May 24

Plan for this week

Today: Lecture

Wed: Discussion

Fri: Galois's criterion

FUND THM OF GALOIS THEORY

Let $K \subset L$ be a Galois field ext.

① There is a bijective correspondence

$$\left\{ \begin{array}{c} \text{int. field ext} \\ K \subset E \subset L \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{subgroups} \\ H \subset \mathrm{Gal}(L/K) \end{array} \right\}$$

$$E \longmapsto \mathrm{Gal}(L/E)$$

$$L^H \longleftarrow\!\shortmid \; H$$

② $|L:E| = \#\mathrm{Gal}(L/E)$ and $|E:K| = |\mathrm{Gal}(L/K) : \mathrm{Gal}(L/E)|$

In particular, $|L:K| = \#\mathrm{Gal}(L/K)$

③ $K \subset E$ normal $\Longleftrightarrow$ $\mathrm{Gal}(L/E) \trianglelefteq \mathrm{Gal}(L/K)$ normal subgp.

In this case $\mathrm{Gal}(E/K) = \mathrm{Gal}(L/K) / \mathrm{Gal}(L/E)$

Ex: $f \in \mathbb{Q}[x]$ $\quad \mathbb{Q} \to L$ splitting field

$\searrow L_1 \to L_2 \to L_2$

Galois's Criterion

Let K be a field of char $=0$.
Let $f(x) \in K[x]$ with splitting field $K \subset L$.

Then

$f(x)$ is solvable using radical
$\iff$ $Gal(L/K)$ solvable.

Finite group theory

Defn A finite group G is solvable if $\exists$ chain

$$\{1\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_{n-1} \trianglelefteq H_n = G$$

where

- $H_i \trianglelefteq H_{i+1}$ normal
- $H_{i+1}/H_i \cong \mathbb{Z}/p_i$ for a prime i.

HW(9.4) G is solvable $\iff$ if $\exists$ chain

$$\{1\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_{n-1} \trianglelefteq H_n = G$$

where

- $H_i \trianglelefteq H_{i+1}$ normal
- H_{i+1}/H_i abelian.

Reason! $\exists$ classification of finite abelian groups: any finite abelian group $G \cong \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_k$

Why do we care?

(1) Galois theory: normal subgps correspond to normal extension . . . .

(2) We care about abelian groups — we know a lot more about them.

- Solvable groups are not that different from abelian.
- Many properties can be shown for solvable by induction & using abelian case

HW If $H \trianglelefteq G$ normal

G solvable $\Leftrightarrow$ H solvable & G/H solvable

Observation: If $\mathcal{P}$ is a property of finite groups s.t. for $H \trianglelefteq G$

G has $\mathcal{P}$ $\Leftrightarrow$ H has $\mathcal{P}$ & G/H has $\mathcal{P}$

If $\mathbb{Z}/p$ has $\mathcal{P}$ $\forall$ prime p, then any solvable group has $\mathcal{P}$.

Defn We say $K \subset L$ is a radical field extension if $\exists$

$$K = K_0 \subset K_1 \subset \cdots \subset K_{n-1} \subset K_n = L$$

such that

- $K_i = K_{i-1}(\alpha_i)$ where $a_i = \alpha_i^{n_i} \in K_{i-1}$

i.e. $K_i = K_{i-1}(\sqrt[n_i]{a_i})$

Defn We say $f(x) \in K[x]$ is solvable by radicals if the splitting field L is contained in a radical field ext $K \subset L'$.

(So $K \subset \underset{\text{splitting field}}{L} \subset \underset{\text{radical}}{L'}$)

L contains all the roots of f. Since $L \subset L'$, the roots can be expressed by using iterated radicals.

Galois's Criterion

Let K be a field of char $=0$.
Let $f(x) \in K[x]$ with splitting field $K \subset L$.

Then

$f(x)$ is solvable using radical
$\iff$ $Gal(L/K)$ solvable.

Which groups are solvable?

solvable	not solvable
$\mathbb{Z}/2$	S_5
$\mathbb{Z}/p$ for p prime	S_6
abelian group	S_7
S_3	$\vdots$
S_4	

Ex $\langle (12) \rangle \subset S_3$ not normal

$\langle (123) \rangle \trianglelefteq S_3 \to \mathbb{Z}/2$
$\langle (123) \rangle \cong \mathbb{Z}/3$

Ex S_4 ✓ $\{1,2,3,4\}$

- Can view $S_3 \subset S_4$ not normal!
  $(123) \in S_3$
  $(14)(123)(14) = (1)(234)$
- Look at $A_4 \subset S_4$
  - It is normal. $(|S_4 : A_4| = 2)$
  - Reduces to solvability of A_4
-
  $\langle (1234) \rangle$

Let's search for
$H \trianglelefteq S_4$ w/ $S_4/H \cong S_3$
$\implies |H| = 4$
$H = \langle 1, (12)(34), (13)(24), (14)(23) \rangle$