Lecture #5 (09/10/2024)

Plan for today: - proof of Galois correspondence
- solvable extensions
- Galois/Abel criterion for solvability

- A rough plan for what is coming next (in some order)

examples and the inverse Galois problem

cyclotomic and cyclic extensions

Kummer theory

Artin-Schreier theory

Normal basis theorem

Galois cohomology and Brauer groups

Infinite Galois extensions

proof (Galois correspondence, Part I)

Let L/K be a (finite) Galois extension.

We want to show that

$$F \longmapsto \mathrm{Gal}(L/F) \qquad \star$$

is a bijection with inverse

$$H \longmapsto L^H$$

Thus, given $K \subset F \subset L$ we need to show that $F = L^{\mathrm{Gal}(L/F)}$ (i.e. $\star$ is injective) and that given $H \leq G$, $\mathrm{Gal}(L/L^H) = H$ (i.e. $\star$ is surjective).

The 2nd part follows from Artin's lemma.

For the first, we first observe that

1) L/K separable (resp. normal) $\Rightarrow$ L/F separable (resp. normal); hence, Galois.

2) L/F Galois $\Rightarrow$ $|\mathrm{Gal}(L/F)| = [L:F]$

3) We always have the inclusion

$$F \subset L^{\mathrm{Gal}(L/F)}.$$

Now, Artin's lemma tells us that

$$[L : L^{\mathrm{Gal}(L/F)}] = |\mathrm{Gal}(L/F)| \overset{2)}{=} [L : F]$$

and since $[L:F] = [L : L^{\mathrm{Gal}(L/F)}]\,[L^{\mathrm{Gal}(L/F)} : F]$

it must be the case that $[L^{\mathrm{Gal}(L/F)} : F] = 1$

Thus, we have equality in 3). ∎

Rmks It is clear that

$$K \subset F \subset F' \subset L \Rightarrow \mathrm{Gal}(L/F') \subset \mathrm{Gal}(L/F)$$

and that

$$H' \subset H \Rightarrow L^{H} \subset L^{H'}$$

Proof (Galois correspondence, Part II)

Fix $H \trianglelefteq G$ and let $F = L^H \Rightarrow \mathrm{Gal}(L/F) = H$.

We want to show that F/K is Galois and $\mathrm{Gal}(F/K) \simeq G/H$.

always separable

Assume that F/K is not normal, then

$\exists\, \sigma \in \mathrm{Hom}_K(F, L)$ s.t. $\sigma(F) \neq F$

Let $\tilde{\sigma} \in \mathrm{Aut}_K(L) = G$ be an extension of σ,

then $\tilde{\sigma} H \tilde{\sigma}^{-1} = \mathrm{Gal}(L/\sigma(F)) \neq H$

Thus, $H \not\trianglelefteq G$. $= \mathrm{Gal}(L/F)$

<u>Claim</u> We have a short exact sequence

$$1 \to \underset{\mathrm{Gal}(L/F)}{H} \to \mathrm{Gal}(L/K) \xrightarrow{\mathrm{res}|_F} \mathrm{Gal}(F/K) \to 1$$

That is, $\mathrm{res}|_F$ is surjective and has kernel isomorphic to $\mathrm{Gal}(L/F) = H$.

$K \subset F \subset L \subset \bar{L} = \bar{K}$

- $\text{res}|_F$ is surjective because any $\tau \in \text{Gal}(F/K)$ extends to some $\tilde{\tau} \in \text{Hom}_K(L, \bar{L})$ with $\tilde{\tau} \in \text{Aut}_K(L)$.
  ↖ because L/K is normal

- note that $G = \text{Gal}(L/K)$

$$\ker \text{res}|_F = \{\sigma \in \text{Gal}(L/K);\ \sigma|_F = \text{id}_F\}$$

Thus, $H = \text{Gal}(L/F) \subset \ker \text{res}|_F$

Moreover,

$$|\ker \text{res}|_F| = |G| / \text{Gal}(F/K) = \frac{[L:K]}{[F:K]} = [L:F]$$

$$= H = \text{Gal}(L/F)$$

∎

Corollary If L/K is Galois with abelian Galois grp, then all its subextensions are Galois.

Solvable extensions

Definition A field extension L/K is called radical if there exists a radical tower

$$K_0 = K \subset K_1 \subset \cdots \subset K_n = L$$

such that $K_{j+1} = K_j(\alpha_j)$ where α_j is a root of $x^{m_j} - \beta_j$ for some $m_j \geq 2$ and $\beta_j \in K_j^{\times}$.

Definition A field extension is called solvable if it is contained in a radical one.

Definition Let K be a field and $f \in K[x] \setminus K$. Then the equation $f(x) = 0$ is solvable by radicals iff $SF_K(f)/K$ is solvable.

Theorem (Abel + Galois) Let K be a field of char $= 0$ and let L/K be a (finite) Galois extension. TFAE:

1. L/K is solvable
2. $G = \mathrm{Gal}(L/K)$ is solvable

$\left(1 \overset{\text{Abel}}{\Longrightarrow} 2 \,,\; 2 \overset{\text{Galois}}{\Longrightarrow} 1 \right)$

Rmk.: Assume $L = SF_K(f)$, $f \in K[x]$ and $\underset{\| }{\text{char}\, K} > 0$.

Then $f = 0$ may be solvable by radicals even when f is not separable. And $x^p - x - \alpha = 0$ may not be solvable by radicals even though such polynomial is separable and the corresponding Galois group is abelian (hence solvable) $(\simeq C_p)$

proof

(1) $\Rightarrow$ (2)

If L/K is solvable, $\exists$ M/K radical with $L \subset M$

Write

$$K = K_0 \subset K_1 \subset \cdots \subset K_n = M$$

as in the definition of a radical extension.

Let $m = \prod_{j=1}^{n} m_j$ and consider $F_m = M(\mu_m)$.

Then F_m/K is still radical. Let $F = F_m^{Gal}$.

Then F/K is Galois and radical.

In fact, we can write (we will prove this later)

$$K = F_0 \subset F_1 = K(\mu_m) \subset F_2 \subset \cdots \subset F_\ell = F$$

cyclotomic — all cyclic

where $F_{i+1} = F_i(\gamma_i)$ with $\gamma_i^m \in F_i$

Thus, each F_{i+1}/F_i has abelian Galois group. By Galois correspondence, this gives us that $Gal(F/K)$ is solvable.

But then

$$\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(F/K)/\mathrm{Gal}(F/L)$$

is also solvable.

∎

RmKs

- Recall that $K \subset L \subset F$

  and F/K Galois $\Rightarrow$ F/L Galois

- Fm/K is finite $\Rightarrow$ algebraic
  + char $K = 0$
  $\Rightarrow$ Fm/K is separable

- every quotient of a solvable grp. is solvable

proof (2) $\Rightarrow$ (1)

We will need

Lemma 1 Consider $K \subset F \subset L$ (finite).

L/K is solvable $\Leftrightarrow$ L/F and F/K are solvable

Lemma 2 Let L/K be (finite) Galois

with $\mathrm{Gal}(L/K)$ cyclic and char $K=0$.

Then L/K is solvable.

Assume that $G = \mathrm{Gal}(L/K)$ is solvable.

Write

$$\{e_G\} = G_n \triangleleft G_{n-1} \triangleleft \cdots \triangleleft G_1 \triangleleft G_0 = G$$

with G_j / G_{j+1} cyclic (check that you can do this)

Let $K_j = L^{G_j}$ for $j = 0, \ldots, n$.

Then each L/L_j is Galois with Galois grp. G_j and each L_{j+1}/L_j is Galois with cyclic Galois grp.

Now, consider $K \subset L_1 \subset L$.

By Lemma 2 this is solvable. Using induction on n and Lemma 1 we can deduce that L/K is solvable.

∎

Corollary Let $f \in K[x]$ be a general polynomial of degree $d \geq 5$. Assume that $\operatorname{char} K = 0$. Then f is not solvable by radicals.

(The extension $SF_K(f)/K$ is not solvable as it has Galois group $\simeq S_d$)

Finally, we prove:

Proposition Let L/K be a finite extension. If L/K is radical, then L^{Gal}/K is also radical.

proof Write $L = K(\alpha_1, \dots, \alpha_n)$. Then

$$L^{Gal} = K\left(\text{all roots of the } \min_K \alpha_i\right)$$

$$= K\left(\sigma(\alpha_1), \dots, \sigma(\alpha_n) \ \forall \sigma \in G\right)$$

where $G = Gal\left(L^{Gal}/K\right)$.

Up to relabelling,

Since L/K is radical, we have

$$K = K_0 \subset K_1 = K(\alpha_1) \subset K_2 = K(\alpha_1, \alpha_2) \subset \cdots \subset K_n = L = K(\alpha_1, \cdots, \alpha_n)$$

where $\alpha_j^{m_j} \in K_{j-1}$ for some $m_j \geq 2$.

Now, let $F_i := K\left(\sigma(\alpha_j) \,;\, 1 \leq j \leq i \,,\, \sigma \in G\right)$

Then

$$K = F_0 \subset F_1 \subset \cdots \subset F_n = L^{Gal}$$

And to show that this is a radical tower, by induction on n, it suffices to show that F_1/F_0 is radical.

We have $G = \{1, g_1, g_2, g_3, \cdots\}$ and

$$K = F_0 \subset K(\alpha_1) \subset K\left(\alpha_1, g_1(\alpha_1)\right) \subset K\left(\alpha_1, g_1(\alpha_1), g_2(\alpha_1)\right) \subset \cdots \subset F_1$$