Lecture 1 19/04

I.1. Galois groups of infinite Galois extensions

K perfect field, $F|K$ normal $G(F|K) = \mathrm{Gal}(F|K) = \{\sigma : F \to F \mid \sigma|_K = Id\}$.
(every finite extn. is sep)

$G(\bar{K}|K) = G_K$ abs. Galois group.

If F/K finite $\Rightarrow$ Σ: Subgroups of $G(F/K) \xrightarrow{1-to-1}$ subextensions of F/K

$$H \longmapsto F^H$$

$$G(F/L) \longleftarrow L/K$$

This doesn't work for infinite extensions:

ex $K = \mathbb{F}_p$ $\quad \phi_p : \bar{\mathbb{F}}_p \to \bar{\mathbb{F}}_p$, $x \mapsto x^p$ Frobenius at p.

$\forall n \; \exists! \; \mathbb{F}_{p^n}/\mathbb{F}_p$ of deg n, $Z(x^{p^n} - x)$, $\mathrm{Gal}(\mathbb{F}_{p^n}|\mathbb{F}_p) = \langle \phi_p \rangle = \{Id, \phi, \phi^2, \dots, \phi^{n-1}\}$

$Z := \langle \phi_p \rangle$ infinite cyclic group fixing $\mathbb{F}_p$. Is it $Z = G_{\mathbb{F}_p}$?

Choose $\{a_m\}$ s.t $a_n \equiv a_m \mod m$ if $m|n$

Define $\psi : \bar{\mathbb{F}}_p \to \bar{\mathbb{F}}_p$ by setting $\psi|_{\mathbb{F}_{p^n}} = \phi_p^{a_n}$. This is compatible and hence
$m|n \Rightarrow \mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$, $x \in \mathbb{F}_{p^m}$: $\phi_p^{a_n}(x) = x^{p^{a_n}} = x^{p^{a_m} \cdot p^{mt}} = x^{p^{a_m}} = \phi_p^{a_m}(x)$

ψ is well defined $\Rightarrow \psi \in G_{\mathbb{F}_p}$.
$\psi = \phi_p^a$

Now, $\psi \in Z \iff \exists a$ s.t $a_n = a \;\; \forall n$!! $\Rightarrow Z \subsetneq G_{\mathbb{F}_p}$.

P.1.1 Show that many $\{a_n\}$ exist and compatibility.

P.1.2 How big is $G_{\mathbb{F}_p}$? $\quad a_p \in \mathbb{Z}/p\mathbb{Z}, \dots a_{p^r} \in \mathbb{Z}/p^r\mathbb{Z}$ $\quad a_{p^r} \equiv a_p \mod p$
$\Rightarrow G_{\mathbb{F}_p} \supseteq \mathbb{Z}_p$.

Is it countable?

$\bar{\mathbb{F}}_p^{Z} = \mathbb{F}_p \quad Z \neq G_{\mathbb{F}_p}$

$\bar{Z} = G_{\mathbb{F}_p} \neq Z$

Solution: Introduce topology, so that Galois corr works with closed subgroups.

Def: F/K Galois extension. $\forall K'/K$ finite Galois subext, consider $G(K'/K)$.

$K \subseteq K' \subseteq K''$, Res: $G(K''/K) \to G(K'/K)$.

This defines an inverse system and define $G(F/K) = \varprojlim_{\substack{K'/K \\ \text{finite}}} G(K'/K)$ with its profinite topology. (basis of open subsets $= gV$, $\underset{\text{finite index}}{V \leq G(F/K)}$)

An element of the inverse limit is $\{\sigma_{K'} \in G(K'/K)\}$ compatible w/ restriction.

This is similar to $\{a_m\}$ before.

· <u>On inverse limits</u> (Complements to lecture 1)

I : partially ordered set, directed set. $\forall i,j \in I \ \exists k \in I$ s.t $i \leq k$, $j \leq k$.

e.g. $I = (\mathbb{N}_+, \leq)$ or $(\mathbb{N}_+, |)$. $\quad a,b \in \mathbb{N}_+$ $d=(a,b)$ $d=[a,b]$ $a|d$, $b|d$

- directed set I
- $\forall i \in I$, G_i group/ring/set.
- $\forall i,j \in I$ s.t $i \leq j$, $\phi_{ij} : G_j \to G_i$ homomorphism of groups/rings/sets.

require: $\phi_{ii} = Id$, $\quad i \leq j \leq k \Rightarrow \phi_{ik} = \cancel{\phi_{jk}} \cancel{\phi_{ij}}$ $\phi_{ij} \circ \phi_{jk}$

$$\begin{tikzcd} G_k \arrow[r, "\phi_{ik}"] \arrow[dr] & G_i \\ & G_j \arrow[u] \end{tikzcd}$$

<u>e.g.</u> $I = (\mathbb{N}_+, \leq)$ p prime $\forall n$, $G_n := \mathbb{Z}/p^n\mathbb{Z}$ ring.

if $n \leq m$, $\phi_{nm} = $ red mod n.

<u>P.1.33.</u> This defines an inverse system

<u>e.g.</u> $I = (\mathbb{N}_+, |)$ $\forall n \in I$, $G_n := \mathbb{Z}/n\mathbb{Z}$, $n | m$ $\phi_{nm} = $ red mod n

<u>P.1.34</u> This defines inverse system.

<u>e.g.</u> F/K field extn, $I = $ finite Galois subextensions.

$\underset{\text{finite}}{\forall K'/K \in I}$, $G_{K'} := G(K'/K)$, $K' \leq K''$, $\phi_{K',K''} = \mathrm{Res}\ G(K''/K) \to G(K'/K)$

P.1.35 This defines an inverse system.

Inverse limits: Given an inverse system of groups/rings/sets, G group/ring/set is the inverse limit of the system if:

- $\exists\ \psi_i : G \to G_i$ s.t $i \leq j \Rightarrow \psi_i = \phi_{ij} \circ \psi_j$

- G is universal: given G' group/ring/set with that set of homomorphisms $\exists!\ G' \to G$ through which they factor.

Not: $G = \varprojlim_i G_i$.

Construction: $P = \prod_{i \in I} G_i$, $G = \{(g_i)_{i\in I} \mid \phi_{ij}(g_j) = g_i\ ,\ i \leq j\}$

P.1.36 Check it works.

$+: G\times G \to G$ continuous.
$i: G \to G\ a \mapsto a^{-1}$

P.1.37 If each of the G_i is a topological group, ϕ_{ij} continuous $\Rightarrow$ G is the inverse limit as topological groups.

Most of situations, G_i are finite (like $\mathbb{Z}/p^n\mathbb{Z}$), give discrete topology ($\Rightarrow$ compact)
$\Rightarrow$ P compact w/ product topology $\Rightarrow$ G closed subset hence compact (and T_2)

The previous inverse limits are $\mathbb{Z}_p, \hat{\mathbb{Z}}, G(F/K)$.

Def: A profinite group is a topological group w/ is the inverse limit of an inverse system of finite groups (w/ discrete topology)

Let F/K infinite Galois. $G = \{\sigma : F \to F \mid \sigma|_K = Id\}$

P.1.38 $\forall$ K'/K finite Galois. $G(F/K')$ = normal subgroup of $G = \{\sigma : F \to F \mid \sigma|_{K'} = Id\}$.

Define a topology on G ; $\forall g \in G$, a basis of neighbourhoods of g is $\{g\,G(F/K') \mid K'/K$ finite Galois K-ext$\}$ $\Rightarrow$ this agrees with before.

P.1.4 $G(F/K)$ is Hausdorff, compact and tot. disconnected.

P.1.5 G topological group. Show that all open subgroups of G are also closed. $G \setminus H = \bigcup_{g \notin H} gH$ open. If G is compact $\Rightarrow$ all open subgroups are of finite index in G.

Any closed subgroup w/ finite index is open.

Suppose G profinite, $G = \varprojlim_{i} G_i$, $K_i = \mathrm{Ker}(\phi_i : G \to G_i)$. G_i discrete $\Rightarrow$ K_i open.

$G/K_i \cong G_i$ finite + closed $\Rightarrow$ open.

P.1.40: $\{K_i, i \in I\}$ is a basis of open neighbourhoods of $1 \in G$.

Thm: G Hausdorff, compact topological group. TFSAE:

i) G profinite

ii) G totally disconnected.

iii) G has a set of open normal subgroups which is a system of neighbourhoods of $1 \in G$.

Being profinite is kept by taking closed subgroups, quotients by closed subgroups, arbitrary direct products and inverse limits.

Thm 1.1 (Galois correspondence for ∞ extns)

F/K Galois $\Rightarrow$ $K'/K \longmapsto G(F/K')$

defines a bijective 1-to-1 reversing arrows correspondence between K'/K subext and closed subgroups of $G(F/K)$. The inverse is $H \mapsto F^H$.

Notice that open ⇒ closed and finite index ⇒ give finite subextensions.

e.g. $G(\mathbb{F}_{p^n}|\mathbb{F}_p) \simeq \mathbb{Z}/n\mathbb{Z} \Rightarrow G_{\mathbb{F}_p} = \hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ red: mod m.

$\mathbb{Z}$ dense (⇒not closed) in $G_{\mathbb{F}_p}$ (say $\mathbb{Z}$ "topologically generates")

P. 1.10 $\hat{\mathbb{Z}} \simeq \prod_p \mathbb{Z}_p$.

Def: Let G be a topological group. A G-modules is an abelian top. group M

with $G \times M \to M$ continuous s.t. i) $1m = m \ \forall m \in M$
$(\sigma, m) \mapsto \sigma m$

ii) $\sigma(m+n) = \sigma m + \sigma n \ \ \forall \sigma \in G,\ n, m \in M$

iii) $(\sigma\tau)(m) = \sigma(\tau m), \ \forall \sigma, \tau \in G, m \in M$.

Usually M is discrete (like p^k-torsion points).

P. 1.12. G profinite group. M discrete, $\forall H \subseteq G$, M^H = fixed by H.

$G \times M \to M$ continuous $\Leftrightarrow M = \bigcup_{H \text{ open}} M^H$.

we say that.

Let A be a topological ring s.t the abelian group is profinite ⇒ A profinite.

check:

$A \simeq \varprojlim_{\substack{I \text{ closed ideal} \\ \text{of finite index}}} A/I$. obs: $A \neq 0 \Rightarrow I$ closed, finite index exists.

Def: G is a pro-p group if every quotient of G is a p-group E.g. $\mathbb{Z}_p$.

P.1.15 $\Gamma_2(\mathbb{Z}_p) = \operatorname{Ker}\{GL_2(\mathbb{Z}_p) \to GL_2(\mathbb{F}_p)\}$ is a pro-p group.

Def: $G^{(p)} := \varprojlim_{\substack{H \text{ open normal} \\ G/H \text{ p-group}}} G/H$.

Prop: i) $\exists \pi: G \to G^{(p)} \to 1$ canonical continuous s.t. $\forall\, \varphi: G \to \Upsilon$ discrete p-group

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d] & \Upsilon \\ G^{(p)} \arrow[ur] & \end{tikzcd}$$

ii) $G = \hat{\mathbb{Z}}$ ¿$G^{(p)}$?

· The absolute Galois group

There are many ways of extending the p-adic valuation on $\mathbb{Q}$ to $\bar{\mathbb{Q}}$. Choose 1.

get $G_{\mathbb{Q}_p} := \mathrm{Gal}(\bar{\mathbb{Q}}_p|\mathbb{Q}_p) \hookrightarrow G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}|\mathbb{Q})$. $1 \xrightarrow{\text{cont}} \mathrm{Gal}(\bar{\mathbb{Q}}_p|\mathbb{Q}_p) \xrightarrow{\text{Res}} \mathrm{Gal}(\bar{\mathbb{Q}}|\mathbb{Q})$, $\sigma \longmapsto \sigma_{|\bar{\mathbb{Q}}}$ fixes $\mathbb{Q}$.

Changing the embedding changes the inclusion by conjugation. The image is called decomposition group at p and we identify it w/ $G_{\mathbb{Q}_p}$.

Def: $\mathbb{Q}_p^{ur} \equiv$ max unramified extension of $\mathbb{Q}_p$

Fact: $G(\mathbb{Q}_p^{ur}|\mathbb{Q}_p) \cong G(\bar{\mathbb{F}}_p|\mathbb{F}_p)$. Prove! $1 \to G(\mathbb{Q}_p^{ur}|\mathbb{Q}_p) \to G(\bar{\mathbb{F}}_p|\mathbb{F}_p) \to 1$. $\sigma \longmapsto \{ \mathcal{O}_{\mathbb{Q}_p^{ur}}/\pi \to \mathcal{O}_{\mathbb{Q}_p^{ur}}/\pi \}$, $x + \pi \longmapsto \sigma(x) + \pi$

$\Rightarrow$ Res: $G_{\mathbb{Q}_p} \to \underbrace{G_{\mathbb{F}_p}}_{\langle \phi_p \rangle} \to 1$, Ker(Res) $:= I_p$ inertia.

lift ϕ_p to $G_{\mathbb{Q}_p}$: a Frobenius automorphism.

There is a large normal Sylow pro-p subgroup of I_p: $W_p \triangleleft I_p$. (if p^α highest $|n$, subgr. of order p^α is p-Sylow.) (wild inertia.)

Fact: $I_p/W_p :=$ tame inertia

Fact: $I_p/W_p \cong \prod_{\ell \neq p} \mathbb{Z}_\ell$, ϕ_p Frob, $\bar{\sigma} \in I_p/W_p \Rightarrow \phi_p \bar{\sigma} \phi_p^{-1} = \bar{\sigma}^p$!

P.1.17 I_p/W_p corresponds to an extension of $\mathbb{Q}_p^{ur}$, the max tamely ramified extension of $\mathbb{Q}_p$. Describe it. Hint: ℓ^n roots of 1.

$K|\mathbb{Q}_p$ Galois $\Rightarrow$ $G_{\mathbb{Q}_p} \xrightarrow{\text{Res}} \text{Gal}(K|\mathbb{Q}_p) \to 1$. We say that $K|\mathbb{Q}_p$ unramified if $\text{Res}(I_p) = \{1\}$. It's tamely ramified if $\text{Res}(W_p) = \{1\}$ otherw wildly ramified

We have: $W_p \trianglelefteq I_p \trianglelefteq G_p \leq G_{\mathbb{Q}}$.

<u>Thm</u> $K|\mathbb{Q}$ finite $\Rightarrow$ K is ramified at finitely many primes. Every $K|\mathbb{Q}$ ramifies at at least 1 prime (not always true for base $\neq \mathbb{Q}$).