<u>Recall:</u> $G \subseteq \mathrm{Aut}(E) \longrightarrow E_G := \{\alpha \in E \mid \sigma(\alpha) = \sigma, \forall \sigma \in G\}$

<u>Prop</u> Let $G \subseteq \mathrm{Aut}(E)$ be a finite subgroup, with E a field, and let $F = E_G$. Then $[E:F] \leq |G|$.

(Proof.) Write $G = \{\sigma_1, \dots, \sigma_n\} \subseteq \mathrm{Aut}(E)$.

WTS: E has dim'n at most n over F.

So we'll show that <u>any</u> collection $\alpha_1, \dots, \alpha_{n+1} \in E$ is linearly dependent over F.

i.e., $\exists\ c_1, \dots, c_{n+1} \in F$, not all 0, s.t.

$$c_1 \alpha_1 + c_2 \alpha_2 + \dots + c_{n+1} \alpha_{n+1} = 0. \qquad (\star)$$

To this end, consider the following system of equations in E:

$$\begin{aligned}
\sigma_1(\alpha_1) X_1 + \sigma_1(\alpha_2) X_2 + \cdots + \sigma_1(\alpha_{n+1}) X_{n+1} &= 0 \\
\sigma_2(\alpha_1) X_1 + \sigma_2(\alpha_2) X_2 + \cdots + \sigma_2(\alpha_{n+1}) X_{n+1} &= 0 \\
\vdots \qquad\qquad \vdots \qquad\qquad\qquad \vdots \quad &= \vdots \\
\sigma_n(\alpha_1) X_1 + \sigma_n(\alpha_2) X_2 + \cdots + \sigma_n(\alpha_{n+1}) X_{n+1} &= 0
\end{aligned}$$

Here, $X_1, \dots, X_{n+1} \in E$ are indeterminates.

$|G| = n \Rightarrow n$ equations.

Underdetermined $\Longrightarrow \exists\ a_1, \dots, a_{n+1} \in E$ not all zero satisfying the eqns.

Notice that if $\sigma_i = \mathrm{id} \in G$, then then the i^{th} equation of our system is $(\star)$.

So we win if $a_1, \dots, a_{n+1} \in F$.

Suppose $(a_1, \dots, a_{n+1}) \in E^{n+1}$ is a nontrivial sol'n with minimal # of nonzero entries.

WLOG, $a_1 \neq 0$.

Scaling by a_1^{-1} gives us another sol'n, so we can assume $a_1 = 1$.

$\S$ $a_2 \notin F = E_G$.

Then $\exists\, \sigma_i \in G$ with $\sigma_i(a_2) \neq a_2$.

Now set $x_j = a_j - \sigma_i(a_j)$, for $1 \le j \le n+1$.

i.e.,
$$\begin{aligned} x_1 &= a_1 - \sigma_i(a_1) = 1 - \sigma_i(1) = 0 \\ x_2 &= a_2 - \sigma_i(a_2) \neq 0 \\ &\vdots \\ x_{n+1} &= a_{n+1} - \sigma_i(a_{n+1}) \end{aligned}$$

But $(a_1, \dots, a_{n+1})$ & $(\sigma_i(a_1), \dots, \sigma_i(a_{n+1}))$ are sol'ns to the system.

$\therefore$ $(x_1, \dots, x_{n+1})$ is a nontrivial sol'n with fewer nonzero entries than $(a_1, \dots, a_{n+1})$ $\times$. $\blacksquare$

Def'n. Let $E \supset F$ be an algebraic extension field. Call E a normal extension if every irreducible polynomial in $F[x]$ with at least one root in E splits in E.

Ex $\mathbb{Q}(\sqrt[4]{5}) \supset \mathbb{Q}$ is not normal.

$x^4 - 5 \in \mathbb{Q}[x]$ does not split in $\mathbb{Q}(\sqrt[4]{5})$

Thm. Let $E \supset F$ be an extension field. TFAE:

1. E is a finite, normal, separable extension of F.
2. E is the S.F. of a separable polynomial in $F[x]$.
3. $F = E_G$ for some finite subgroup $G \leq \mathrm{Aut}(E)$.

Ex. $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{5})/\mathbb{Q}) = \{id, \tau\} \cong \mathbb{Z}_2$,

with τ fixes $\underbrace{\mathbb{Q}(\sqrt{5})}_{\text{the actual fixed field strictly contains the base field.}} \subset \mathbb{Q}(\sqrt[4]{5})$.

Cor. Let $K \supset F$ be a field extension s.t. $F = K_G$ for some finite subgroup $G \leq \mathrm{Aut}(K)$. Then $G = G(K/F)$.

Thm (Fundamental Theorem of Galois Theory)

Let F be a field of characteristic 0, $E \supset F$ a finite, normal extension of F with Galois group $G(E/F)$.

Then:

1. The map $K \mapsto G(E/K)$ is a bijection from subfields of E containing F to the subgroups of $G(E/F)$.

2. For any $E \supseteq K \supseteq F$,

$$[E:K] = |G(E/K)| \quad \& \quad [K:F] = [G(E/F) : G(E/K)].$$

3. Subfields $F \subseteq K, L \subseteq E$ satisfy $K \subseteq L$ iff

$$\{id\} \leq G(E/L) \leq G(E/K) \leq G(E/F).$$

4. A subfield $K \subset E$ is a normal extension of F iff $G(E/K)$ is a normal subgroup of $G(E/F)$.
   Moreover, in this case we have an isomorphism

$$G(K/F) \cong \frac{G(E/F)}{G(E/K)}.$$

Ex. Consider $f(x) = x^4 - 2 \in \mathbb{Q}[x]$.

$F := \mathbb{Q}$

① The splitting field.

$$x^4 - 2 = (x^2 - \sqrt{2})(x^2 + \sqrt{2})$$
$$= (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x - i\sqrt[4]{2})(x + i\sqrt[4]{2}),$$

So the S.F. of $f(x)$ is $\mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}, i). =: E$

② The order of $G(E/F)$.

$\mathbb{Q}(\sqrt[4]{2}) \supset \mathbb{Q}$ has basis $\{1, \sqrt[4]{2}, (\sqrt[4]{2})^2, (\sqrt[4]{2})^3\}$

$E \supset \mathbb{Q}(\sqrt[4]{2})$ has basis $\{1, i\}$

So $\left.[E:F] = [E : \mathbb{Q}(\sqrt[4]{2})] \cdot [\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}]\right\}$ by FToGT

$= 2 \cdot 4 = 8.$

So $\left.|G(E/F)| = [E:F] = 8.\right\}$ E is the S.F. of a separable polynomial

③ Identifying $G(E/F)$

Let's define $\sigma, \tau : E \longrightarrow E$ by

90° CCW rotation
$$\left[\begin{array}{lcl} \sigma(\sqrt[4]{2}) := i\sqrt[4]{2} & ; & \tau(\sqrt[4]{2}) := \sqrt[4]{2} \\ \sigma(i) := i & & \tau(i) := -i \end{array}\right]$$
reflection

Check: $id, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau$ are all distinct.

Upshot: 8 distinct elements of $G(E/F)$.

Since we know $|G(E/F)| = 8$,

$$G(E/F) = \{id, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\} \cong D_4$$

④ The subgroups of $G(E/F)$.

$$\begin{tikzcd}
 & & \{id\} \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
\{id, \tau\} \arrow[dr, dash] & \{id, \sigma^2\tau\} \arrow[d, dash] & \{id, \sigma^2\} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \{id, \sigma\tau\} \arrow[d, dash] & \{id, \sigma^3\tau\} \arrow[dl, dash] \\
 & \{id, \sigma^2, \tau, \sigma^2\tau\} \arrow[dr, dash] & \{id, \sigma, \sigma^2, \sigma^3\} \arrow[d, dash] & \{id, \sigma^2, \sigma\tau, \sigma^3\tau\} \arrow[dl, dash] & \\
 & & G(E/F) & &
\end{tikzcd}$$

$\sigma(\sqrt[4]{2}) = i\sqrt[4]{2}$

$$\sigma^2(\sqrt[4]{2}) = \sigma(i\sqrt[4]{2})$$
$$= \sigma(i)\,\sigma(\sqrt[4]{2})$$
$$= i(i\sqrt[4]{2}) = -\sqrt[4]{2}$$

⑤ The fixed fields

$$\begin{tikzcd}
 & & E \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
\mathbb{Q}(\sqrt[4]{2}) \arrow[dr, dash] & \mathbb{Q}(\sqrt[4]{2}\, i) \arrow[d, dash] & \mathbb{Q}(\sqrt{2}, i) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \mathbb{Q}((1+i)\sqrt[4]{2}) \arrow[d, dash] & \mathbb{Q}((1-i)\sqrt[4]{2}) \arrow[dl, dash] \\
 & \mathbb{Q}(\sqrt{2}) \arrow[dr, dash] & \mathbb{Q}(i) \arrow[d, dash] & \mathbb{Q}(\sqrt{2}\, i) \arrow[dl, dash] & \\
 & & F & &
\end{tikzcd}$$