0.0.1 Preparation for Galois' Solvability Theorem

Def: G is called solvable if there exists a sequence of subgroups $G = G_0 \triangleright G_1 \triangleright \ldots \triangleright G_m = \{1\}$. s.t. G_i/G_{i+1} is abelian.

Theorem 0.1 *Let $N \triangleright G$. G is solvable $\iff$ $N, G/N$ is solvable.*

Proof: $\Longrightarrow$

$G/N \checkmark$

$N_i = G_i \cap N$.

$N = N_0 \supset N_1 \supset \ldots \supset N_m = 1$.

$N_{i+1} \triangleleft N_i$? Yes, because $N \cap G_{i+1} \triangleleft G_i$

N_i/N_{i+1} Abelian? $N \cap G_i \hookrightarrow G_i \twoheadrightarrow G_i/G_{i+1}$

$f : N \cap G_i \to G_i/G_{i+1}$. composition of above.

Kernel of f? $n \to nG_{i+1}$, $n \in \ker f \iff n \in G_{i+1} \cap N$.

$N_i/N_{i+1} = N \cap G_i/N \cap G_{i+1} \cong \mathrm{im} f < G_i/G_{i+1}$.

$\Longleftarrow$

Construct a series for G.

$N = N_0 \triangleright N_1 \triangleright \ldots \triangleright N_m = \{1\}$

$G/N = H_0 \triangleright H_1 \triangleright \ldots \triangleright H_m = \{1\}$

$$\begin{aligned} \{1\} = N_m \triangleleft \ldots \triangleleft N_0 = N - G_n < G_{n-1} \ldots G < G \\ \{1\} \triangleleft H_n \ldots \triangleleft H_0 = G/N \end{aligned}$$

$\phi : G \to G/N$

$\vee \quad \vee$

$\phi^{-1}(H_1) \to H_i$

So $G_{i+1} \triangleleft G_i$ because $H_{i+1} \triangleleft H_i$.

$G_i/G_{i+1} \cong G_i/N/G_{i+1}/N = H_i/H_{i+1}$

By 3rd homo. them.

$\therefore G_i/G_{i+1}$ abelian.

■

0.0.2 Cyclic Extensions

.

Theorem 0.2 *(Dedekind) Let F be a field, and G a group. Then every finite set $\{\chi_1, \ldots, \chi_m\}$ of homomorphisms*

$G_i : G \to F^{\times}$ is linearly independent over F

Remark: X set, F field.

$Func(X, F) = \{f : X \to F\}$ is a vector space over f.

$(f_1 + f_2)(x) = f_1(x) + f_2(x)$.

$(\alpha \cdot f)(x) = \alpha f(x)$.

$\chi_1, \ldots, \chi_m \in Func(G, F)$ are linearly independent.

Theorem 0.3 $\sum_i a_i \chi_i = 0 \implies a_1 = \cdots = a_m = 0$.

Proof: $m = 1\checkmark$.

$a\chi = 0 \implies a = 0$.

Assume $m - 1$.

$a_1\chi_1 + a_m\chi_m = 0$. $\star$

$a_i \in F$ need to show all zero.

$\chi_1 \neq \chi_2 \implies \exists g \in G$

$\chi_1(g) \neq \chi_2(g)$

$\forall x \in G : a_1\chi_1 + \cdots + a_m\chi_m = 0$

also for $gx : a_1\chi_1(gx) + \cdots + a_m\chi_m(gx) = 0$

(*) $a_1\chi_1(x)\chi_1(g) + \cdots + a_m\chi_m(x)\chi_m(g) = 0$.

(**) $a_1\chi_1(x)\chi_1(g) + \cdots + a_m\chi_1(x)\chi_m(g) = 0$. By mult above with $\chi_1(x)$

$(*) - (**) = \sum_{j=2}^{m} a'_j \chi_j(x) = 0$. $\forall x \in G$.

$a'_j = a_j(\chi_j(g) - \chi_1(g))$.

By induction, $a'_j = 0$.

In particular, $a'_2 = 0$.

$0 = a'_2 = a_2(x_2(g) - x_1(g)) \neq 0$

$\implies a_2 = 0$

So in $\star$, there are $m - 1$ terms, by induction $a_1 = a_3 = \cdots = a_m = 0$

$\blacksquare$

0.0.3 Back to Cyclic Extensions

$F = F_0 \subset F_1 \subset \dots F_m$.

$F_{i+1} = F_i(\sqrt[n_i]{a_i})$

Theorem 0.4 *Let F be a field containing a primitive n^{th} root of 1. Let $E = F[\alpha], \alpha^n = a \in F$ and no smaller power of $\alpha \in F$. Then E/F is Galois ext with $Gal(E/F) \cong \mathbb{Z}/n\mathbb{Z}$.*

Conversely, if E/F is cyclic Galois Ext of degree n, then $\exists \alpha \in E$ s.t. $E = F[\alpha], \alpha^n \in F$.

Proof: ($\implies$)

$\alpha, \zeta\alpha, \zeta^2\alpha, \dots, \zeta^n\alpha$ are the roots of $x^n - a \in F[x]$.

$Gal(F[\alpha]/F) \to \mathbb{Z}/n\mathbb{Z}$

$\sigma \to i\sigma$, $\sigma(\alpha) = \zeta^{i\sigma}\alpha$

$\impliedby$

enough to find $\alpha \in E^\times$ s.t. $\sigma(\alpha) = \zeta^{-1}\alpha$

$\blacksquare$