Galois Theory.

Last time, we proved that

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

We are taking the definition for <u>Galois</u> to be normal extension (meaning irreducible $f(x)$ has a root in $K \Leftrightarrow f$ splits in K).

Rmk 1. If you read textbook, then. def. for Galois is
$|Aut(K/\mathbb{Q})| = [K:\mathbb{Q}]$.

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/F with char 0. or finite exts over $\mathbb{F}_p$ or $\mathbb{F}_q$).

We want to show now that.

$\Leftrightarrow$ 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 $\Leftrightarrow$ K is the splitting field for some $f(x) \in \mathbb{Q}[x]$

Pf: "$\Rightarrow$" By primitive elmt 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

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

To construct a field automorphism $\sigma: K \to K$.

we construct by induction over $K_i = \mathbb{Q}[\alpha_1, \cdots, \alpha_i]$.

$K = \mathbb{Q}[\alpha_1, \cdots, \alpha_n]$

K_i

$K_2 = \mathbb{Q}[\alpha_1, \alpha_2]$

$K_1 = \mathbb{Q}[\alpha_1]$ $\quad \boxed{\mathbb{Q}[\alpha_k]}$

$\mathbb{Q}$

α_k and α_1 shares the same irreducible poly

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

$\mathbb{Q}[\sqrt[3]{2}, \zeta_3]$ $\Big|\, 2$ $\mathbb{Q}[\sqrt[3]{2}]$ $\Big|\, 3$ $\mathbb{Q}$

Firstly, we count the number of inclusions

$\sigma_1: K_1 = \mathbb{Q}[\alpha_1] \hookrightarrow K$.

If $f_1(x)$ is the minimal deg polynomial s.t. $f_1(\alpha_1) = 0$. then

$[K_1 : \mathbb{Q}] = \deg(f_1)$

$= \#$ of roots of f_1

$f_1 | f$ so f_1 also splits in K. i.e. all the roots of f_1 are in K.

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

by $\quad \sigma_1 : \mathbb{Q}[\alpha_1] \xrightarrow{\sim} \mathbb{Q}[x]/\langle f_1(x)\rangle \xrightarrow{\sim} \mathbb{Q}[\alpha] \hookrightarrow K.$

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

Now for the next step, we consider

$$\begin{tikzcd}
\sigma_2 : \mathbb{Q}[\alpha_1, \alpha_2] \arrow[r, hook] \arrow[d, dash] & K \arrow[d, dash] \\
\sigma_1 : \mathbb{Q}[\alpha_1] \arrow[r, "\sim", dash] \arrow[d, dash] & M_1 \arrow[d, dash] \\
\mathbb{Q} \arrow[r, dash] & \mathbb{Q}
\end{tikzcd}$$

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. $f_2(\alpha_2) = 0$.

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

$$\begin{aligned}
[\mathbb{Q}[\alpha_1, \alpha_2] : \mathbb{Q}[\alpha_1]] &= \deg f_2(x) \\
&= \#\text{ of roots of } f_2(x) \\
&= \#\text{ of extension of } \sigma_1 \text{ to } \\
&\quad \sigma_2.
\end{aligned}$$

Ex. Given $\mathbb{Q}[\alpha_1] \overset{\varphi}{\simeq} M_1$. 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.
$$\mathbb{Q}[\alpha_1][x]/\langle f_2(x)\rangle \simeq M_1[x]/\langle f_2'(x)\rangle .$$

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

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

By induction, eventually, you will get.

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

So K is Galois. $\square$.

Application.

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

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

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

eg.

$f(x) = x^2 - 2$. $\quad \mathrm{Gal}(f) = C_2$

$$\mathrm{Gal}(f) \, \| \, \mathrm{Gal}(\mathbb{Q}[\sqrt{2}]/\mathbb{Q}) = \left\{ \sigma : \sqrt{2} \to \begin{cases} -\sqrt{2} \\ \sqrt{2} \end{cases} \right\}$$

$f(x) = (x^2-2)(x^2-3)$ $\quad \mathrm{Gal}(f) = C_2 \times C_2$.

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

$$\simeq \left\{ \begin{array}{l} \sigma: \sqrt{2} \to \pm\sqrt{2} \\ \quad \sqrt{5} \to \pm\sqrt{5} \end{array} \right\} \quad \text{4 elements.}$$

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

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.

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

$f(x) = (x^2-2)(x^2-5)(x^2-3)$ 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

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

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

$\sigma: K_f \longrightarrow K_f$ indues a permutation of α_is.

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

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

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

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

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

recall G is solvable iff $e \subseteq G_1 \subseteq \cdots \subseteq G_n = G$. G_i/G_{i-1} is abelian.

Pf:

$$\begin{array}{cc}
K_n & \{e\} \\
| & | \\
K_{n-1} & G_{n-1} \\
| & | \\
\vdots & \vdots \\
K_2 & G_2 \\
| & | \\
K_1 & G_1 \\
\mathbb{Q} & G
\end{array}$$

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

Galois ext over $\mathbb{Q}$

$$\begin{tikzcd}
K_2 = \mathbb{Q}[\zeta_k, \sqrt[k]{a}] \arrow[d, dash] \arrow[dd, dash, bend right] \\
K_1 = \mathbb{Q}[\zeta_k] \arrow[d, dash] \\
\mathbb{Q}
\end{tikzcd}$$

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

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

$$\overset{\shortparallel}{\{ \sigma_i : \zeta_k \to \zeta_k^i \}}$$ ← notice not all integers work for i. eg. $\underset{i}{\underset{\shortparallel}{\zeta_4}} \not\to \underset{-1}{\underset{\shortparallel}{\zeta_4^2}}$

$$\sigma_i \circ \sigma_j = \sigma_j \circ \sigma_i : \zeta_k \to \zeta_k^{i \cdot j}$$

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

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

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

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

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

that all K_i are Galois by construction.

$$G \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq \{e\}.$$

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.

$\sqrt{1-\sqrt{2}}$

$$\begin{array}{c} \mathbb{Q}[\underset{\alpha}{\sqrt{1-\sqrt{2}}}, -\sqrt{1-\sqrt{2}}] \\ | \\ \mathbb{Q}[\sqrt{2}] = F \\ | \\ \mathbb{Q} \end{array}$$

will not be Galois over $\mathbb{Q}$

$f(x) \in F[x]$.

find the

Rmk. 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

$(a\ b\ c)$

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

$\sigma H = H\sigma$