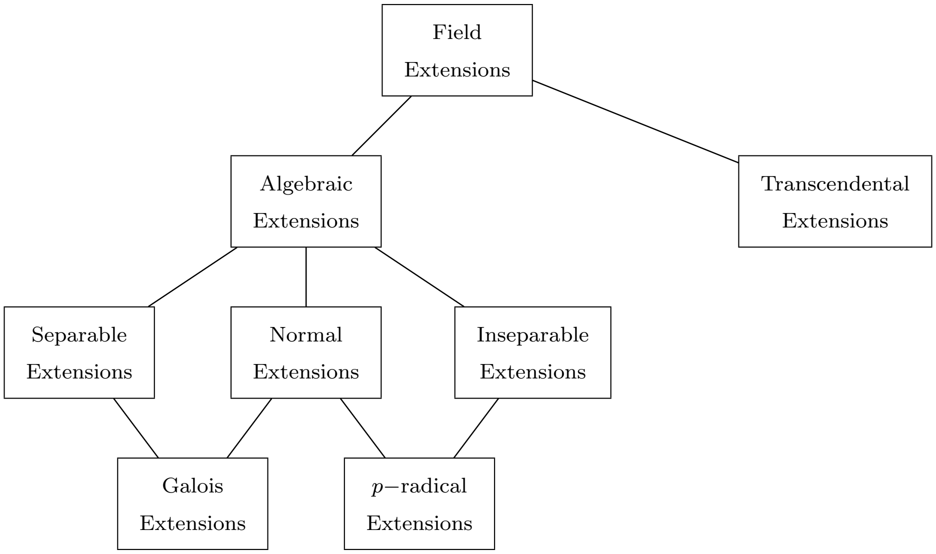
LECTURE 31

(31.0) Summary of the results so far.– Let K be a field and L/K be a field extension.

- L/K is either algebraic or transcendental.
- If L/K is algebraic, then it is called (i) *normal* if it is a splitting extension of some set $P \subset K[x]$ (ii) *separable* if for every $\alpha \in L$, the minimal polynomial $\mathsf{m}_\alpha(x)$ is separable (i.e, has distinct roots in its splitting extension).
- In most fields (called perfect fields, which include fields of characteristic zero, finite fields and algebraically closed fields) every irreducible polynomial is separable. In some cases (for imperfect fields) this doesn't have to be the case.
- We say L/K is a Galois extension if $L^{\mathsf{G}(L/K)} = K$. Last time we proved that an algberaic extension is Galois if and only if it is the splitting extension of a set of separable polynomials.



Note that for perfect fields, inseparable extensions do not exist. So, if K is perfect, then every algebraic extension is separable. It is Galois if and only if it is a splitting extension.

In this lecture, without further mention, we will only focus on algebraic extensions.

Recall the following two important results from the last lecture.

- For a field L and a group G, every distinct set of group homomorphisms $\mathrm{Hom}_{gp}(G, L^\times)$ is linear independent over L (Dedekind's independence of characters).

- For a field L and a finite subgroup $\Gamma \subset \mathrm{Aut}_{field}(L)$, the extension L/L^Γ is finite of degree $|\Gamma|$ (Artin's theorem).

It is perhaps worth recalling Theorem 27.0 here:

Theorem. *Let K be a field and let $P \subset K[x]$.*

(1) *There exists a splitting extension L/K of P.*
(2) *Let L'/K' be another field extension, and assume that there is a homomorphism $f : K \to K'$. Further assume that for every $p(x) \in P$, $f(p(x))$ splits into a product of linear factors in $L'[x]$. Then there exists a homomorphism $\widetilde{f} : L \to L'$ such that $\widetilde{f}|_K = f$.*

In particular splitting extensions are unique up to (non-unique in general) isomorphism. We will denote this field extension by $\mathcal{E}(P, K)$.

As an application of this theorem, we have the following:

Corollary. *Let $f(x) \in K[x]$ be a monic, irreducible polynomial. Let L/K be a Galois extension such that $f(x) = (x - r_1) \dots (x - r_n)$ in $L[x]$. Here, $n = \deg f$ and r_i's are necessarily distinct. For any $g \in \mathsf{G}(L/K)$, there exists a permutation $\sigma \in \mathfrak{S}_n$ such that $g(r_i) = r_{\sigma(i)}$. This gives a group homomorphism:*

$$\varphi_f : \mathsf{G}(L/K) \to \mathfrak{S}_{\deg(f)}.$$

Let E/K be the subextension $K(r_1, \dots, r_n) \subset L$. Then we have a restriction homomorphism:

$$\rho_{E,L} : \mathsf{G}(L/K) \to \mathsf{G}(E/K),$$

which commutes with φ_f:

$$\begin{tikzcd}
\mathsf{G}(L/K) \arrow[rr, "\rho_{E,L}"] \arrow[dr, "\varphi_f"'] & & \mathsf{G}(E/K) \arrow[dl, "\varphi_f"] \\
& \mathfrak{S}_n &
\end{tikzcd}$$

Moreover, the action of $\mathsf{G}(E/K)$ on $\{1, \dots, n\}$ is transitive[1].

(31.1) Fundamental theorem of Galois Theory (finite case).– Let L/K be a finite Galois extension. Let $\Gamma = \mathsf{G}(L/K)$. Note that $|\Gamma| = [L : K]$.

Given a subgroup $G \subset \Gamma$, let $\mathcal{F}(G) = L^G \subset L$. This is a subextension of L/K. Conversely, given a subextension $K \subset E \subset L$, let $\mathcal{G}(E) \subset \Gamma$ be the subgroup $\mathsf{G}(L/E) \subset \mathsf{G}(L/K)$.

Theorem. *$\mathcal{F}$ and $\mathcal{G}$ are mutually inverse of each other.*

$$\begin{tikzcd}
\boxed{\begin{array}{c}\textit{Subextensions}\\ \textit{of } L/K\end{array}} \arrow[r, bend left=10, "\mathcal{F}"] & \boxed{\begin{array}{c}\textit{Subgroups}\\ \textit{of } \mathsf{G}(L/K)\end{array}} \arrow[l, bend left=10, "\mathcal{G}"]
\end{tikzcd}$$

[1] A group G acting on a set X is said to act transitively if for every $x, y \in X$, there exists $g \in G$ such that $g(x) = y$.

Moreover, a subextension $K \subset E \subset L$ is normal if and only if $\mathcal{G}(E) = \mathsf{G}(L/E)$ is a normal subgroup of $\mathsf{G}(L/K)$.

Proof. Note that $\mathcal{G}(\mathcal{F}(G)) = G$, since $\mathcal{F}(G) = L^G$ and by Artin's theorem L/L^G is a Galois extension of degree $|G|$. Thus the canonical map $G \to \mathsf{G}\left(L/L^G\right)$ is an isomorphism.

Conversely, if $K \subset E \subset L$ is a subextension, then L/E is also a Galois extension. This is because L is the splitting extension (over K) of a separable set of polynomials $P \subset K[x]$. Thus $L^{\mathsf{G}(L/E)} = E$ by definition. Hence, $\mathcal{F}(\mathcal{G}(E)) = E$ as claimed.

Let us assume that E/K is a normal extension. As explained in Theorem 30.1, $\mathsf{G}(L/E)$ is identified with the kernel of the restriction homomorphism $\rho_f : \mathsf{G}(L/K) \to \mathsf{G}(E/K)$, and hence is a normal subgroup.

Now assume that $\mathsf{G}(L/E) \subset \mathsf{G}(L/K)$ is a normal subgroup. We want to prove that E is a normal extension, that is for every $\alpha \in E$, $\mathsf{m}_\alpha(x) \in K[x]$ splits into linear factors in $E[x]$. Let $\{r_1, \ldots, r_n\}$ be the set of roots of $\mathsf{m}_\alpha(x)$ in $L[x]$, with $r_1 = \alpha$. For each $2 \leq i \leq n$, there exist $g_i \in \mathsf{G}(L/K)$ such that $g_i(\alpha) = r_i$. Thus, it is enough to show that for every $\sigma \in \mathsf{G}(L/K)$, $\sigma(E) = E$. Note that the following relation holds, for any subextension $L/E/K$ and $\sigma \in \mathsf{G}(L/K)$:

$$\sigma \circ \mathsf{G}(L/E) \circ \sigma^{-1} = \mathsf{G}(L/\sigma(E))$$

The two sides are equal, for every σ, if and only if $\mathsf{G}(L/E)$ is normal. Using the bijection established above, we get $E = \sigma(E)$ as we wanted. □

(31.2) Infinite Galois group.– Theorem 31.1, as stated above, is false when $\Gamma = \mathsf{G}(L/K)$ is infinite. A standard example for this is given as follows. Consider the following extension of $\mathbb{Q}$:

$$K = \mathbb{Q}(\sqrt{p} : p \in \mathbb{Z}_{\geq 2} \text{ prime}) \subset \mathbb{R}.$$

It is easy to see that:

$$G = \mathsf{G}(K/\mathbb{Q}) = \prod_{\substack{p \in \mathbb{Z}_{\geq 2} \\ \text{prime}}} \mathbb{Z}/2\mathbb{Z},$$

upon identifying $\mathbb{Z}/2\mathbb{Z} \cong \mathsf{G}\left(\mathbb{Q}(\sqrt{p})/\mathbb{Q}\right)$, via $\sigma(\sqrt{p}) = -\sqrt{p}$. Consider the subgroup:

$$H = \bigoplus_{\substack{p \in \mathbb{Z}_{\geq 2} \\ \text{prime}}} \mathbb{Z}/2\mathbb{Z} \subsetneq G.$$

It is clear that $K^H = \mathbb{Q} = K^G$, even though $H \neq G$.

To make the statement precise, we need to consider a *canonically defined topology* on $\mathsf{G}(L/K)$, relative to which the bijection of Theorem 31.1 is restricted to *closed* subgroups and subextensions.

(31.3) Topology on $\mathsf{G}(L/K)$.– Assume that L/K is a Galois extension. Let us choose a set

$$I \subset \{f(x) \in K[x] \text{ monic, irreducible polynomial}\},$$

such that $L \cong \mathcal{E}(I, K)$. We define a partially ordered set $\mathcal{I}$:

$$\mathcal{I} = \{J \subset I : |J| < \infty\}, \qquad \text{partially ordered by inclusion.}$$

For each $J \in \mathcal{I}$, we denote by $L_J = \mathcal{E}(J, K)$ the splitting extension of $J \subset I$. Recall that we have an isomorphism of fields:

$$L \cong \varinjlim_{J \in \mathcal{I}} L_J.$$

At the level of Galois groups, we obtain an inverse system of groups, labelled by $\mathcal{I}$. Recall that, by Theorem 30.1, we have restriction maps:

$$G_J := \mathsf{G}\left(L_J/K\right), \ \forall J_1 \subset J_2, \text{ we have } \rho_{J_1,J_2} : G_{J_2} \to G_{J_1}$$

such that $\rho_{J,J} = \mathrm{Id}_{G_J}$ and for every $J_1 \subset J_2 \subset J_3$, we have $\rho_{J_1,J_2} \circ \rho_{J_2,J_3} = \rho_{J_1,J_3}$. Additionally, each of the restriction homomorphism is surjective.

We also have (surjective) group homomorphisms $\phi_J : G = \mathsf{G}\left(L/K\right) \to G_J$ which commute with restrictions, and hence define:

$$\phi : G \to \varprojlim_{J \in \mathcal{I}} G_J, \quad \text{such that } \pi_J \circ \phi = \phi_J \text{ for every } J \in \mathcal{I},$$

where $\pi_J : \varprojlim_{J' \in \mathcal{I}} G_{J'} \to G_J$ is the canonical group homomorphism.

Proposition. *$\phi : G \to \varprojlim_{J \in \mathcal{I}} G_J$ is an isomorphism of groups.*

The statement of this proposition is a direct consequence of $L \cong \varinjlim_{J \in \mathcal{I}} L_J$, and is left as an exercise.

Definition. The *Krull topology* on $\mathsf{G}\left(L/K\right)$ is the coarsest topology such that for every finite subset $J \subset I$, $\phi_J : \mathsf{G}\left(L/K\right) \to \mathsf{G}\left(L_J/K\right)$ is continuous, where $\mathsf{G}\left(L_J/K\right)$ is given a discrete topology.

Remark. In general, for topological spaces $\{X_a\}_{a \in A}$, and set maps from a fixed set Y, $\{f_a : Y \to X_a\}_{a \in A}$, there exists a unique coarsest topology on Y, making f_a continuous, for every $a \in A$. For instance, when A is a finite set, and $Y = \prod_{a \in A} X_a$, we get the product topology:

$$\text{Open sets in } \prod_{a \in A} X_a = \left\{ \prod_{a \in A} U_a \text{ where } U_a \subset X_a \text{ is open} \right\}.$$

In general, for each $a \in A$ and $U_a \subset X_a$ open, the following set:

$$\mathcal{U}_a = f_a^{-1}(U_a) \subset Y$$

has to be open. So we take the smallest topology generated by these sets. Since finite intersections of open sets are open, the following sets are necessarily open as well:

$$\mathcal{U}_B = \bigcap_{b \in B} \mathcal{U}_b, \text{ where } B \subset A \text{ is a finite set.}$$

The topology on Y can be described more explicitly as follows. A subset $Z \subset Y$ is open if and only if for every $z \in Z$, there exists a finite $B \subset A$ such that $z \in \mathcal{U}_B \subset Z$. Similarly, closure of a set $W \subset Y$ is given by:

$$z \in \overline{W} \iff \forall B \subset A \text{ finite, such that } z \in \mathcal{U}_B, \text{ we have } W \cap \mathcal{U}_B \neq \emptyset.$$

(31.4) Fundamental theorem of Galois theory (general case).– Let L/K be a Galois extension. Recall that assignments $\mathcal{F}$ and $\mathcal{G}$ from §31.1. For a subextension $K \subset E \subset L$, and a subgroup $G \subset \mathsf{G}(L/K)$:

$$\mathcal{G}(E) = \mathsf{G}(L/E), \qquad \mathcal{F}(G) = L^G.$$

We have the following analogue of Theorem 31.1.

Theorem. *$\mathcal{F}$ and $\mathcal{G}$ are mutually inverse of each other:*

$$\begin{tikzcd}
\boxed{\begin{array}{c}\textit{Subextensions}\\ \textit{of } L/K\end{array}} \arrow[r, bend left, "\mathcal{F}"] & \boxed{\begin{array}{c}\textit{Closed subgroups}\\ \textit{of } \mathsf{G}(L/K)\end{array}} \arrow[l, bend left, "\mathcal{G}"]
\end{tikzcd}$$

Moreover, for any subgroup $H \subset \mathsf{G}(L/K)$, we have $L^H = L^{\overline{H}}$, where $\overline{H}$ is the closure of H.

We will prove this theorem next time.

(31.5) Example.– Let us revisit the example from §31.2. We defined

$$K = \mathbb{Q}(\sqrt{p} : p \in \mathbb{Z}_{\geq 2} \text{ prime}).$$

Then, we have:

$$G = \mathsf{G}(K/\mathbb{Q}) = \prod_{\substack{p \in \mathbb{Z}_{\geq 2} \\ \text{prime}}} \mathbb{Z}/2\mathbb{Z}.$$

To describe topology on G, we consider finite subsets of $\mathcal{P} = \{p \in \mathbb{Z}_{\geq 2} : p \text{ is prime}\}$. For $P \subset \mathcal{P}$, a finite set, set $G_P = \prod_{p \in P} \mathbb{Z}/2\mathbb{Z}$ finite discrete group. Given any element $\sigma_P \in G_P$, define

$$U(\sigma_P) = \{\sigma_P\} \times \prod_{p \notin P} \mathbb{Z}/2\mathbb{Z} \subset G.$$

Let $e_P \in G_P$ be the neutral element. Then we have:

(1) $\{U(e_P) : P \subset \mathcal{P} \text{ is finite}\}$ is the fundamental system of neighbourhoods of $e \in G$. Each $U(e_P)$ is a (normal) subgroup of G and is both open and closed.

By *fundamental system of neighbourhoods*, we mean that any subset $X \subset G$ containing e is open if and only if there exists a finite $P \subset \mathcal{P}$ such that $U(e_P) \subset X$. Note that

$$U(e_P) = \mathrm{Ker}\,(\pi_P : G \to G_P)$$

hence is a normal subgroup. Moreover, $\{e_P\} \subset G_P$ is open, which is the reason why $U(e_P) \subset G$ is open. It is also closed since $G \to G_P$ is surjective and G_P has discrete topology.

(2) For every $\sigma \in G$, we have:

$$\sigma U(e_P) = U(e_P)\sigma = U(\pi_P(\sigma)), \quad \text{for every finite subset } P \subset \mathcal{P},$$

which form a fundamental system of neighbourhoods of σ.

(3) Recall that $H = \bigoplus_{p \in \mathcal{P}} \mathbb{Z}/2\mathbb{Z}$. We claim that $\overline{H} = G$. To see this let $\sigma \in G$ be arbitrary and let $P \subset \mathcal{P}$ be a finite set. Then $\tau \in H \cap U(\pi_P(\sigma))$, where the coordinates of τ are given by:

$$\tau_p = \begin{cases} \sigma_p & \text{if } p \in P, \\ e_p & \text{otherwise.} \end{cases}$$

Hence $\sigma \in \overline{H}$ (see Remark 31.3, page 4 above). Thus, $\overline{H} = G$ so they have the same subfield of invariants consistent with Theorem 31.4 above.