LECTURE 32

(32.0) Generalities on topological groups.– A topological group is a group G, together with a topology $\mathcal{T} \subset 2^G$ (that is, (i) $\emptyset, X \in \mathcal{T}$, and (ii) $\mathcal{T}$ is closed under arbitrary unions and finite intersections), such that multiplication and inverse

$$m : G \times G \to G, \qquad i : G \to G$$

(here, $m(a,b) = ab$ and $i(a) = a^{-1}$) are continuous maps.

For $a \in G$, we will denote by $\mathcal{T}(a) = \{U \in \mathcal{T} : a \in U\}$. A subset $\mathcal{B}(a) \subset \mathcal{T}(a)$ is said to be a *fundamental system of neighbourhoods* if for every $U \in \mathcal{T}(a)$, there exists $V \in \mathcal{B}(a)$ such that $V \subset U$.

The continuity of multiplication can be written more explicitly as the following condition on $\mathcal{T}$: for any $a, b \in G$ and $U \in \mathcal{T}(ab)$, there exist $U_1 \in \mathcal{T}(a)$ and $U_2 \in \mathcal{T}(b)$ such that $U_1U_2 \subset U$. Similarly, inverse being a homeomorphism (as $i \circ i = \mathrm{Id}$) can be written as: $\mathcal{T}(a)^{-1} = \mathcal{T}(a^{-1})$. Here, by a little abuse of notation, for any subset $V \subset G$, we write $V^{-1} = \{a^{-1} : a \in V\}$. Thus,

$$\mathcal{T}(a)^{-1} = \{V^{-1} : V \in \mathcal{T}(a)\}.$$

The following properties of a topological group follow directly from definitions:

(1) For $g \in G$, let $L_g : G \to G$ be the multiplication on the left by g. *Then L_g is a homeomorphism.* Note that it is enough to show that L_g is continuous, since $L_g \circ L_{g^{-1}} = \mathrm{Id}_G$. That is, for $h \in G$ and $U \in \mathcal{T}(gh)$, there exists $V \in \mathcal{T}(h)$ such that $gV \subset U$. This is clear, since we have $U_1 \in \mathcal{T}(g)$ and $U_2 \in \mathcal{T}(h)$, such that $U_1U_2 \subset U$, we can take $V = U_2$.

(2) Similarly, right multiplication by $g \in G$ is a homeomorphism.

(3) Let $H \subset G$ be a subgroup. *If H is open, then H is closed.* This is because, we have the following disjoint union:

$$G = \bigsqcup_{g \in G/H} gH, \qquad H - \text{cosets in } G.$$

Thus, H is the complement of $\displaystyle\bigcup_{g \notin H} gH$ which is open, being a union of open sets.

(4) Again let $H \subset G$ be a subgroup. *Then $\overline{H}$ is a subgroup.* To see this, let $g, h \in \overline{H}$. We need to show that $gh \in \overline{H}$. That is, for every $U \in \mathcal{T}(gh)$, we have $U \cap H \neq \emptyset$. By definition, we have $U_1 \in \mathcal{T}(g)$ and $U_2 \in \mathcal{T}(h)$ such that $U_1U_2 \subset U$. Since $g, h \in \overline{H}$, we have $U_1 \cap H \neq \emptyset$ and $U_2 \cap H \neq \emptyset$. Since H is a group, we get $U_1U_2 \cap H \neq \emptyset$. Same argument can be used to show that $\overline{H}$ is closed under inverse.

(32.1) Topology of the Galois group.– Let L/K be an algebraic, Galois extension. We simplify the notation from the previous lecture.

Hypothesis. Let $(I, \leq)$ be a *right directed* partially ordered set. Assume that we have a direct system of *finite, Galois* subextensions: $K \subset L_i \subset L$ (L_i/K is finite and Galois); $L_i \subset L_j$ for every $i \leq j$, such that

$$\varinjlim_{i \in I} L_i \xrightarrow{\sim} L.$$

Note that such direct systems always exist - for instance, we can take I to be the indexing set labelling *all finite, Galois* subextensions, ordered by inclusion.

Since each L_i/K is a normal extension, we get restriction homomorphisms:

$$\rho_{ij} : \mathsf{G}\left(L_j/K\right) \to \mathsf{G}\left(L_i/K\right), \ \forall i \leq j,$$

which form an inverse system of (finite) groups. We also have:

$$\phi_i : \mathsf{G}\left(L/K\right) \to \mathsf{G}\left(L_i/K\right), \ \forall i \in I,$$

such that each ϕ_i is surjective, and for $i \leq j$, we have: $\rho_{ij}\phi_j = \phi_i$. Thus there is a group homomorphism $\phi : \mathsf{G}\left(L/K\right) \to \varprojlim_{i \in I} \mathsf{G}\left(L_i/K\right)$, uniquely determined by: $\pi_i \circ \phi = \phi_i$, for every $i \in I$. Here $\pi_i : \varprojlim_{j \in I} \mathsf{G}\left(L_j/K\right) \to \mathsf{G}\left(L_i/K\right)$ is the canonical homomorphism.

Proposition. $\phi : \mathsf{G}\left(L/K\right) \to \varprojlim_{i \in I} \mathsf{G}\left(L_i/K\right)$ *is an isomorphism of groups.*

Proof. It is clear that $\mathrm{Ker}(\phi)$ is trivial, since if $\phi_i(g) = \mathrm{Id}_{L_i}$ for each $i \in I$, and $L \cong \varinjlim_{i \in I} L_i$, then $g = \mathrm{Id}_L$. Conversely, if $(g_i)_{i \in I} \in \varprojlim_{i \in I} \mathsf{G}\left(L_i/K\right)$, then we can define $g \in \mathsf{G}\left(L/K\right)$ via $g|_{L_i} = g_i$. This definition is unambiguous since $\rho_{ij}(g_j) = g_i$. □

Definition. The Galois group $\mathsf{G}\left(L/K\right)$ is assumed to be equipped with the coarsest topology which makes each of the restriction homomorphisms $\phi_i : \mathsf{G}\left(L/K\right) \to \mathsf{G}\left(L_i/K\right)$ continuous, when $\mathsf{G}\left(L_i/K\right)$ is given the discrete topology.

(32.2) Explicit description of open sets.– We retain the set up of the previous paragraph. Let us use the notation:

$$G = \mathsf{G}\left(L/K\right), \qquad G_i = \mathsf{G}\left(L_i/K\right).$$

Then, we have the following inverse system of finite, discrete groups:

$$\mathcal{G} = \left(\{G_i\}_{i \in I}; \{\rho_{ij} : G_j \to G_i\}_{i \leq j}\right).$$

Also, for each $i \in I$ we have $\phi_i : G \to G_i$ which induces an isomorphism $\phi : G \xrightarrow{\sim} \varprojlim_{i \in I} G_i$. Thus G can be viewed as a subgroup of $\widetilde{G} = \prod_{i \in I} G_i$. The topology on G and $\widetilde{G}$ is the coarsest one that makes the following homomorphisms continuous.

$$\begin{tikzcd}
G \arrow[rr, hook] \arrow[dr, "\phi_i"'] & & \widetilde{G} \arrow[dl, "\pi_i"] \\
& G_i &
\end{tikzcd}$$

It makes it clear that the topology of $G \subset \widetilde{G}$ is that of a subspace.

Recall that, by our definition, the following are open sets containing the identity element $e \in \widetilde{G}$:

$$\text{For each } i \in I, \ \widetilde{U}_i(e) := \mathrm{Ker}(\pi_i) = \{\sigma \in \widetilde{G} : \pi_i(\sigma) = e_i\} \subset \widetilde{G}.$$

This is because $\{e_i\} \subset G_i$ is open.

Note that we are assuming $(I, \leq)$ to be *right directed.* So, for finite intersections, for every $i_1, \ldots, i_n \in I$, choose $i \in I$ such that $i_j \leq i$ for each j. Then we have:

$$\widetilde{U}_i(e) \subset \bigcap_{j=1}^{n} \widetilde{U}_j(e).$$

Thus, $\widetilde{\mathcal{B}}(e) := \{\widetilde{U}_i(e) : i \in I\} \subset 2^{\widetilde{G}}$ is a fundamental system of neighbourhoods of the identity element.

It is also clear that $G \subset \widetilde{G}$ is closed. This is because,

$$G = \bigcap_{i \leq j} F_{ij}, \quad \text{where } F_{ij} = \{\sigma \in \widetilde{G} : \rho_{ij}(\pi_j(\sigma)) = \pi_i(\sigma)\} \subset \widetilde{G}.$$

Each F_{ij} is closed, hence so must be G.

Let $U_i(e) = G \cap \widetilde{U}_i$, for each $i \in I$. Note that $U_i(e) = \mathrm{Ker}(\phi_i)$ is a normal subgroup, which is open and hence closed. It is naturally identified with $U_i(e) = \mathsf{G}(L/L_i) \subset \mathsf{G}(L/K)$.

For any $\sigma \in G$, we get a fundamental system of neighbourhoods $\mathcal{B}(\sigma) = \sigma\mathcal{B}(e) = \mathcal{B}(e)\sigma$. If $\sigma \neq \tau$ are two elements of G, then there exists $i \in I$ such that $\phi_i(\sigma) \neq \phi_i(\tau)$. Thus, we obtain

$$(\sigma U_i(e)) \cap (\tau U_i(e)) = \emptyset.$$

We have shown that *any two points can be separated by sets which are both open and closed.* That is, G is totally disconnected (two distinct points belong to different connected components).

(32.3) Proof of the fundamental theorem.– Recall the set maps

$$\mathcal{F} : \{\text{Subgroups of } \mathsf{G}(L/K)\} \to \{\text{Subextensions of } L/K\},$$

$$\mathcal{G} : \{\text{Subextensions of } L/K\} \to \{\text{Subgroups of } \mathsf{G}(L/K)\}$$

given by $\mathcal{F}(H) = L^H$ and $\mathcal{G}(E) = \mathsf{G}(L/E)$.

1. For each subextension $K \subset E \subset L$, $\mathsf{G}(L/E) \subset \mathsf{G}(L/K)$ is a closed subgroup.

Let $H = \mathsf{G}(L/E)$ and $G = \mathsf{G}(L/K)$. To show that $H = \overline{H}$, it is enough to prove that every $\sigma \in \overline{H}$ is an element of H. For σ to be in the closure of H, it is necessary and sufficient that for each $i \in I$, $\sigma U_i(e) \cap H \neq \emptyset$. For $z \in E$, choose $i \in I$ so that $z \in L_i$. Let $h = \sigma g \in \sigma U_i(e) \cap H$ (recall $U_i(e)$ is normal). Then $z = h(z) = \sigma(g(z)) = \sigma(z)$. Thus $\sigma|_E = \mathrm{Id}_E$ proving that $\sigma \in H$ as claimed.

2. For any subgroup H of $\mathsf{G}(L/K)$, we have $L^H = L^{\overline{H}}$.

(It is the same argument as for the proof of **1** above). Since $H \subset \overline{H}$, it is clear that $L^{\overline{H}} \subset L^H$. Conversely, let $z \in L$ be fixed by every element of H, and let $\sigma \in \overline{H}$. We want to show that $\sigma(z) = z$. Choose $i \in I$ such that $z \in L_i$. As $\sigma U_i(e) \cap H \neq \emptyset$, we can write $\sigma = gh$, where $g \in U_i(e)$ and $h \in H$. Now $h(z) = z = g(z)$, which implies $\sigma(z) = z$.

3. Finally, if $H \subset \mathsf{G}(L/K)$ is a subgroup, and $E = L^H$, then $\mathsf{G}(L/E) = \overline{H}$.

We already know that L/E is a Galois extension, and $\mathsf{G}(L/E)$ contains H and is closed. Therefore, $\overline{H} \subset \mathsf{G}(L/E)$. Now assume that $\sigma \in \mathsf{G}(L/E)$. In order to show that $\sigma \in \overline{H}$, we need to prove that for every $i \in I$, $\sigma U_i(e) \cap H \neq \emptyset$. That is, there exists $h \in H$ such that $\phi_i(h) = \phi_i(\sigma)$.

Now let $N_i = L_i E \subset L$ be the smallest field containing both L_i and E. Note that N_i/E is a finite Galois extension: (i) if L_i is the splitting extension of a set $P_i \subset K[x]$, then $L_i E$ is the splitting extension of the same set of polynomials, viewed as elements of $E[x]$, (ii) $[N_i : E] \leq [L_i : K] < \infty$.

Let $p_i : \mathsf{G}(L/E) \to \mathsf{G}(N_i/E)$ be the restriction map. Note that $N_i^{p_i(H)} = E$ since $L^H = E$. From the theorem for the finite case (Theorem 31.1), we conclude that $p_i(H) = \mathsf{G}(N_i/E)$. So, there exists $h \in H$ such that $p_i(h) = p_i(\sigma)$. Since ϕ_i restricted to $\mathsf{G}(L/E)$ can be written as the composition:

$$\mathsf{G}(L/E) \xrightarrow{p_i} \mathsf{G}(N_i/E) \hookrightarrow \mathsf{G}(N_i/K) \to \mathsf{G}(L_i/K),$$

we conclude that $\phi_i(g) = \phi_i(\sigma)$, as required.