Fundamental Theorem of Galois

Let K be a finite normal extension of F with Galois group $G(K/F)$

1) There is an inclusion-reversing bijection

$$\lambda : \begin{Bmatrix} \text{intermediate} \\ \text{fields } F \leq K \end{Bmatrix} \longrightarrow \begin{Bmatrix} \text{subgroups of} \\ G(K/F) \end{Bmatrix}, \quad \lambda(E) = G(K/E)$$

$$[K:E] = |G(K/E)| \text{ and } [E:F] = (G(K/F) : G(K/E))$$

2) Let $F \leq E \leq K$ then E is a normal extension of F if and only if $G(K/E)$ is a normal subgroup of $G(K/F)$.

When $G(K/E) \leq G(K/F)$ is normal $G(E/F) \cong G(K/F)/G(K/E)$.

normal $\Leftrightarrow$ normal E is normal over F $\Longleftrightarrow$ E is a splitting field over F. (E is separable over F since $E \leq K$ & sep. over F)

Thm 50.3

$\Longleftrightarrow$ $\forall\ \sigma \in G(K/F)$ and $\alpha \in E$ $\sigma(\alpha) \in E$

$E = K_{G(K/E)}$. So $\sigma(\alpha) \in E \Longleftrightarrow \forall\ \tau \in G(K/E)$

$\tau\sigma(\alpha) = \sigma(\alpha) \Longleftrightarrow \sigma^{-1}\tau\sigma(\alpha) = \alpha$ $\forall\ \alpha \in E$
$\forall\ \tau \in G(K/E)$
$\sigma \in G(K/F)$

$\Longleftrightarrow$ $\sigma^{-1}\tau\sigma \in G(K/E)$ $\forall\ \tau \in G(K/E)$ and $\forall\ \sigma \in G(K/F)$.

This is precisely the definition of $G(K/E)$ being a normal subgroup of $G(K/F)$.

Suppose E is a normal extension of F. Then the map $\varphi : G(K/F) \to G(E/F)$ is onto

$$\sigma \longmapsto \sigma|_E$$

(By iso exth theorem + since K is normal)

(Since E is normal $\sigma|_E$ is an automorphism ie $\sigma|_E(E) = E$.)

The $\ker \varphi := \{\sigma : K \to K \mid \underset{\sigma|_E}{\overset{\shortparallel}{\varphi(\sigma)}} = id : E \to E\} \leq G(K/F)$

$$= G(K/E)$$

By surjectivity of φ $G(E/F) \cong G(K/F)/G(K/E)$.

$\square$

First an example: Cyclotomic Extensions (Section 55)

Def 55.1 The splitting field of $x^n - 1$ over F is the n^{th} cyclotomic extension of F.

- The zeros of $x^n - 1$ over $\mathbb{Q}$ are $1, \zeta, \zeta^2, \dots, \zeta^{n-1}$ where $\zeta = e^{2\pi i/n} \in \mathbb{C}$ (or any primitive n^{th} root of unity $\Rightarrow e^{2\pi i m/n}$) for $\gcd(m,n) = 1$.

- The splitting field of $x^n - 1$ is $K = F(\zeta)$.
- For $F = \mathbb{Q}$ irreducible polynomial of ζ over $\mathbb{Q}$ is

$$\Phi_n(x) = \prod_{\zeta_i \text{ primitive } n^{th} \text{ root of unity}} (x - \zeta_i)$$

$\deg \Phi_n = \varphi(n)$ Euler function $= \#\{k \mid 1 \le k \le n, \gcd(k,n) = 1\}$

- $\tau \in G(K/\mathbb{Q})$ then $\tau(\xi)$ is a primitive n^{th} root of unity $\Rightarrow$ $\tau(\xi) = \xi^{m}$ where $\gcd(n,m)=1$. So if $\tau' \in G(K/\mathbb{Q})$

$$\tau\tau'(\xi) = \tau(\xi^{m'}) = \xi^{m'm} = \tau'(\xi^{m}) = \tau'\tau(\xi).$$

$$G(K/\mathbb{Q}) \cong G_n = \text{"}\mathbb{Z}_n^{\times}\text{"} = \left\{ k \;\middle|\; \begin{array}{l} 1 \le k \le n \\ \gcd(k,n)=1 \end{array} \right\}$$ with operation multiplication

$\Rightarrow$ $G(K/\mathbb{Q})$ is abelian

Solving by radicals

Can zeros of $f(x) \in \mathbb{Q}[x]$ be expressed in terms of radicals?

- $\deg f(x) = 2$ quadratic formula Brahmagupta ~600 AD $r = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$
- $\deg f(x) = 3$ Cardano's formula 1545
- $\deg f(x) = 4$ Ferrari 1540
- $\deg f(x) = 5$ Insolvable by radicals in general! We will give a different proof.

Abel – Ruffini Theorem. 1799/1824.

$\Longrightarrow$ Galois

Insolvability by radicals of the quintic

Def 56.1 An extension K of F is an <u>extension by radicals</u> if $\exists$ $\alpha_1, \dots, \alpha_r \in K$ and $n_1, \dots, n_r > 0$ s.t. $K = F(\alpha_1, \dots, \alpha_r)$ and $\alpha_1^{n_1} \in F$ and $\alpha_i^{n_i} \in F(\alpha_1, \dots, \alpha_{i-1})$ for $1 < i \leq r$.

$\boxed{\Rightarrow \alpha_i \text{ is the } n_i^{th}\text{-root of some elt of } F(\alpha_1, \dots, \alpha_{i-1}) \mid \alpha_i \text{ is a zero of } x^{n_i} - \alpha_i^{n_i}}$

A polynomial $f(x) \in F[x]$ is <u>solvable by radicals</u> if its splitting field is contained in an extension by F by radicals ($F \leq \underset{\text{splitting field}}{E} \leq K \leq \overline{F}$)

K $\leftarrow$ extn by radicals

Eg. • $x^n - a \in \mathbb{Q}[x]$ is solvable by radicals

• $ax^2 + bx + c \in \mathbb{Q}[x]$ is solvable by radicals.

• cubics and quartics over $\mathbb{Q}$ are solvable by radicals.

Thm (Galois) Let char $F = 0$. Then $f(x) \in F[x]$ is solvable by radicals over F if and only if the splitting field E over F has solvable Galois group.

Recall A group G is solvable if a composition series $0 = H_0 \triangleleft H_1 \triangleleft \dots \triangleleft H_{n-1} \triangleleft H_n = G$ is such that H_{i+1}/H_i is abelian $\forall\ 0 \leq i \leq n-1$.

A composition series is a sequence of subgroups as above with H_i normal in H_{i+1} and H_{i+1}/H_i is simple for $\forall\ 0 \leq i \leq n-1$.

Example • If G is abelian G is solvable.

• S_5 is not solvable: $0 < A_5 < S_5$. A_5 is simple not abelian!

NOTE There's no subgp $A_5 < H < S_5$ since $(S_5 : A_5) = 2 = (S_5 : H)(H : A_5)$ so either $(S_5 : H)$ or $(H : A_5) = 1$ $\Rightarrow S_5 = H$ or $H = A_5$.

• S_n, A_n not solvable for $n \geq 5$.

• If $0 = N_0 \triangleleft N_1 \triangleleft N_2 \ldots \triangleleft N_n = G$ is a subnormal series with N_{i+1}/N_i solvable then G is solvable. Exercise 56.6.

& $N_{i+1} \triangleleft N_i$

not necessary that N_{i+1}/N_i is simple.

• Quotients of solvable groups are solvable Exercise 35.29

Lemma 56.3 Let char $F = 0$, $a \in F$, and K be the splitting field of $x^n - a$ over F. Then $G(K/F)$ is solvable.

Proof Case 1 Suppose F contains a primitive n^{th} root of unity ξ. Then zeros of $x^n - a$ are $\beta, \xi\beta, \dots, \xi^{n-1}\beta$ and $K = F(\beta)$. $G(K/F) \cong G_n$ ← multiplicative group mod n. and is abelian hence solvable.

Case 2 $\xi \notin F$. Then let $F' = F(\xi)$ ← cyclotomic ext'n so $G(F'/F)$ is abelian. Also K/F' is the extension from case 1 $\Rightarrow$ $G(K/F')$ is abelian.

$$\begin{array}{c} K = F'(\beta) \\ | \\ F' = F(\xi) \\ | \\ F \end{array}$$

F' is splitting field of $X^n - 1$ over $F \Rightarrow F'$ is a normal ext'n of $F \Rightarrow G(K/F')$ is a normal subgroup of $G(K/F)$. Consider $0 \lhd G(K/F') \lhd G(K/F)$

Then $G(K/F)/G(K/F') \cong G(F/F') \Rightarrow$ abelian

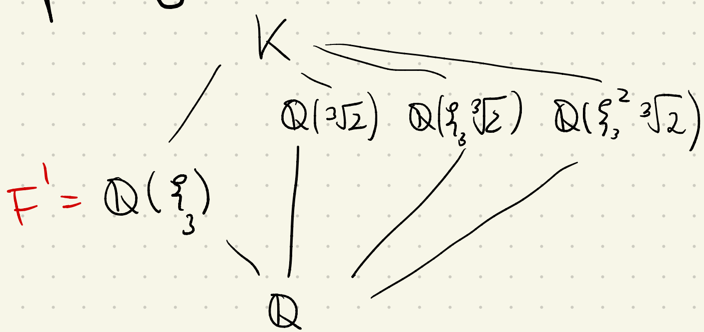
$\Rightarrow G(K/F)/G(K/F')$ solvable.

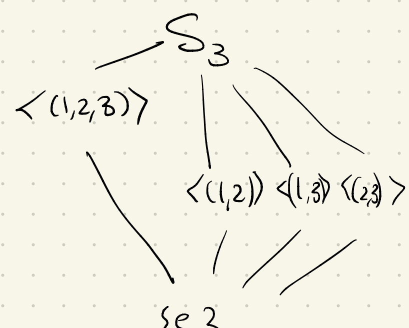
$G(K/F')/0$ abelian $\Rightarrow$ solvable.

$\Longrightarrow G(K/F)$ is solvable by Exercise 56.6 $\square$

Example

K is splitting field of $X^3 - 2$ over $\mathbb{Q}$.





Thm 56.4 Let F be a field of char 0 and suppose $F \leq E \leq K \leq \overline{F}$ where E is a normal extension and K is an extension by radicals. Then $G(E/F)$ is a solvable group.

Proof Let $K = F(\alpha_1, \dots, \alpha_r)$ and form L_{i+1} as the splitting field of

$x^{n_{i+1}} - \alpha_{i+1}$ over L_i. Let $L = L_r$. By Lemma 56.3 $G(L_1/F)$ is solvable. Suppose L_i is solvable then

$0 \triangleleft G(L_i/F) \triangleleft G(L_{i+1}/F)$ with $G(L_{i+1}/F) / G(L_i/F) \cong G(L_{i+1}/L_i)$

$\Rightarrow G(L_{i+1}/F)$ is solvable $\Rightarrow$

Hence $G(L/F)$ is solvable. Now,

$$G(L/F) / G(L/E) \cong G(F/E)$$

and quotients of solvable groups are solvable

Exercise 35.29 $\square$.

Corollary A quintic polynomial of degree 5 over a field F with $\operatorname{char} F = 0$ is not solvable by radicals if $G(K/F) \cong S_5$ where K is the splitting field.

Such polynomials exist!

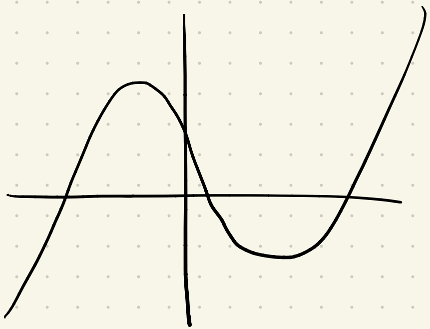
$/\mathbb{R}$ see text book using symmetric polynomials and transcendental #'s over $\mathbb{Q}$.

$y_1, \dots, y_5 \in \mathbb{R}$ transcendental

$$f(x) = \prod (x - y_i) \in \mathbb{Q}(s_1, \dots, s_5)[x]$$

Then claim $G(K/F) \cong S_5$.

Over $\mathbb{Q}$. Suppose $f(x) \in \mathbb{Q}[x]$ is a irreducible degree 5 polynomial with 3 real zeros and 2 complex conjugated zeros. i.e. $f(x) = 2x^5 - 5x^4 + 5$.



(show this using calculus and Eisenstein's criterion $p = 5$.)

Claim $G(K/F) \cong S_5$ where K is the splitting field.

Exercise 56.8. $G(K/F) \leq S_5 \Leftarrow$ group of permutations of 5 zeros of $f(x)$.

To show = enough to show $G(K/F)$ contains a transposition and a 5-cycle.

A transposition is $(1,2)$.

An example of a 5-cycle is $(1,2,3,4,5)$