Theorem: Let $F \subset K$ be a finite extension satisfying ...

There is a bijection between intermediate fields of $F \subset K$ and subgroups of $G = \mathrm{Aut}_F(K)$.

Moreover the diagram of intermediate fields is the same as the diagram of subgroups, reversed.

$$\begin{tikzcd}
 & K & \\
 & K_3 \arrow[u] & \\
K_1 \arrow[ur] & & K_2 \arrow[ul] \\
 & F \arrow[ul] \arrow[ur] &
\end{tikzcd}
\qquad
\text{degree} \longleftrightarrow \text{index}
\qquad
\begin{tikzcd}
 & \{id\} \arrow[d] & \\
 & H_3 \arrow[dl] \arrow[dr] & \\
H_1 \arrow[dr] & & H_2 \arrow[dl] \\
 & G &
\end{tikzcd}$$

$$F \subset K_i \mapsto \mathrm{Aut}(K/K_i)$$

$$\left\{ x \in K \;\middle|\; \begin{array}{l} \forall \sigma \in H \\ \sigma(x) = x \end{array} \right\} \longmapsfrom H$$

$\underbrace{\mathbb{Q} \subset K}_{\text{finite ext}^n} \subset \mathbb{C}$

could be reducible.

Def: K is the splitting field of $f(x) \in \mathbb{Q}[x]$
if $K = \mathbb{Q}[\alpha_1, \dots, \alpha_n]$ where
$\alpha_1, \dots, \alpha_n$ are all the complex roots of $f(x)$.

Ex. The splitting field of $x^3 - 2$ is

$$\mathbb{Q}[2^{1/3}, 2^{1/3} e^{2\pi i/3}, 2^{1/3} e^{4\pi i/3}]$$
$$\parallel$$
$$\mathbb{Q}[2^{1/3}, e^{2\pi i/3}]$$

Rem: $\underset{\text{finite}}{\mathbb{Q} \subset K}$ then $\exists$ $\underbrace{\mathbb{Q} \subset K \subset L}_{\text{finite}}$ s.t. L is a splitting field.

More generally,

$F \subset K$ finite ext^n is called a splitting field of $f(x) \in F[x]$ if

(1) $f(x) = \text{const} \cdot (x-\alpha_1) \cdots (x-\alpha_n)$ for $\alpha_i \in K$ holds in $K[x]$

(2) $K = F[\alpha_1, \dots, \alpha_n]$

The smallest subfield of K containing F & $\alpha_1, \dots, \alpha_n$ is K itself.

$F \subset K$ splitting field of $f(x)$

$\uparrow$ roots are $\alpha_1, \dots, \alpha_n$.

Elts here are poly expns in $\alpha_1, \dots, \alpha_n$ with coeff in F.

Key: Identify elements that lie in F.

monic $f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$.

$\Rightarrow$ $\alpha_1\alpha_2\cdots\alpha_n \in F$

$\alpha_1\alpha_2\cdots\alpha_{n-1} + \cdots\cdots +$ (drop 1) $\in F$

$\alpha_1\alpha_2\cdots\alpha_{n-2} + \cdots$ (drop 2) $\in F$

$\vdots$

$\alpha_1 + \alpha_2 + \cdots + \alpha_n$ (drop $n-1$) $\in F$

Thm: Any symmetric poly in $\alpha_1, \dots, \alpha_n$ with coeff in F is an elt of F.

True because of the following - R any ring.

$R[X_1, \dots, X_n]$ = Poly in R in n variables.

Elementary sym. poly.

$$\sigma_1 = X_1 + X_2 + \dots + X_n$$
$$\sigma_2 = X_1X_2 + \dots$$
$$\sigma_3 = X_1X_2X_3 + \dots$$
$$\vdots$$
$$\sigma_n = X_1X_2X \dots X_n$$

<u>Thm</u>: Any sym. poly in $R[X_1, \dots, X_n]$ can be written as a polynomial in $\sigma_1, \dots, \sigma_n$ with R coeff.

<u>Ex.</u> $n=2$ $\quad \mathbb{Q}[X, Y]$

$$x^2y + y^2x = xy \cdot (x+y) = \sigma_2 \cdot \sigma_1$$

$$x^3 + y^3 = (x+y)^3 - 3x^2y - 3xy^2 = (x+y)^3 - 3xy(x+y) = \sigma_1^3 - 3 \cdot \sigma_2 \cdot \sigma_1$$

3 vars.   2 vars

$$(x^3+y^3+z^3) \xrightarrow{z=0} x^3+y^3 = \sigma_1^3 - 3\sigma_2\sigma_1$$

Try $$(x^3+y^3+z^3) = \sigma_1(x,y,z)^3 - 3\sigma_2(x,y,z)\sigma_1(x,y,z) + R(x,y,z).$$

symmetric
vanishes if $z=0$.

symmetry $\Rightarrow$ $R(x,y,z) = \underbrace{xyz}_{\sigma_3} \cdot R'(x,y,z)$

$$= \sigma_1(x,y,z)^3 - 3\sigma_2(x,y,z)\sigma_1(x,y,z) + \sigma_3(x,y,z)\, R'(x,y,z).$$

$$(x^4+y^4) = \cancel{(x+y)^4} - \cancel{4x^3y}\ (x+y)^4 - xy\,(\underbrace{4x^2+6xy+4y^2}_{4(x+y)^2 - xy\,(2)}).$$