Abstract Algebra
: Lecture 21

Leo

2024.12.15

Theorem 1. *(Galois Thm) Let* $\operatorname{Char} F = 0$. *Then* $f(x) \in F[x]$ *is soluble by radicals if and only if* $\mathrm{Gal}(f)$ *is a soluble group.*

Example 2. *Let* $f(x) = x^5 - 8x + 2 \in \mathbb{Q}[x]$, *you can check that* f *is irreducible.* $\mathrm{Gal}(f) \simeq S_5$, S_5 *is not a soluble group, so* f *is not soluble by radicals.*

Lemma 3. *Let* G *be transitive permutation group on* Ω. *Assume that* G *contains a transposition. And* $|\Omega| = p$ *is a prime. Then* $G \simeq \mathrm{Sym}(\Omega) \simeq S_p$.

证明. Since G is trnasitive on Ω, by Orbit-Stabilizer Theorem, $|\Omega| \mid |G|$, so $p \mid G$, and by Lagrange theorem, G contains an element of order p, i.e. $g = (12\dots p)$ without loss of generality. Let $(ij) \in G$, then $< (12\dots p), (ij) >= S_p$. i.e. $G \geqslant S_p$. Since $G \leqslant \mathrm{Sym}(\Omega) \simeq S_p$. Therefore, $G \simeq S_p$. □

Proposition 4. *Let* $f(x) \in F[x]$ *with* $F = \mathbb{Q}$. *Assume that* $f(x)$ *is irreducible of degree* p *where* p *is a prime. Assume further that* $f(x)$ *has exactly two complex roots. Then* $\mathrm{Gal}(f) \simeq S_p$.

证明. The complex conjugation is a transposition of $\mathrm{Gal}(f)$ acting on $\Omega = \{\text{roots of } f(x)\}$. And since $f(x)$ is irreducible, $\mathrm{Gal}(f)$ acts on Ω transitively (chack it by yourself !). By the lemma, $\mathrm{Gal}(f) \simeq S_p$ □

Example 5. $f(x) = x^p - a \in \mathbb{Q}[x]$. *Where* $\sqrt[p]{a} \notin \mathbb{Q}$. $Gal(f) \simeq Z_p : Z_{p-1} = \mathrm{Hol}(Z_P) \simeq \mathrm{Aut}(D_{2p})$ *(when* $p \neq 2$*).*
Let $\omega = e^{\frac{2\pi i}{p}}$, *root of* $x^{p-1} + \cdots + x + 1$, $\alpha = a^{\frac{1}{p}} \notin \mathbb{Q}$. *Then* $\alpha, \alpha\omega, \dots, \alpha\omega^{p-1}$ *are the* p *roots of* $x^p - a$.
Let $E = \mathbb{Q}(\alpha, \alpha\omega, \dots, \alpha\omega^{p-1})$. *Then* E *is a splitting field of* $x^p - a$. *Thus a normal extension of* $\mathbb{Q}$.
Let $L = \mathbb{Q}(\omega) \subset E$, *then* $\mathbb{Q} \subset L \subset E$. *And* L *is a normal extension of* $\mathbb{Q}$, *since it is a splitting field of* $x^p - 1$ *over* $\mathbb{Q}$.
Thus $\mathrm{Gal}(E/L) \lhd \mathrm{Gal}(E/\mathbb{Q})$, *and* $\mathrm{Gal}(E/\mathbb{Q})/\mathrm{Gal}(E/L) \simeq \mathrm{Gal}(L/\mathbb{Q})$.
Consider $\mathrm{Gal}(E/L)$ *and* $\mathrm{Gal}(L/\mathbb{Q})$.
Notice that if f *is irreducible,* $\mathrm{Gal}(f)$ *acts transitively on the roots of* f. *Furthermore, since* $f(x) = x^p - a$ *consider that* $\mathrm{Gal}(f)$, *you can check the action of* $\mathrm{Gal}(f)$ *has no non-trivial blocks, i.e. this action is primitive.*

Now $\mathrm{Gal}(L/\mathbb{Q})$ *is a splitting field of irreducible polynomial* $x^{p-1}+\ldots x+1$*, so* $\mathrm{Gal}(L/\mathbb{Q})$ *is transitive on the* $p-1$ *roots:* $\omega, \omega^2, \ldots, \omega^{p-1}$.
The group $\mathrm{Gal}(E/L)$*, where* $E = L(\alpha)$*, contains an element* $\rho : \alpha \to \alpha\omega \to \cdots \to \alpha\omega^{p-1}$*. And* $< \rho > \simeq Z_p$.
Claim: $\mathrm{Gal}(E/\mathbb{Q}) = \mathrm{Gal}(E/L) \cdot \mathrm{Gal}(L/\mathbb{Q}) = Z_p : Z_{p-1}$.

证明. 1. Claim $\mathrm{Gal}(E/L) =< \rho >$.
Otherwise, $\exists \tau \in \mathrm{Gal}(E/L)$ s.t. $\alpha^\tau = \alpha$, $(\alpha\omega^i)^\tau = \alpha\omega^j$ with $i \neq j$. $\tau : \omega^i \mapsto \omega^j$. But $\tau \in \mathrm{Gal}(E/L)$ i.e. τ fixes L pointwise, contradiction.
2. Claim $\mathrm{Gal}(L/\mathbb{Q}) =< \sigma >$, where $\sigma : \omega \mapsto \omega^r$ with r is a primitive root of p. i.e. $\mathrm{Ord}_p(r) = p-1$.
Now $Z_{p-1} \simeq < \sigma > \leqslant \mathrm{Gal}(L/\mathbb{Q}) = G$. As $< \sigma >$ is a transitive subgroup of G we can write $G =< \sigma > G_\omega$. And it's obvious $G_\omega = e$.
Therefore, $\mathrm{Gal}(E/\mathbb{Q}) = \mathrm{Gal}(E/L) \cdot \mathrm{Gal}(L/\mathbb{Q}) =< \rho > \cdot < \sigma > \simeq Z_p \cdot Z_{p-1}$. Since $|Z_p|$ and $|Z_{p-1}|$ coprime, this is a splitting extension of groups. so $\mathrm{Gal}(E/\mathbb{Q}) = \mathrm{Gal}(E/L) \cdot \mathrm{Gal}(L/\mathbb{Q}) =< \rho > \cdot < \sigma > \simeq Z_p : Z_{p-1}$.
Actually, this splitting extension is faithful. i.e. this group is exact $\mathrm{AGL}(1,p)$.
Recall, if $G = N : H$, where N is abelian and regular. Let $C_G(N) = \{g \in G \mid [g,N] = 1\}$. Then $N \leqslant C$. And a trnasitive abelian group is regular (prove it !). So $N = C$.
By this fact, this extension $Z_p : Z_{p-1}$ is faithful. □

Exercise 6. *Prove that* $f = x^5 - 6x + 3$*, or* $x^5 - 4x + 2$ *are not soluble by radicals, i.e.* $\mathrm{Gal}(f)$ *is insoluble.*