).$$

($\approx$ char. poly. of $Frob_K$ on unramified subrep^n of ρ)

e.g. $P(\chi_{cyc}, T) = 1 - \frac{1}{q} T$.

DEFINITION:

E/K elliptic curve, ρ = representation on ℓ-adic Tate module.
Write
$$\rho_E = \rho^* \qquad (\text{i.e. } \rho_E(g) = (\rho(g)^{-1})^T)$$
(This is in fact the representation of $H^1_{et}(E/\bar{K}, \mathbb{Q}_\ell)$).

THEOREM

E/K an elliptic curve, $\ell \neq p$. Then

(1) E has good reduction $\Leftrightarrow$ ρ_E is unramified (Néron-Ogg-Shafarevich)

(2) $\det \rho_E = \chi_{cyc}^{-1}$ (Weil pairing)

(3) $P(\rho_E, \frac{1}{q}) = \frac{\#\tilde{E}_{ns}(\mathbb{F}_K)}{q}$ $\qquad q = \#\mathbb{F}_K$.

($\tilde{E}$ = reduction of the min. Weierstrass model).

REMARK:

(i) By (1), E has pot. good reduction $\Leftrightarrow$ I_K acts through a finite quotient.

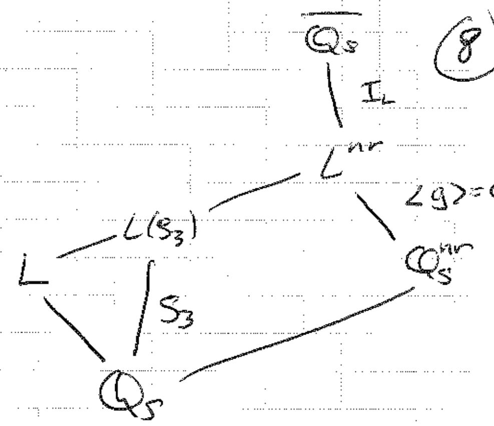
(ii) By (1), (2), (3) if E has good reduction then
$$P(\rho_E, T) = 1 - aT + qT^2 \qquad a = 1 + q - \#\tilde{E}(\mathbb{F}_K)$$

(iii) By (1) & (3)

E has additive red^n $\Rightarrow$ $P(\rho_E, 1) = 1$

E has split mult red^n $\Rightarrow$ $P(\rho_E, 1) = 1 - T$

E has non-split — " — $\Rightarrow$ $P(\rho_E, 1) = 1 + T$



Example

$E/\mathbb{Q}_5 : \; y^2 = x^3 + 5^2$

$L = \mathbb{Q}_5(\sqrt[3]{5})$

$E/\mathbb{Q}_5$ additive red^n $\Rightarrow \rho_E(I_{\mathbb{Q}_5}) \neq Id$

E/L good red^n, has model $E' : y^2 = x^3 + 1$

$\Rightarrow \rho_E(I_L) = Id \quad , \quad \rho_E(g)$ order 3

Weil pairing $\Rightarrow$ WLOG $\quad \rho_E(g) = \begin{pmatrix} \zeta_3 & 0 \\ 0 & \zeta_3^{-1} \end{pmatrix}$ as $\det \rho_E(g) = 1$.

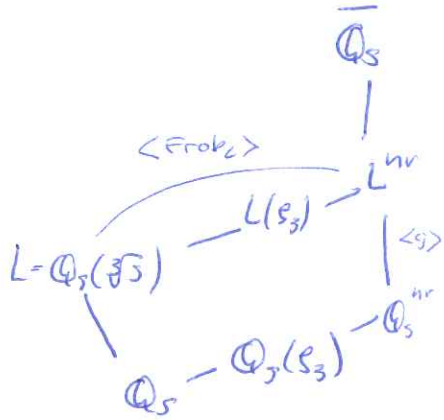
$\tilde{E}'(\mathbb{F}_5) = \{ \mathcal{O}, (-1,0), (0,\pm 1), (2,\pm 2) \} \Rightarrow P(\rho_E, T) = 1 + 5T^2$

$\Rightarrow$ Frob_L has eigenvalues $\pm 1/\sqrt{-5}$

$\mathrm{Frob}_L \, g \, \mathrm{Frob}_L^{-1} = g^{-1}$ (using $\mathrm{Gal}(L(\zeta_3)/\mathbb{Q}_5) = S_3$)

$$\Rightarrow \rho_E(\mathrm{Frob}_L) = \begin{pmatrix} 0 & 1/\sqrt{-5} \\ 1/\sqrt{-5} & 0 \end{pmatrix}.$$

§2 Classification of ℓ-adic representations



Example: In last lecture we had

$\rho_0 : S_3 \to GL_2(\bar{\mathbb{Q}}_\ell)$ $\quad \rho_0(t) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ $\quad \rho_0(s) = \begin{pmatrix} \varsigma_3 & 0 \\ 0 & \varsigma_3^{-1} \end{pmatrix}$

$\rho : \mathrm{Gal}(\bar{\mathbb{Q}}_5/\mathbb{Q}_5) \to GL_2(\bar{\mathbb{Q}}_\ell)$ $\quad \rho(\mathrm{Frob}_L) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ $\quad \rho(g) = \begin{pmatrix} \varsigma_3 & 0 \\ 0 & \varsigma_3^{-1} \end{pmatrix}$

and $E/\mathbb{Q}_5$ with

$$\rho_E(\mathrm{Frob}_L) = \begin{pmatrix} 0 & 1/\sqrt{-5} \\ 1/\sqrt{-5} & 0 \end{pmatrix} \qquad \rho_E(g) = \begin{pmatrix} \varsigma_3 & 0 \\ 0 & \varsigma_3^{-1} \end{pmatrix}.$$

We clearly have
$$\rho_E = \rho \otimes \psi$$
where ψ is 1-dimensional with $\psi(I_{K/K}) = 1$, $\psi(\mathrm{Frob}_K) = 1/\sqrt{-5}$.

THEOREM: Every continuous ℓ-adic representation τ for which

(i) $\tau(I_{\bar{K}/K})$ is finite,

(ii) $\tau(\mathrm{Frob}_K)$ is diagonalisable for some ($\Leftrightarrow$ every) choice of Frob_K,

is of the form
$$\tau = \bigoplus_i \rho_i \otimes \psi_i$$
for ρ_i factoring through finite extensions of K and ψ_i 1-dimensional unramified.

REMARK: This applies to elliptic curves and abelian varieties with potentially good reduction.

EXAMPLE:

E/K with split multiplicative reduction.

Recall $\det(1 - T\,\mathrm{Frob}_K^{-1} \mid \rho_E^{I}) = P(\rho_E, T) = 1 - T$.

$\Rightarrow \quad \rho_E(h) = \begin{pmatrix} 1 & ? \\ 0 & ? \end{pmatrix}$ for $h \in \mathrm{Gal}(\bar{K}/K)$.

Since $\det \rho_E = \chi_{cyc}^{-1}$ and $\chi_{cyc}(h) = 1 \quad \forall h \in I_{\bar{K}/K}$,

$\Rightarrow \quad \rho_E(h) = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \quad \forall h \in I_{\bar{K}/K}$, $*$ not always 0

$$\begin{tikzcd}
\bar{K} \arrow[d, dash, "p\text{-gp}"'] \\
M \arrow[d, dash, "\prod_{t \neq \ell} \mathbb{Z}_t"'] \\
L = \bigcup_{n=1}^{\infty} K^{nr}\left(\sqrt[\ell^n]{\pi_K}\right) \arrow[d, dash, "\langle g \rangle = \mathbb{Z}_\ell"'] \\
K^{nr} \arrow[d, dash] \\
K
\end{tikzcd}$$

Continuity $\Rightarrow \quad \rho_E(h) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ for $h \in \mathrm{Gal}(\bar{K}/L)$

and WLOG

$$\rho_E(g) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

As $\det \rho_E = \chi_{cyc}^{-1}$ and $\chi_{cyc}(\mathrm{Frob}_K) = q$,

$$\rho_E(\mathrm{Frob}_K) = \begin{pmatrix} 1 & * \\ 0 & q \end{pmatrix}$$

($*$ depends on choice of Frob_K and can be made 0)

DEFINITION:

The <u>special representation</u> $sp(n)$ over K is

$$sp(n)(h) = \begin{pmatrix} 1 & t & t^2/2 & \cdots & t^{n-1}/(n-1)! \\ & 1 & t & t^2/2 & \\ & & \ddots & & \\ & 0 & & & t \\ & & & & 1 \end{pmatrix} \quad \text{for } h \in I_{\bar{K}|K}$$

$$sp(n)(\mathrm{Frob}_K) = \begin{pmatrix} 1 & & & 0 \\ & q & & \\ & & \ddots & \\ 0 & & & q^{n-1} \end{pmatrix}, \quad q = \# \mathbb{F}_K .$$

Here $t = t(h)$ is the <u>ℓ-adic tame character</u> given by $h(\sqrt[\ell^n]{\pi_K}) = \zeta_{\ell^n}^{t(h)} \sqrt[\ell^n]{\pi_K}$, $\forall n$.

($sp(1) = \mathbb{1}$, $sp(2) = \rho_E$ from last example)

THEOREM: Every continuous ℓ-adic representation τ such that $\tau(\mathrm{Frob}_k)$ acts diagonalizably on τ^I for every $I \le I_{E/K}$ of finite index, is of the form

$$\tau = \bigoplus_i \rho_i \otimes sp(n_i)$$

for some $n_i \in \mathbb{N}$ and ρ_i continuous ℓ-adic representations with $\rho_i(I_{E/K})$ finite and $\rho_i(\mathrm{Frob}_k)$ diagonalisable.

EXAMPLE: E/K split multiplicative red^n

$\Rightarrow$ $\rho_E(I_{E/K})$ infinite, τ^I 0 or 1-dimensional $\forall I \le I_{E/K}$ of finite index.

$\Rightarrow$ $\rho_E \cong \rho \otimes sp(2)$ $\quad \rho$ 1-dimensional

$P(\rho_E, T) = 1 - T$ $\Rightarrow$ $\rho = \mathbb{1}$ $\Rightarrow$ $\rho_E \cong sp(2)$.

REMARK:

Theorem applies to all elliptic curves and abelian varieties (and all $n_i = 1$ or 2).

REMARK: We always have $\ell \neq p$ but otherwise ℓ is arbitrary. Eg.

- $\chi_{cyc}(I) = 1$ $\quad \chi_{cyc}(\mathrm{Frob}_K) = q$ morally does not depend on ℓ.
  It actually does due to topology: χ_{cyc} factors through $\bigcup_{n=1}^{\infty} K(\zeta_{\ell^n})$ which depends on ℓ.

- We had $\rho_E(g) = \begin{pmatrix} \zeta_3 & 0 \\ 0 & \zeta_3^{-1} \end{pmatrix}$ $\quad \rho_E(\mathrm{Frob}_L) = \begin{pmatrix} 0 & 1/\sqrt{-5} \\ 1/\sqrt{-5} & 0 \end{pmatrix}$.
  Again, this is independent of ℓ provided we only look at $\rho_E(I_{\bar{K}/K})$ and $\rho_E(\mathrm{Frob}_K^n)$ for $n \in \mathbb{Z}$.

- E/K split mult. red^n $\Rightarrow$ $\rho_E \simeq sp(2)$ again, morally, does not depend on ℓ.

<u>DEFINITION</u>: The <u>Weil group</u> $W_{\bar{K}/K}$ is the subgroup of $G_{\bar{K}/K}$ consisting of elements whose image modulo $I_{\bar{K}/K}$ is an <u>integer</u> power of Frob_K.
(Topology: profinite on $I_{\bar{K}/K}$, discrete on $W_{\bar{K}/K}/I_{\bar{K}/K}$).

<u>THEOREM</u>: Let E/K be an elliptic curve (or an abelian variety). Then the decomposion of ρ_E as $\bigoplus_i \rho_i \otimes sp(n_i)$ is "independent of ℓ" as a $W_{\bar{K}/K}$-rep, i.e. $\rho_i \otimes_{\mathbb{Q}_\ell} \mathbb{C}$ and n_i do not depend on ℓ.

<u>COROLLARY</u>: E/K elliptic curve (or AV) with potentially good reduction. Then $\rho_E \otimes_{\mathbb{Q}_\ell} \mathbb{C}$ is independent of ℓ as a representation of $W_{E/K}$.
("Weil representation")

(Pf: By Néron-Ogg-Shafarevich $n_i = 1$ $\forall i$.)

<u>COROLLARY</u>: E/K elliptic curve (or AV).
Then $P(\rho_E, T) \in \mathbb{Q}[T]$. The char. poly. of $\rho_E(h)$ for $h \in I_{\bar{K}/K}$ also lie in $\mathbb{Q}[X]$

(Pf: $P(\rho_E, T) \in \mathbb{Q}_\ell(T) \cap \bar{\mathbb{Q}}[T] \; \forall \ell \neq p$ and is independent of ℓ
$\Rightarrow \; \in \mathbb{Q}[T]$
and similarly for the other case).

<u>Example</u>:
Let $p \geq 5$, E/K elliptic curve with pot. good red^n.
If $h \in I_{\bar{K}/K} \Rightarrow \rho_E(h)$ has finite order and rational char. poly. of degree 2

$\Rightarrow \rho_E(h)$ has order 1, 2, 3, 4 or 6.

In particular wild inertia acts trivially
$\Rightarrow$ image of inertia is cyclic, (tame inertia)
ie. C_1, C_2, C_3, C_4 or C_6
$\Rightarrow$ E/K acquires good reduction over a ramified extension of degree 1,2,3,4 or 6.