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

irreducible normal extension (meaning \( f(x) \) 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, \( L/F \) 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: "\( \Rightarrow \)" By primitive element thm.

By primitive element thm.

\[ K = \mathbb{Q}[x] \text{ then say } f(x) \text{ is the minimal degree poly in } \mathbb{Q}[x] \text{ s.t. } f(x) = 0. \]
$f(x)$ is in $K$, so $f(x)$ splits in $K$.
And since $K = \mathbb{Q}[x]$ is the minimal subfield of $\mathbb{C}$
that contains $x$. 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 $K_i = \mathbb{Q}[x_1, \ldots, x_i]$. 

\[
K = \mathbb{Q}[x_1, \ldots, x_n] \quad \text{Firstly, we count the}
\]

number of inclusions

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

If $f_i(x)$ is the minimal
deg polynomial s.t. 
$f_i(x_i) = 0$, then

\[
[K_i : \mathbb{Q}] = \text{deg } (f_i) \quad = \# \text{ of roots of}
\]

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

eg. $\mathbb{Q}, \sqrt{2} \subseteq \mathbb{Q} \left\{ \sqrt{2}, \sqrt{3} \right\}$ 

\[
1 \quad 2
\]

$\mathbb{Q} \left\{ \sqrt{2}, \sqrt{3} \right\}$ 

\[
1 \quad 3
\]

$\mathbb{Q}$

\[
\mathbb{Q} \left\{ \sqrt{2} \right\}$ 

\[
1 \quad 2
\]

$\mathbb{Q}$
So there are $\deg(f_1)$ many choices to define $\sigma_1$.

by $\sigma_1 : \mathbb{Q}[x] \xrightarrow{f_1(x)} \mathbb{Q}[x] \xrightarrow{f_1(x)} \mathbb{Q}[x] \xrightarrow{} K.$

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

Now for the next step, we consider

$$\sigma_2 : \mathbb{Q}[x_1, x_2] \xrightarrow{} K$$

$$\sigma_1 : \mathbb{Q}[x_1] \xrightarrow{} \mathbb{M}_1$$

$$\mathbb{Q} \xrightarrow{} \mathbb{Q}$$

To define $\sigma_2$, we take $f_2(x) \in K[x]$, s.t. $f_2(x)$ is the minimal deg polynomial s.t. $f_2(\sigma_1 x) = 0$.

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

$$[\mathbb{Q}[x_1, x_2] : \mathbb{Q}[x_1]] = \deg f_2(x)$$

$$\Rightarrow \# \text{ of roots of } f_2(x)$$

$\Rightarrow \# \text{ of extension of } \sigma_1 \text{ to } \sigma_2.$

Ex. Given $\mathbb{Q}[x] \xrightarrow{} \mathbb{M}_1$, and $f_2(x)$ irreducible $\in \mathbb{Q}[x]$, denote $f_2(x) = \Psi(f_2(x))$, then there is an isomorphism between the field.

$$\mathbb{Q}[x] \xrightarrow{\left< f_2(x) \right>} \mathbb{M}_2 \xrightarrow{\left< f_2'(x) \right>} \mathbb{Q}[x] \xrightarrow{\left< f_2'(x) \right>} .$$

We have shown for each fixed $\sigma_1$, there’re $[K_2 : K_1]$ extensions to $\sigma_2$. So altogether, the $\# \text{ of } \sigma_2 : K_2 \xrightarrow{} K$
is \[ [K_2 : K_1] \cdot [K_1 : \mathbb{Q}] = [K_2 : \mathbb{Q}] \].

By induction, eventually, you will get

\[ \mathbb{Q} = K_n = [K_n : \mathbb{Q}] \] which implies \[ [\text{Aut}(K/\mathbb{Q})] = [\mathbb{Q} : \mathbb{Q}] \].

So \( K \) is Galois. \( \square \).

Application.

Def (Galois gap 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.

\[ f(x) = x^2 - 2. \]

\[ \text{Gal}(f) = C_2 \]

\[ \text{Gal}(\mathbb{Q}[\sqrt{2}]/\mathbb{Q}) = \left\{ 6 : \sqrt{2} \rightarrow \pm \sqrt{2} \right\} \]

\[ f(x) = (x^2 - 2)(x^2 - 3) \text{ and } x^2 - 7x^2 + 10 \]

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

\[ \left\{ 6 : \sqrt{2} \rightarrow \pm \sqrt{2}, \sqrt{3} \rightarrow \pm \sqrt{3} \right\} \]

\[ \text{and } 6^2 = \text{id. } \forall 6 \in \text{Gal}(f). \]

We say \( f(x) \) is solvable with radicals if:

the roots of \( f(x) \) can be written as \( +, -, \times, \div \) and

taking radicals of numbers.

\[ ax^2 + bx + c = 0 \]

\[ x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \]

\[ f(x) = (x^2 - 2)(x^2 - 5)(x^2 - 3) \text{ you can still solve by radicals.} \]
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 $K_f = \mathbb{Q}[\alpha_1, \ldots, \alpha_n]$.

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

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

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

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

**Remk.** (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 $e \in G, e \cdots e G_n = G, G_i/G_{i+1}$ is abelian.

**Pf:**

\[
\begin{array}{c|c|c|c|}
K_n & \{e\} & & \\
K_{n-1} & G_{n-1} & & \\
\vdots & \vdots & \ddots & \vdots \\
K_2 & G_2 & & \\
K_1 & G_1 & & \\
\end{array}
\]

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

Suppose $f(x)$ is solvable with radicals, say $\sqrt[n]{a}$ where $a \in \mathbb{Q}$ appear in the expression of roots.
then \( k_2 = \mathbb{Q} \left[ 3_k, \sqrt[3]{\alpha} \right] \) is splitting field of \( f_2(x) = x^k - a \) \( a \in \mathbb{Q} \)

Cyclotomic over \( \mathbb{Q} \) by construction

\[
\begin{align*}
&\text{Gal} (\mathbb{Q}[3_k] / \mathbb{Q}) \text{ is abelian since } \\
&\text{all } G_i \text{ are Galois by construction.}
\end{align*}
\]

Inductively taking all the roots in the expression, then we can get a sequence of fields

\[ \mathbb{Q} \subseteq k_1 \subseteq k_2 \subseteq \ldots \subseteq k_n \]

Notice that \( f(x) \) splits in \( k_n \) via construction so \( k_f \) is a quotient of \( k_n \), and solvable gap
has solvable quotient, so \( G(\mathbb{K}_f/\mathbb{Q}) \) is solvable.

\[ \sqrt{1 - \sqrt{2}} \]

will not be Galois over \( \mathbb{Q} \)

\[ \mathbb{Q} \left[ \sqrt{2} \right] = \mathbb{Q} \quad \text{find the} \]

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. fix \( \alpha \) with \( \deg \alpha > 5 \) is not always solvable with radicals, because \( S_n \) is not solvable when \( n > 5 \).

Start 1:30 pm — End 5:30 pm

\( 6 H = H \)

\( \sigma \)

\( \sigma \) is solvable with radicals because \( S_n \) is not solvable when \( n > 5 \).

\( \sigma H = H \)

( a b c )

\( \sigma^3 = (a b c) \)