

Ramification

$$\rho: G_{\mathbb{Q}} \longrightarrow GL_n(K)$$

$$\tau_p = (x \mapsto x^p) \in G_{\mathbb{F}_p}$$

$\rho(\tau_p) \in GL_n(K)$ well-defined up to conjugation.

Want decomposition group $D_p \leq G_{\mathbb{Q}}$ s.t. $D_p \twoheadrightarrow G_{\mathbb{F}_p}$.

$$1 \longrightarrow I_p \longrightarrow D_p \longrightarrow G_{\mathbb{F}_p} \longrightarrow 1$$

\uparrow
 inertia group

\downarrow
 τ_p

If $I_p \subseteq \ker \rho$, then $\rho(\tau_p)$ makes sense.
 If so we say that ρ is unramified at p .

Some choices are made in defining D_p
 Different choice lead to conjugate D_p 's.

Two ways of defining D_p :

Way 1 (w/o details)

$$\begin{array}{c} \overline{\mathbb{Q}} \\ | \\ \mathbb{Q} \end{array} \quad \left. \begin{array}{c} p \\ \\ p \end{array} \right\}$$

$$D_p = \{ \tau \in G_{\mathbb{Q}} : \tau(\wp) = \wp \}$$

$$\overline{\mathbb{Z}} \xrightarrow{\tau} \overline{\mathbb{Z}}$$

$$\downarrow \quad \downarrow$$

$$\mathbb{F}_p \xrightarrow{\tau} \mathbb{F}_p = \overline{\mathbb{Z}}/\wp$$

This gives a map $D_p \rightarrow G_{\mathbb{F}_p}$

Let I_p be the kernel.

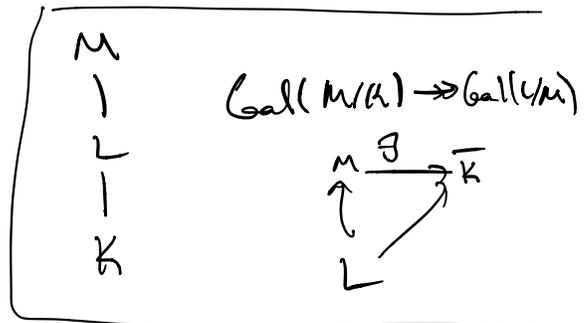
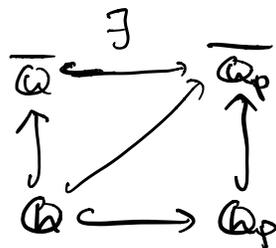
Gives

$$1 \rightarrow I_p \rightarrow D_p \rightarrow G_{\mathbb{F}_p} \rightarrow 1.$$

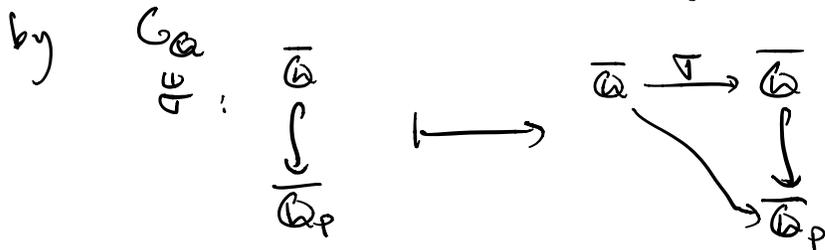
Different choices of $\varphi|_p$ gives conjugate D_p 's, therefore conjugate I_p 's

Since $\ker \rho$ is normal, $I_p \subseteq \ker \rho$ for one choice of $\varphi|_p$ iff $I_p \subseteq \ker \rho$ for all choices.

Way 2 (with some details)



This gives (non-uniquely) an embedding $\bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_p$
The set of such embeddings is acted on



This action is transitive.

(Picture: an embedding $\bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_p$ "is" a prime φ of $\bar{\mathbb{Q}}$ over p).

Fix an embedding $\bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_p$.

$$\text{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) \hookrightarrow \text{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}) \xrightarrow{\quad} \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$$

\uparrow
 injective!

Let $D_p \leq G_{\mathbb{Q}}$ be the image of this injection.

We have a map $G_{\mathbb{Q}_p} \rightarrow G_{\mathbb{F}_p}$

$$\parallel \qquad \parallel$$

$$\text{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) \rightarrow \text{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$$

Gives a map $D_p \rightarrow G_{\mathbb{F}_p}$, giving

$$1 \rightarrow I_p \rightarrow D_p \rightarrow G_{\mathbb{F}_p} \rightarrow 1.$$

The embeddings $\bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_p$ are conjugate (acted on transitively by $G_{\mathbb{Q}}$), and conjugate embeddings give conjugate D_p 's.

Remark

K \mathfrak{o} (choice of p is like a choice of
 fr. | | $K \hookrightarrow \bar{\mathbb{Q}}_p$)
 \mathbb{Q} \mathfrak{p} $\searrow_{K_{\mathfrak{p}}} \nearrow$

$$\begin{array}{ccc} \text{Gal}(K_{\wp}/\mathbb{Q}_p) & \longrightarrow & \text{Gal}(K/\mathbb{Q}) \\ \wr & & \wr \\ \tau & \longrightarrow & \tau|_K \end{array}$$

τ, τ^{-1} are continuous on K_{\wp}

$$\implies \tau(\wp) = \wp$$

so

$$\begin{array}{ccc} \text{Gal}(K_{\wp}/\mathbb{Q}_p) & \xrightarrow{\sim} & D_{\wp} = \{\tau \in \text{Gal}(K/\mathbb{Q}) : \tau(\wp) = \wp\} \\ \wr & & \wr \\ \uparrow & \xleftarrow{\text{extend continuity}} & \uparrow \end{array}$$

Rank

$$\begin{array}{c} K \\ \text{fn} | \\ \mathbb{Q} \end{array}$$

Ostrowski's Theorem

$$\begin{array}{ccc} \{\text{primes } \wp | p\} & \longleftrightarrow & \{\text{absolute values on } K \\ & & \text{extending } |\cdot|_p \text{ on } \mathbb{Q}\} \\ & & \longleftrightarrow \{\text{embeddings } K \hookrightarrow \overline{\mathbb{Q}_p}\} \end{array}$$

Ostrowski's Thm: nonarchimedean absolute values on K are $|\cdot|_{\wp}$ for primes \wp of K .

$$\begin{array}{ccc} \{\text{absolute values on } K \\ \text{extending } |\cdot|_p\} & \longleftrightarrow & \{\text{embeddings } K \hookrightarrow \overline{\mathbb{Q}_p}\} \\ |\cdot|_{\wp} & \longleftrightarrow & (K \hookrightarrow K_{\wp} \hookrightarrow \overline{\mathbb{Q}_p}) \\ |\cdot|_{\mathbb{Q}_p} & \longleftrightarrow & (K \hookrightarrow \overline{\mathbb{Q}_p}) \end{array}$$

$$\begin{array}{c}
 1.1 \longrightarrow (K \longleftarrow K_{i-1} \xrightarrow{*} \overline{\mathbb{Q}_p}) \\
 \searrow \quad \downarrow \\
 \quad \quad 1.1
 \end{array}$$

Monday's lecture: analytic facts about $\zeta(s)$

- Proving meromorphic continuation
- Proving functional eqn.

Prop Let D_p be a choice of absolute decomposition group, $I_p \leq D_p$ be the inertia group. Let K/\mathbb{Q} fin. Gal. Then $D_p|_K$ is a decomp. group for K/\mathbb{Q} . Same for I_p .

Pf.

$$\begin{array}{ccccc}
 G_{\mathbb{Q}_p} \cong D_p & \longrightarrow & G_{\mathbb{Q}} & & K \quad \wp \\
 \downarrow & & \downarrow & & | & | \\
 \text{Gal}(K/\mathbb{Q}_p) \cong D_{\wp} & \longrightarrow & \text{Gal}(K/\mathbb{Q}) & & \mathbb{Q} & \wp \\
 & & & & & \\
 & & & & K \longleftarrow \overline{\mathbb{Q}} \longrightarrow \overline{\mathbb{Q}_p} \\
 & & & & \searrow & \swarrow \\
 & & & & & \wp
 \end{array}$$

Ex. $\chi_l: G_{\mathbb{Q}} \longrightarrow \mathbb{Q}_l^*$ l -adic cyclotomic character

Unram'd at all $p \neq l$.

Let $p \neq l$ be prime.

$I_p|_{\mathbb{Q}(\mu_{p^n})} \leq \text{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q})$ is an inertia group for $\mathbb{Q}(\mu_{p^n})/\mathbb{Q}$, hence trivial.

$$G_{\mathbb{Q}} \rightarrow \text{Gal}(\mathbb{Q}(\mu_{l^n})/\mathbb{Q}) \cong \varprojlim_{n \geq 1} \text{Gal}(\mathbb{Q}(\mu_{l^n})/\mathbb{Q}) \rightarrow \varprojlim_{n \geq 1} (\mathbb{Z}/l^n\mathbb{Z})^\times \cong \mathbb{Z}_l^\times \hookrightarrow \mathbb{Q}_l^\times$$

$$I_p \longrightarrow \left(I_p|_{\mathbb{Q}(\mu_{l^n})} \right)_{n \geq 1} = \{1\}.$$

$$\sigma_p \mapsto \left(\frac{p}{\mathbb{Q}(\mu_{l^n})/\mathbb{Q}} \right) \mapsto \left(\left(\frac{p}{\mathbb{Q}(\mu_{l^n})/\mathbb{Q}} \right) \right)_{n \geq 1} \mapsto (p)_{n \geq 1} \mapsto p \mapsto p$$

\uparrow
 Frobenius at p
 of $\mathbb{Q}(\mu_{l^n})/\mathbb{Q}$

$$\chi_l(\sigma_p) = p \in \mathbb{Q}_l^\times \quad \forall p \neq l.$$

Note: χ_l is unramified at almost every prime

$\chi_l(\sigma_p)$ does not depend on l !

$\{\chi_l\}_l$ "compatible system"

L-functions

Examples

$$\chi: (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$$

$$\zeta(s) = \sum_{n \geq 1} n^{-s}$$

$$L(\chi, s) = \sum_{n \geq 1} \chi(n) n^{-s}$$

converge, holomorphic on $\text{Re}(s) > 1$.

$$\zeta(s) = \prod_p \frac{1}{1 - p^{-s}} \leftarrow \begin{array}{l} \text{characteristic polynomials} \\ \text{of } \rho(\sigma_p) \end{array}$$

$$L(\chi, s) = \prod_{p \nmid N} \frac{1}{1 - \chi(p)p^{-s}}$$

Deeper facts: analytic continuation, functional eqn.

$$L(\rho, s)$$

↑
Galois representation

2 dim'l Gal rep.

$$\frac{1}{1 - p^{-s} + p^{-2s}}$$