# Lecture 2

## · The absolute Galois group (cont)

$G_{\mathbb{Q}_p} = \mathrm{Gal}(\overline{\mathbb{Q}}_p|\mathbb{Q}_p) \hookrightarrow G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) \leftarrow \overline{\mathbb{Q}}$ is dense in $\overline{\mathbb{Q}}_p$ since $\mathbb{Q}$ is dense in $\mathbb{Q}_p$.

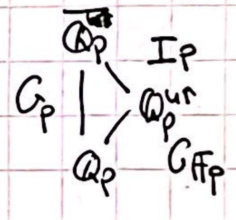
$G_{\mathbb{Q}_p} \equiv$ decomposition group.

**Def**: $\mathbb{Q}_p^{ur} \equiv$ max unramified extension of $\mathbb{Q}_p$ $= \bigcup_{\substack{F|\mathbb{Q}_p \\ \text{unram finite}}} F = \varinjlim_F F$

**fact**: $G(\mathbb{Q}_p^{ur}|\mathbb{Q}_p) \cong G(\overline{\mathbb{F}}_p|\mathbb{F}_p)$

$F|\mathbb{Q}_p$ unram deg $n$ $\Rightarrow$ $\mathrm{Gal}(F|\mathbb{Q}_p) \cong G(\mathbb{F}_{p^n}|\mathbb{F}_p) \Rightarrow \mathrm{Gal}(\mathbb{Q}_p^{ur}|\mathbb{Q}_p) =$

$$= \varprojlim_{\substack{F|\mathbb{Q}_p \\ \text{finite ur}}} \mathrm{Gal}(F|\mathbb{Q}_p) = \varprojlim_{n} G(\mathbb{F}_{p^n}|\mathbb{F}_p) = G_{\mathbb{F}_p} = \langle \phi_p \rangle .$$




$\Rightarrow$ $\mathrm{Res}: G_{\mathbb{Q}_p} \to G_{\mathbb{F}_p} \to 1$ $\quad$ $\mathrm{Ker}(\mathrm{Res}) = I_p$ inertia

$I_p = \{\sigma : \overline{\mathbb{Q}}_p \to \overline{\mathbb{Q}}_p \mid \sigma_{|\mathbb{Q}_p^{ur}} = \mathrm{Id}\}$.

we can lift $\phi_p \in G_{\mathbb{F}_p}$ (in a non-unique manner) to $G_p$. "a Frobenius automorphi

**Def**: A finite group. A Sylow p-~~gro~~subgroup is $B \leq A$ s.t. $p^k$ is the max p-power dividing $|A|$

of order $p^k$

A Sylow pro-p subgroup is an inverse limit of Sylow p-subgroups of $A_i$

$A = \varprojlim A_i$ profinite.

**Fact**: There exist a large normal Sylow pro-p subgroup of $I_p$

**Fact**: $I_p/W_p \cong \prod_{\ell \neq p} \mathbb{Z}_\ell$ $\qquad$ $\phi_p$ Frobenius as $\phi_p \in G_{\mathbb{Q}_p} \Rightarrow \forall \bar{\sigma} \in I_p/W_p$

$$\phi_p \bar{\sigma} \phi_p^{-1} = \bar{\sigma}^p$$

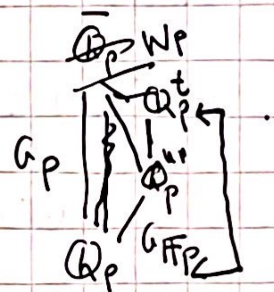
P. 1.17 $I_p / W_p$ corresponds to an extension of $\mathbb{Q}_p^{ur}$, the max. "tamely ramified" extn of $\mathbb{Q}_p$. Describe it (hint: $l^n$-th roots of 1, $l \neq p$).

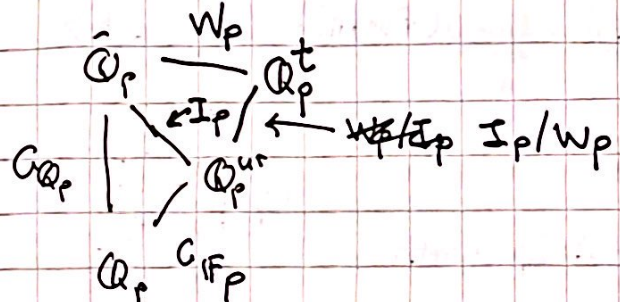
$K|\mathbb{Q}_p$ Galois $\Rightarrow$ $G_{\mathbb{Q}_p} \xrightarrow{Res} G(K|\mathbb{Q}_p) \to 1$ we say that $K|\mathbb{Q}_p$ is unramified

if $Res(I_p) = \{I\}$ i.e. if $\forall \sigma \in I_p$ $\sigma_{|K} = Id.$

It's tamely ramified if $Res(W_p) = \{I\}$ i.e. if $\forall \sigma \in W_p$, $\sigma_{|K} = Id.$ Other wildly ramified.

we have: $W_p \triangleleft I_p \triangleleft G_{\mathbb{Q}_p} \leq G_{\mathbb{Q}}$





Recall: $K|\mathbb{Q}$ finite $\Rightarrow$ $K$ is ramified at finitely many primes.

Every $K|\mathbb{Q}$ ramifies at least at a prime (not true for $F \neq \mathbb{Q}$).

· cyclotomic extensions

$\zeta_m := e^{2\pi i/m}$ primitive root of 1, $G(\mathbb{Q}(\zeta_m)|\mathbb{Q}) \simeq (\mathbb{Z}/p^m\mathbb{Z})^*$ abelian.

$K_l := \bigcup_{m \geq 1} \mathbb{Q}(\zeta_{l^m}) = \varinjlim_{m \geq 1} \mathbb{Q}(\zeta_{l^m}) \Rightarrow G(K_l|\mathbb{Q}) = \varprojlim_{m \geq 1} G(\mathbb{Q}(\zeta_{l^m})|\mathbb{Q}) \simeq \mathbb{Z}_l^*$.

$\varepsilon_l : G_{\mathbb{Q}} \to G(K_l|\mathbb{Q}) \simeq \mathbb{Z}_l^*$

$\sigma \mapsto \sigma_{|K_l} \mapsto \varepsilon_l(\sigma)$ $l$-adic cyclotomic char.

$\forall$ $l$-power root of 1, $\zeta_{l^m}$, $\sigma \in G_{\mathbb{Q}}$ $\sigma(\zeta_{l^m}) = \zeta_{l^m}^{a_m}$ $\Rightarrow$ $\sigma(\zeta) = \zeta^{\varepsilon_l(\sigma)}$ $\varepsilon_l(\sigma) = \sum_{m \geq 0} a_m l^m$

$\zeta_{l^{m+1}}^l = \zeta_{l^m}$ $a_m \in (\mathbb{Z}/l^m\mathbb{Z})^*$ $\zeta \in K_l$

$K_\ell | \mathbb{Q}$ is ramified at $\ell$ and $\infty$

$\boxed{c|K_\ell \neq Id.}$

Ramification at $\infty$:

$\mathbb{Q}_\infty = \mathbb{R}$

$\overline{\mathbb{Q}}_\infty = \mathbb{C}$

$Gal(\overline{\mathbb{Q}}_\infty | \mathbb{Q}_\infty) \hookrightarrow Gal(\overline{\mathbb{Q}}|\mathbb{Q})$

$\langle Id, c\rangle = G_\infty$

$\mathbb{Q}_\infty^{ur} = \mathbb{R}^{ur} = \mathbb{R}$

$G(\mathbb{Q}_\infty^{ur}, \mathbb{Q}_\infty) = \cancel{G(\mathbb{C}, \mathbb{R}) = Gal(\mathbb{C}|\mathbb{R})}$. $\{1\}$.

$I_\infty = G_\infty$.

$G_\infty = I_\infty = \{1, c\}$

~~Res~~

$\forall p \neq \ell \Rightarrow \varepsilon_\ell(\Phi_p) = p \in \mathbb{Z}_\ell^*$.

Def: $G$ group, $G^{ab} :=$ unique max abelian quotient of $G$ i.e. $G/[G,G]$ closed subgroup topologically generated by commutators $ghg^{-1}h^{-1}$

Thm: (Kr.-Weber) $\forall p$, padic character $= \varepsilon_p \Rightarrow \prod \varepsilon_p : G_{\mathbb{Q}}^{ab} \xrightarrow{\sim} \prod_p \mathbb{Z}_p^* \simeq \widehat{\mathbb{Z}}^*$

Thus $\Rightarrow$ classical: $F|\mathbb{Q}$ abelian $G(F|\mathbb{Q}) \simeq Gal(\overline{\mathbb{Q}}|\mathbb{Q}) / Gal(\overline{\mathbb{Q}}|F)$

$\Downarrow$ $G_{\mathbb{Q}}^{ab} \simeq \prod_p \mathbb{Z}_p^*$ (max) $\Rightarrow G(F|\mathbb{Q}) \hookrightarrow \prod_{p_i \text{ finite}} \mathbb{Z}_{p_i}^*$ (finite)

$\Downarrow$ local version:

$\pi : G_{\mathbb{Q}_p} \to G_{\mathbb{F}_p} \overset{I_p}{\Rightarrow} \pi \times \varepsilon_p : G_{\mathbb{Q}_p}^{ab} \xrightarrow{\sim} G_{\mathbb{F}_p} \times \mathbb{Z}_p^*$

$G_{\mathbb{Q}_p}^{ur} \simeq \widehat{\mathbb{Z}}^* \hookrightarrow G_{\mathbb{Q}}^{ab} \Leftarrow\hookrightarrow \widehat{\mathbb{Z}}^*$

Conj (inverse Galois problem) Any finite group can be obtained as a discrete quotient of $G_{\mathbb{Q}}$. ($\leadsto G_{\mathbb{Q}}$ complicated!!) i.e. $G_{\mathbb{Q}} / Gal(\overline{\mathbb{Q}}|F) \simeq Gal(F|\mathbb{Q}) \to$ finite

Known (Waterhouse, 1974) Every profinite group can be obtained as $Gal(F/K)$ for some Galois extension $L/K$ $\to$ maybe ~~(surely)~~ not of a number field even in finite case!!

· Restricting ramification

Natural (geometric) representations are finitely ramified too

$S =$ finite set of rational primes (abs. values) $\ni \infty$.

Want $K|\mathbb{Q}$ unramified outside $S$ (i.e. $\forall v \notin S$ $Res(I_v) = \{Id\}$) Galois.

Maybe $c \neq Id$

$\mathbb{Q}_S \equiv$ maximal extension of $\mathbb{Q}$ unramified outside $S$, $G_{\mathbb{Q},S} = G(\mathbb{Q}_S, \mathbb{Q})$

$S \equiv$ primes of $K \ni \infty$'s

$K_S \equiv \dots$ $\quad K \dots \quad S$, $G_{K,S} = \mathrm{Gal}(K_S | K)$.

<u>Thm (Hermite-Minkowski)</u> $K|\mathbb{Q}$ finite. $S \equiv$ finite set of primes $d \in \mathbb{N}$.

$\Rightarrow \exists$ finitely many $F|K$ unramified outside $S$.

<u>Cor</u>: $\mathrm{Hom}_{\mathrm{cont}}(G_{K,S}, \mathbb{Z}/p\mathbb{Z})$ is finite.

$\phi: G_{K,S} \to \mathbb{Z}/p\mathbb{Z}$ cont $\Rightarrow \mathrm{Ker}(\phi)$ open-closed in $G_{K,S} \Rightarrow$

it has finite index and corresponds with ~~$G(\bar{K}/F)$~~ $G(K_S|F)$ of finite index

~~$G(F|K) \cong G(\bar{K}/K)$~~
$\Uparrow$
~~finite~~

$$G(F|K) \cong G(K_S|K)/G(K_S/F)$$

moreover $F/K$ unramified outside $K$ by construction $\Rightarrow$ finitely many choices.

$$G_{K,S}/\mathrm{Ker}(\phi) \cong \mathbb{Z}/p\mathbb{Z} \leftarrow \text{also.}$$
$\Uparrow$
finitely many choices

<u>Thm (Mazur p-finiteness condition)</u>

$\boxed{\text{Let } p \text{ prime, } K|\mathbb{Q} \text{ finite, } S \equiv \text{set of non-arch places. } G \subseteq G_{K,S} \text{ open} \Rightarrow \exists \text{ finitely many } f: G \to \mathbb{Z}/p\mathbb{Z} \text{ continuous}}$

<u>Thm</u>: $K|\mathbb{Q}_p$ finite $\Rightarrow G_K$ is top. f.g.

<u>Prop</u>: $G_{K,S}$ countably f.g.

<u>Conj (Šafarevič)</u> $G_{K,S}$ is top. f.g. (replace by p-finiteness)

$\mathfrak{P} \subseteq \mathbb{Q}_S$ $\quad \sigma \in I_p \quad \sigma|_{\mathbb{Q}_p^{ur}} = Id \quad \mathbb{Q}_{p,S} \subseteq \mathbb{Q}_p^{ur} \Rightarrow \sigma|_{\mathbb{Q}_{p,S}} = Id$

$p \subseteq \mathbb{Q}_S$

$\forall p, \quad \varphi : G_{\mathbb{Q}_p} \xrightarrow{Res} G_{\mathbb{Q},S}$, $\quad p \notin S \Rightarrow \varphi(I_p) = \{1\} \Rightarrow \exists \Phi_p \in G_{\mathbb{Q},S}$ well def.

$\sigma : \bar{\mathbb{Q}}_p \to \bar{\mathbb{Q}}_p \mapsto \sigma|_{\mathbb{Q}_{p,S}}$ $\quad$ respects ramification!!

<u>conj</u>: i) $p \in S \Rightarrow G_{\mathbb{Q}_p} \hookrightarrow G_{\mathbb{Q},S}$

ii) $p \notin S \Rightarrow Ker(\varphi) = I_p$ and $G_{\mathbb{Q}_p} / I_p \hookrightarrow G_{\mathbb{Q},S}$.

Notice: if we don't want to fix $G_{\mathbb{Q}_p} \to G_{\mathbb{Q},S}$ the Frob. element is only a conjugation class.

<u>Thm (Chebotarev)</u>. $K|\mathbb{Q}$ Galois unramified outside $S$. $T$ finite set of primes over $S$ $\forall p \notin T$, $\exists$ well def. Frob $[\Phi_p] \in G(K|\mathbb{Q})$. The union of these is dense in $G(K|\mathbb{Q})$.

- <u>Galois representations</u>

Representations of $G_{\mathbb{Q},S}$ arise naturally from elliptic curves, modular forms, Hilbert, Bianchi forms etc.

The maps $G_{\mathbb{Q}_p} \to G_{\mathbb{Q},S}$ are defined up to conjugation. e.g. $p \notin S \Rightarrow$ $\Phi_p$ is def up to conj but char poly of $\Phi_p$ under $\rho : G_{\mathbb{Q},S} \to GL_n(K)$ is well defined.

<u>Def</u>: A Galois rep over a topological ring $A$, unramified outside $S$ is a continuous hom $\rho : G_{\mathbb{Q},S} \to GL_n(A)$

$\rho_1, \rho_2$ are equivalent if $\exists P \in GL_n(A)$ s.t $P^{-1} \rho_1 P = \rho_2$.

- Given $\rho: G_{\mathbb{Q},S} \to GL_n(A)$ consider the $A$-module (free) of rk $n$ and give it a continuous $G_{\mathbb{Q},S}$-action $g \cdot m = \rho(g)m$.

- Given $M \simeq A^n$ w/ continuous action $g \cdot m$, choose a basis of $M$ over $A$ and we have $\rho: G_{\mathbb{Q},S} \to GL_n(A)$

- $M$ $A$-module (finite free) $G \circlearrowright M$ continuous, $G$ profinite s.t. $M = \varprojlim_H M^H$

$H$ open normal subgroups of $G \Rightarrow M$ is a module over the completed group ring

$A[[G]] = \varprojlim_H A[G/H]$

when $A$ is a profinite ring this happens $\Rightarrow$ a rep. of $G$ over $A$ is the same as an $A[[G]]$-module $M$ finite-free as $A$-module.

$\rho: G \to GL_n(A)$ extends to $A[[G]] \to M_n(A)$ continuous hom of $A$-algebras.

and reciprocally by restriction.

For us: $A = \mathbb{C}$ : Artin reps $\mathrm{Im}(\rho) \subseteq GL_n(A)$ must be finite.

$A = F$ : ~~noetherian~~ finite field, elliptic curves / modular forms. (Serre conj)

most important to us

$A = \mathbb{Z}_p, \mathbb{Q}_p$.

$A$ = complete noetherian local ring w/ finite residual field (prof. ring)

coeff ring.