

Lecture # 5 (09/10/2025)

- 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

$$F \mapsto \text{Gal}(L/F) \quad \star$$

is a bijection with inverse

$$H \mapsto L^H$$

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

3) We always have the inclusion
 $F \subset L^{\text{Gal}(L/F)}$.

Now, Artin's lemma tells us that

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

↑
2)

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

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

Thus, we have equality in 3).

□

Rmks It is clear that

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

and that

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

proof (Galois correspondence, Part II)

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

We want to show that F/K is Galois and

$\text{Gal}(F/K) \cong G/H$. ← always separable

Assume that F/K is not normal, then

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

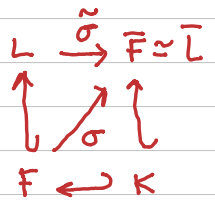
Let $\tilde{\sigma} \in \text{Aut}_K(L) = G$ be an extension of σ ,

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

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

Note: L/F is finite, so it is algebraic. Thus, \exists a K -algebra morphism $L \rightarrow \bar{F}$.

So, we can fix an embedding and then $\text{Hom}_K(F, L) \subset \text{Hom}_K(F, \bar{F})$



Claim We have a short exact sequence

$$1 \rightarrow \overset{\text{Gal}(L/F)}{\text{Gal}(L/F)} \rightarrow \text{Gal}(L/K) \xrightarrow{\text{res}_F} \text{Gal}(F/K) \rightarrow 1$$

That is, res_F is surjective and has kernel isomorphic to $\text{Gal}(L/F) = H$.

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

- $\text{res}|_F$ 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
$$\text{Ker res}|_F = \left\{ \sigma \in \text{Gal} \overset{G}{\parallel} (L/K); \sigma|_F = \text{id}_F \right\}$$

Thus,
$$\text{Gal} \underset{H}{\parallel} (L/F) \subset \text{Ker res}|_F$$

Moreover,

$$\begin{aligned} |\text{Ker res}|_F| &= |G| / |\text{Gal}(F/K)| = \frac{[L:K]}{[F:K]} = [L:F] \\ &= H = \text{Gal}(L/F) \end{aligned}$$

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

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

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 $\beta_j \in K_j^x$.

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 $\text{char} = 0$ and let L/K be a (finite) Galois extension. TFAE:

① L/K is solvable

② $G = \text{Gal}(L/K)$ is solvable

(① $\xrightarrow{\text{Abel}}$ ② , ② $\xrightarrow{\text{Galois}}$ ①)

Rmk.: Assume $L = \text{SF}_K(f)$, $f \in K[x]$ and $\text{char} K \overset{p}{\parallel} 0$.

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

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

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 $F = F_m^{\text{Gal}}$.

Then F/K is Galois and radical.

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

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

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 $\text{Gal}(F/K)$ is solvable.

But then

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

is also solvable.



Rmks

• Recall that $K < L < F$

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

• F_m/K is finite \Rightarrow algebraic } $\Rightarrow F_m/K$ is separable
+ $\text{char } K = 0$

• every quotient of a solvable grp. is solvable

proof $\textcircled{2} \Rightarrow \textcircled{1}$

We will need

Lemma 1 Consider $K < F < L$ (finite).

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

Lemma 2 Let L/K be (finite) Galois

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

Then L/K is solvable.

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

Write

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

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

$$\text{Let } L_j = L^{G_j} \text{ for } j = 0, \dots, n.$$

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 $\text{char } K = 0$. Then f is not solvable by radicals.

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

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

$$L^{\text{Gal}} = K(\text{all roots of the min}_K \alpha_i)$$

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

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

Up to relabelling,

Since L/K is radical, we have

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

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

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

Then

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

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 $G = \{1, g_1, g_2, g_3, \dots\}$ and

$$\begin{aligned} K = F_0 \subset K(\alpha_1) \subset K(\alpha_1, g_1(\alpha_1)) \subset K(\alpha_1, g_1(\alpha_1), g_2(\alpha_1)) \\ \subset \dots \subset F_1 \end{aligned}$$

