

Galois Theory.

Last time, we proved that

$$K/\mathbb{Q} \text{ is Galois} \iff |\text{Aut}(K/\mathbb{Q})| = [K:\mathbb{Q}]$$

We are taking the definition for Galois to be normal extension (meaning ^{irreducible} $f(x)$ has a root in $K \iff f$ splits in K).

Rmk 1. If you read textbook, then. def for Galois is

$$|\text{Aut}(K/\mathbb{Q})| = [K:\mathbb{Q}].$$

Rmk 2. If you read other books. "separable" is included in the definition. (we simply drop this "separable" since all field extensions we talk about, L/\mathbb{F} with char 0. or finite exts over \mathbb{F}_p or \mathbb{F}_q).

We want to show now that.

$\iff K$ being a splitting field of a certain polynomial $f(x) \in \mathbb{Q}[x]$.

practical useful criteria to prove some field is Galois.

Thm. K/\mathbb{Q} is Galois $\iff K$ is the splitting field for some $f(x) \in \mathbb{Q}[x]$

Pf: " \implies " By primitive element thm. $K = \mathbb{Q}[\alpha]$ then. say $f(x)$ is the minimal degree poly in $\mathbb{Q}[x]$ s.t. $f(\alpha) = 0$.

Then since K/\mathbb{Q} is Galois, then all roots of

$f(x)$ is in K . so $f(x)$ splits in K .

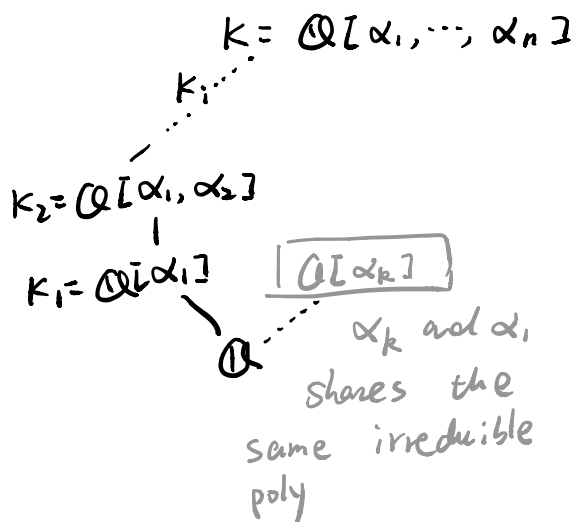
And since $K = \mathbb{Q}[\alpha]$ is the minimal subfield of \mathbb{C} that contains α . So K is the minimal field where $f(x)$ splits.

" \Leftarrow " Suppose K is the splitting field for $f(x) \in \mathbb{Q}[x]$.

say $f(x) = \prod_{i=1}^n (x - \alpha_i)$, we will prove that

$$|\text{Aut}(K/\mathbb{Q})| = [K:\mathbb{Q}] \text{ by construction.}$$

To construct a field automorphism $\sigma: K \rightarrow K$. we construct by induction over $K_i = \mathbb{Q}[\alpha_1, \dots, \alpha_i]$.



Firstly, we count the number of inclusions

$$\sigma_i: K_i = \mathbb{Q}[\alpha_i] \hookrightarrow K.$$

If $f_i(x)$ is the minimal deg polynomial s.t.

$$f_i(\alpha_i) = 0. \text{ then}$$

$$[K_i:\mathbb{Q}] = \deg(f_i)$$

$$= \# \text{ of roots of } f_i$$

$f_i | f$ so f_i also splits in K . i.e. all the roots of f_i are in K .

eg. $\mathbb{Q}[\sqrt[3]{2}] \subseteq \mathbb{Q}[\sqrt[3]{2}, \zeta_3]$

$$\begin{array}{c} | 2 \\ \mathbb{Q}[\sqrt[3]{2}, \zeta_3] \\ | 3 \\ \mathbb{Q} \end{array}$$

So there are $\deg(f_1)$ many choices to define σ_1 .

$$\text{by } \sigma_1: \mathbb{Q}[\alpha, \beta] \xrightarrow{\sim} \mathbb{Q}[x] / \langle f_1(x) \rangle \xrightarrow{\sim} \mathbb{Q}[\alpha] \hookrightarrow K.$$

\uparrow

where α is arbitrary root of $f_1(x)$.

Now for the next step, we consider

$$\begin{array}{ccc} \sigma_2: \mathbb{Q}[\alpha_1, \alpha_2] & \hookrightarrow & K \\ | & & | \\ \sigma_1: \mathbb{Q}[\alpha_1] & \xrightarrow{\sim} & M_1 \\ | & & | \\ \mathbb{Q} & \xrightarrow{\quad} & \mathbb{Q} \end{array}$$

To define σ_2 , we take $f_2(x) \in K_1[x]$, s.t. $f_2(x)$ is the minimal deg polynomial s.t. $f_2(\alpha_2) = 0$.

$f_2(x) \mid f_1(x)$ so $f_2(x)$ splits in K .

$$\begin{aligned} [\mathbb{Q}[\alpha_1, \alpha_2]: \mathbb{Q}[\alpha_1]] &= \deg f_2(x) \\ &= \# \text{ of roots of } f_2(x) \end{aligned}$$

$\rightarrow = \#$ of extension of σ_1 to σ_2 .

Ex. Given $\mathbb{Q}[\alpha_1] \xrightarrow{\varphi} M_1$ and $f_2(x)$ irreducible $\in \mathbb{Q}[\alpha_1][x]$.
 denote $f_2'(x) = \varphi(f_2(x))$. then, there is an isomorphism between
 the field. $\mathbb{Q}[\alpha_1][x] / \langle f_2(x) \rangle \cong M_1[x] / \langle f_2'(x) \rangle$.

We have shown for each fixed σ_1 , there're $[K_2:K_1]$ extensions to σ_2 . So altogether, the $\#$ of $\sigma_2: K_2 \hookrightarrow K$

$$\text{is } [K_2:K_1] \cdot [K_1:\mathbb{Q}] = [K_2:\mathbb{Q}].$$

By induction, eventually, you will get.

$$\# \quad \sigma_n = [K_n:\mathbb{Q}] \text{ which implies } |\text{Aut}(K/\mathbb{Q})| = [K:\mathbb{Q}].$$

So K is Galois. □.

Application.

Def (Galois grp for a polynomial). Given $f(x) \in \mathbb{Q}[x]$,

$$\text{Gal}(f) := \text{Gal}(K_f/\mathbb{Q})$$

where K_f is the splitting field of $f(x)$ over \mathbb{Q} .

eg.

$$f(x) = x^2 - 2.$$

$$\text{Gal}(f) = C_2$$

$$\parallel$$

$$\text{Gal}(\mathbb{Q}[\sqrt{2}]/\mathbb{Q}) = \left\{ \sigma: \sqrt{2} \rightarrow \begin{cases} -\sqrt{2} \\ \sqrt{2} \end{cases} \right\}$$

$$f(x) = (x^2 - 2)(x^2 - 5)$$

$$\text{Gal}(f) = C_2 \times C_2.$$

$$= x^4 - 7x^2 + 10$$

$$\approx \left\{ \begin{array}{l} \sigma: \sqrt{2} \rightarrow \pm\sqrt{2} \\ \sqrt{5} \rightarrow \pm\sqrt{5} \end{array} \right\}$$

↙ 4 elements.

$$\text{and } \sigma^2 = \text{id}. \quad \forall \sigma \in \text{Gal}(f).$$

We say $f(x)$ is solvable with radicals if.

the roots of $f(x)$ can be written as $+$, $-$, \times , \div and taking successive radicals of numbers.

$$ax^2 + bx + c = 0 \quad x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

$f(x) = (x^2 - 2)(x^2 - 5)(x^2 - 3)$ you can still solve by radicals

But generically, if you write down a random $f(x) \in \mathbb{Q}[x]$ with degree $n \geq 5$, then $f(x)$ is not solvable with radicals.

Thm. If $f(x)$ is irreducible in $\mathbb{Q}[x]$, $\deg(f) = n$.

then

$$\text{Gal}(K_f/\mathbb{Q}) \subseteq S_n.$$

Pf. Factor $f(x) = \prod_{i=1}^n (x - \alpha_i)$ and $K_f = \mathbb{Q}[\alpha_1, \dots, \alpha_n]$.

$\sigma: K_f \rightarrow K_f$ induces a permutation of α_i 's.

and we define $\pi_\sigma \in S_n$. $\pi_\sigma(i) = j$ if $\sigma(\alpha_i) = \alpha_j$.

Since $K = \mathbb{Q}[\alpha_1, \dots, \alpha_n]$ so if $\sigma(\alpha_i) = \alpha_i$ for all i ,

then $\sigma = \text{id}$ automorphism. Therefore $\text{Gal}(K_f/\mathbb{Q}) \subseteq S_n$. \square

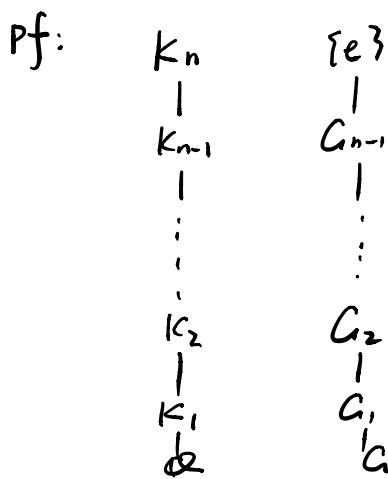
Rmk. (Interesting Fact: a random $f(x)$, then $\text{Gal}(f) = S_n$).

Thm. If $f(x)$ is solvable by radicals, then K_f/\mathbb{Q}

has a solvable Galois grp.

recall G is solvable iff $e \in G_1 \subseteq \dots \subseteq G_n = G$ with G_i/G_{i-1} is

abelian.



By fundamental thm for Galois theory, we have a correspondence between subfields & subgrps.

Suppose $f(x)$ is solvable with radicals.

say $\sqrt[k]{a}$ where $a \in \mathbb{Q}$ appear in the expression of roots.

then $K_2 = \mathbb{Q}[\zeta_k, \sqrt[k]{a}] \leftarrow$ splitting field of $f_2(x) = x^k - a \quad a \in \mathbb{Q}$

Galois ext over \mathbb{Q}

$K_1 = \mathbb{Q}[\zeta_k] \leftarrow$ splitting field of $f_1(x) = x^k - 1$

$\text{Gal}(\mathbb{Q}[\zeta_k] / \mathbb{Q})$ is abelian since

$\{ \sigma_i : \zeta_k \rightarrow \zeta_k^i \}$ \leftarrow notice not all integers work for

i. eg. $\zeta_4 \not\rightarrow \zeta_4^2$

$\begin{matrix} \zeta_4 \\ \text{"} \\ \zeta_4 \end{matrix} \quad \begin{matrix} \zeta_4^2 \\ \text{"} \\ \zeta_4 \end{matrix}$

$$\sigma_i \circ \sigma_j = \sigma_j \circ \sigma_i : \zeta_k \rightarrow \zeta_k^{ij}$$

$$\text{Gal}(\mathbb{Q}[\zeta_k, \sqrt[k]{a}] / \mathbb{Q}[\zeta_k]) = \{ \tau_i : \sqrt[k]{a} \rightarrow \sqrt[k]{a} \cdot \zeta_k^i \}$$

$$\tau_i \circ \tau_j = \tau_j \circ \tau_i : \sqrt[k]{a} \rightarrow \sqrt[k]{a} \cdot \zeta_k^{ij}$$

So we get $\text{Gal}(\mathbb{Q}[\zeta_k, \sqrt[k]{a}] / \mathbb{Q})$ is solvable.

Inductively taking all the roots in the expression. then
we can get a sequence of field

$$\mathbb{Q} \subseteq K_1 \subseteq K_2 \subseteq \dots \subseteq K_n$$

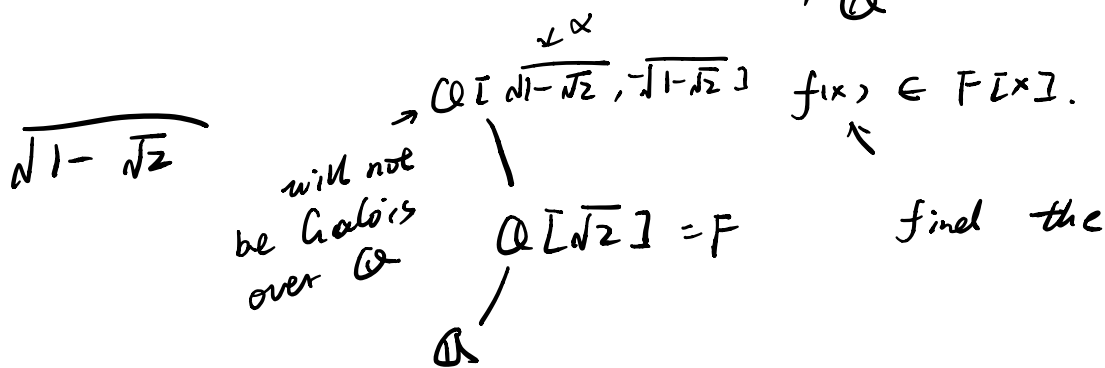
that all K_i are Galois by construction.

$$G \supseteq G_1 \supseteq G_2 \supseteq \dots \supseteq \{e\}$$

where G_i / G_{i+1} is abelian.

Notice that $f(x)$ splits in K_n via construction
so K_f is a quotient of K_n , and solvable grp

has solvable quotient, so. Gal(K_f/\mathbb{Q}) is solvable.



Remk. 1) Galois extension over Galois extension is not necessarily Galois;

2) abelian extension over abelian extension is always solvable (after taking the Galois closure over \mathbb{Q} . equivalently splitting field over \mathbb{Q}).

Coro. $f(x)$ with $\deg \geq 5$ is not always solvable with radicals. because S_n is not solvable when $n \geq 5$.

Start 1:30 pm — End 5:30 pm

$$\sigma H = H \sigma$$

$$\uparrow$$

$$(a \ b \ c)$$

$$\sigma \tau \sigma^{-1} = (\sigma(a) \ \sigma(b) \ \sigma(c))$$