Lecture 39

(39.0) Recall that for a finite Galois extension E/F we have a bijection between

$$\begin{array}{ccc} \text{Sub-}F\text{-extensions of } E & \longleftrightarrow & \text{Subgroups of } gal(E/F) \\ F \subset F' \subset E & \longmapsto & gal(E/F') < gal(E/F) \\ F \subset E^H \subset E & \longleftarrow & H < gal(E/F) \end{array}$$

Moreover $\begin{array}{c} F \subset F' \subset E \text{ s.t.} \\ F'/F \text{ is also Galois} \end{array} \longleftrightarrow \begin{array}{c} \text{Normal subgroups of} \\ gal(E/F) \end{array}$

Also recall that we have proved that

E/F is a Galois extn. $\iff$ Normal and separable.

[Finite case] $\iff$ E is the splitting extension of a separable polynomial $p(X) \in F[X]$

In the infinite case, being a Galois extn. is same as being the splitting extension of a set of separable polynomials.

(39.1) Let us review first an infinite Galois extension where the bijection between subextensions and subgroups fails.

$F = \mathbb{Q}$ $\qquad E = \mathbb{Q}(\sqrt{p} : p \text{ prime})$

$= \text{splitting extn. of } \{X^2 - p : p \in \mathbb{Z}_{\geq 2} \text{ prime}\}$

(Characteristic of F is 0, hence F is perfect, hence separability is not an issue.)

Now $G = \mathrm{Gal}(E/F) = \prod_{p:\text{ prime}} \mathbb{Z}/2\mathbb{Z}$

$$\begin{array}{c} \vee \\ H = \bigoplus_{p:\text{ prime}} \mathbb{Z}/2\mathbb{Z}. \end{array}$$

Then $E^H = E^G = F$ but $H \neq G$.

<u>Fix.</u> G is a <u>topological group</u> and $\overline{H} = G$ ← closure.

We will see later that the bijection is between sub-F-extns. of E and <u>closed subgroups</u> of $\mathrm{Gal}(E/F)$.

Remark. This incorporates the finite case as well, as for finite G, the topology would be <u>discrete</u> – so every subgroup is closed. In fact, taken as the guiding principle.

Closure of a subgroup $H < G$ $=$ $\mathrm{Gal}(E/E^H)$

forces the (correct) topology on G.

(39.2) Brief refresher on the terminology from topology.

(i) A topology on a set X is the prescription of a subset

$\tau \subset 2^X$ ← set of all subsets of X

satisfying
- $\phi \in \mathcal{T}$ and $X \in \mathcal{T}$
- $U_i \in \mathcal{T}$ ($i \in I$ ← any set) $\Rightarrow \bigcup_{i \in I} U_i \in \mathcal{T}$
- $\mathcal{U}_1, \mathcal{U}_2 \in \mathcal{T} \Rightarrow \mathcal{U}_1 \cap \mathcal{U}_2 \in \mathcal{T}$.

(2) We just say that $(X, \mathcal{T})$, or just X if $\mathcal{T}$ is agreed upon, is a topological space. Subsets of X which feature in $\mathcal{T}$ are called <u>open sets</u>. Complements of open sets are called <u>closed sets</u>. The collection of closed sets is stable under taking finite union and arbitrary intersections.

$$\forall \ Y \subset X, \quad \overline{Y} \text{ (closure of } Y) = \bigcap_{\substack{F \supset Y \\ F \text{ is closed}}} F = \text{smallest closed set containing } Y.$$

Fundamental system of (open) neighbourhoods (nhd for short):

Assume we are given, $\forall p \in X$, a collection (i.e. set) of (open) subsets of a topological space $(X, \mathcal{T})$, say $\mathcal{N}(p)$. We say $\{\mathcal{N}(p)\}$ is a fundamental system of nhds, if

$$(*) \quad \mathcal{U} \subset X \text{ is open} \iff \forall p \in \mathcal{U}, \ \exists \ V \in \mathcal{N}(p), \text{ s.t. } V \subset \mathcal{U}.$$

Conversely, if $\mathcal{N}(p) \subset 2^X$ is given, for every $p \in X$,

s.t. (1) $p \in \mathcal{U} \quad \forall\, \mathcal{U} \in \mathcal{N}(p)$

(2) $V_1, V_2 \in \mathcal{N}(p) \Rightarrow V_1 \cap V_2 \in \mathcal{N}(p)$

Then $(*)$ can be taken as a definition of a unique topology $\mathcal{T}$ on X (i.e. $\phi, X \in \mathcal{T}$ and $\phi \neq \mathcal{U} \subsetneq X$ is in $\mathcal{T}$ if $\forall\, p \in \mathcal{U},\ \exists\, V \in \mathcal{N}(p)$ s.t. $V \subset \mathcal{U}$) for which $\{\mathcal{N}(p)\}$ is a fundamental system of nhds. [This is very very easy to prove.].

(39.3) Definition. A topological group G, is a group and a topological space s.t.

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (\sigma_1, \sigma_2) & \longmapsto & \sigma_1 \sigma_2 \end{array} \qquad\qquad \begin{array}{ccc} G & \longrightarrow & G \\ \sigma & \longmapsto & \sigma^{-1} \end{array}$$

are continuous (= inverse image of an open set is open

Recall open sets in $X \times Y$ = $\mathcal{U} \times V$ where $\begin{array}{l} \mathcal{U} \subset X \text{ open} \\ V \subset Y \text{ open} \end{array}$).

Remarks. – (1) G is "group object" in the category of topological spaces. Such notion exists for any category with a final object – needed to define $e \in G$.

(2). The product topology on $X \times Y$, for two topological spaces X and Y is defined so as to have the projection maps

$$\begin{array}{ccc} X \times Y & \longrightarrow & Y \\ \downarrow & & \\ X & & \end{array}$$

continuous. Given a continuous map $X \times Y \xrightarrow{f} Z$ and fixing $x \in X$, gives rise to a continuous map $\begin{array}{ccc} Y & \longrightarrow & Z \\ y & \longmapsto & f(x,y) \end{array}$ as it is the composition of

$$Y \xrightarrow{\sim} \{x\} \times Y \hookrightarrow X \times Y \longrightarrow Z.$$

(39.4) By the remark above we immediately have the following properties of a topological group G.

(a) $\forall\, \sigma \in G$, $\begin{array}{rl} \mathcal{L}_\sigma : G & \longrightarrow G \\ \tau & \longmapsto \sigma\tau \end{array}$ and $\begin{array}{rl} R_\sigma : G & \longrightarrow G \\ \tau & \longmapsto \tau\sigma \end{array}$

are homeomorphisms (iso in the category $\underline{\text{Top}}$).

(b) $\forall \sigma \in G$, $\quad Ad(\sigma) : \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & \sigma x \sigma^{-1} \end{array}$ is a

homeo. and a group ~~ho~~ hom (= iso of topological groups).

(39.5) Some examples of topological groups.

(1) G: any group. $\mathcal{T} = 2^G$ - discrete group.

(2) $G = (\mathbb{R}, +)$ — additive group of real numbers

$H = (\mathbb{R}_{>0}, \cdot)$ — mult. group of positive real numbers.

(Note $G \xrightarrow{\sim} H$ as top. gps - by $x \longmapsto e^x$.)

(3) $\underbrace{G = GL_2(\mathbb{R})^+}_{\text{subspace topology}} = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : \begin{array}{c} ad - bc > 0 \\ (a, b, c, d \in \mathbb{R}) \end{array} \right\} \subset \underbrace{\mathbb{R}^4}_{\text{product topology}}$

~~(39.6) Note: by (39.4) (a), the topology on G is~~

~~complet~~

(39.6) Prop. Let G be a topological group.

(i) If $H < G$ is an open subgroup, then H is closed.

(ii) If $H < G$ is a closed subgroup s.t. $|G/H| < \infty$ then H is open.

Proof. - $G = \bigsqcup_{\substack{\sigma \in G/H \\ \text{coset rep.}}} \sigma H$. <u>(i)</u>: As H is open, so is σH $(\forall \sigma \in G)$. Hence $H = G \setminus \boxed{\bigsqcup_{\substack{\sigma \in G/H \\ \text{coset rep.} \\ \sigma \notin H}} \sigma H}$ arbitrary union of open sets is open

so H is ~~a~~ an complement of open set $\Rightarrow$ H is closed.

<u>(ii)</u> - same argument - with "finite union of closed sets is closed". □

Remark. - A topological space X is called <u>connected</u> if ϕ and X are the only subsets which are both open & closed.

(i.e. $X = X_1 \underset{\text{disjoint}}{\sqcup} X_2$; X_1, X_2 open $\Rightarrow$ $X_1 = X$ or $X_2 = X$.)

(39.7) Note: By (39.4) (a) above, in order to endow a group G with a topology, turning it into a topological group, it is necessary and sufficient to have a collection $\mathcal{N}(e) \subset 2^G$ satisfying:

(0) $e \in \mathcal{U} \quad \forall\, \mathcal{U} \in \mathcal{N}(e)$; (1) $\forall\, \mathcal{U}_1, \mathcal{U}_2 \in \mathcal{N}(e), \exists\, V \in \mathcal{N}(e)$ s.t. $V \subset \mathcal{U}_1 \cap \mathcal{U}_2$

(2) $\forall\, \mathcal{U} \in \mathcal{N}(e)$, $\exists\, V \in \mathcal{N}(e)$ s.t.

$$V \cdot V := \{\sigma\tau \mid \sigma, \tau \in V\} \subset \mathcal{U}$$

(3) $\forall\, \mathcal{U} \in \mathcal{N}(e)$, $\mathcal{U}^{-1} := \{\sigma^{-1} \mid \sigma \in \mathcal{U}\} \in \mathcal{N}(e)$

(4) $\forall\, \sigma \in G$, $\mathcal{U} \in \mathcal{N}(e)$, $\exists\, V \in \mathcal{N}(e)$ s.t. $\sigma V \sigma^{-1} \subset \mathcal{U}$.

(39.8) Profinite groups. - A profinite group is a topological group G is an inverse (or projective) limit of an inverse system of finite discrete groups in the category of topological groups.

That is, we have a partially ordered set $(I, \leq)$, and an inverse system $\left(\{G_i\}_{i \in I}, \{\varphi_{ij} : G_j \to G_i\}_{i \leq j} \right)$ where each G_i is a finite, discrete group and $\varphi_{ij} : G_j \to G_i$ are group homs

$$G = \varprojlim_{i \in I} G_i \subset \prod_{i \in I} G_i =: \tilde{G}$$

Thus, as a group $G = \{ (\sigma_i) \in \tilde{G} \mid \forall\, i \le j \quad \varphi_{ij}(\sigma_j) = \sigma_i \}$

Topology on $\tilde{G}$: is <u>coarsest</u> s.t. $\tilde{G} \xrightarrow{\pi_i} G_i$ is cnts. $\forall\, i \in I$. Namely, sub-base of open sets near $e \in \tilde{G}$ is given by $H_i = \prod_{\substack{j \neq i \\ j \in I}} G_j \times \{e_i\}$. So,

$$\mathcal{N}(e) = \{ H_J = \bigcap_{j \in J} H_j \ : \ J \subset I \text{ finite subset} \}$$

G inherits subspace topology from $\tilde{G}$.

Remarks. — (1) H_J defined above is clearly a normal subgroup. As it is open, it is also closed.

(2) If $(I, \le)$ is directed, as it ~~would~~ will be in next lecture,

For G, $\mathcal{N}(e)_G = \{ H_j \cap G : j \in I \}$.

This is because $\forall$ finite $J \subset I$, $\exists\, i \in I$ s.t. $j \le i \ \forall\, j \in J$.

So, in the inverse system $\varphi_{ji} : G_i \longrightarrow G_j \quad \forall\, j \in J$

$e_i \longmapsto e_j$

$$\Rightarrow \quad H_i \cap G \subset \bigcap_{j \in J} H_j \cap G$$

(39.9) Prop. – Let G be a profinite group. Then G is compact, Hausdorff and totally disconnected.

[These topological properties characterize profinite groups. But we wont prove it here.]

Proof As $G = \varprojlim_{i \in I, \leq} (G_i, \varphi_{ij}) \subset \tilde{G} = \prod_{i \in I} G_i$

$\mathcal{N}(e)_G = \{ H_J \cap G : J \subset I \text{ finite} \}$

$\mathcal{N}(e) = \{ H_J : J \subset I \text{ finite} \}$

$H_J := \{ (\sigma_i) \in \tilde{G} \mid \sigma_j = e_j \in G_j \ \forall j \in J \}$

(1) As G_i is finite and discrete, it is compact ($\forall i \in I$).
Thus $\tilde{G}$ is compact (Tychonoff's theorem $\prod$ compact = compact).
So it is enough to prove that $G \subset \tilde{G}$ is closed. So $\forall i \leq j$,
let $F_{ij} = \{ (\sigma_k) \in \tilde{G} \mid \varphi_{ij}(\sigma_j) = \sigma_i \} \subset \tilde{G}$.

$$F_{ij} = \operatorname{Ker} \begin{pmatrix} \tilde{G} \longrightarrow G_i \\ \underline{\sigma} \longmapsto \sigma_i^{-1} \varphi_{ij}(\sigma_j) \end{pmatrix}$$

Hence is open, (as $\{e_i\} \subset G_i$ is open) subgroup. Hence also closed

$$G = \bigcap_{i \leq j} F_{ij}$$ = intersection of closed sets is closed. Hence G is compact.

The rest is based on the following observation. If $\sigma \neq e$ in G, let $i \in I$ be s.t. $\sigma_i \neq e_i$ in G_i. Then $e \in H_i$ ← open & closed.
$\sigma \notin H_i$

□