Recall:

Thm. Suppose $E \supset F$ is the S.F. of $f(x) \in F[x]$. If $f(x)$ has no repeated roots, then

$$|G(E/F)| = [E:F].$$

dimension of E as a v.s. over F

(Proof.) Induction on $[E:F]$.

Base: $[E:F] = 1 \Rightarrow E = F \Rightarrow G(E/F) = \{id\}$

Inductive step:

$\mathcal{S}$ theorem holds for extension of degree less than $[E:F]$, with $[E:F] > 1$.

Write $f(x) = p(x)q(x)$, with $p(x)$ irreducible.
B/c $[E:F] > 1$, we can assume $\deg p(x) > 1$.
Let $d = \deg p(x)$.

Let $\alpha \in E$ be a root of $p(x)$. For any injective homom. $\phi: F(\alpha) \to E$, $\phi(\alpha) =: \beta$ is also a root of $p(x)$, and $\phi: F(\alpha) \to F(\beta)$ is an isom:

$$p(x) = a_0 + a_1 x + \cdots + a_d x^d$$

ϕ is an injective homom.

$$\Rightarrow 0 = \phi(0) = \phi(p(\alpha)) = p(\phi(\alpha))$$

Consider <u>all</u> isomorphisms $\phi: F(\alpha) \to F(\beta)$ which fix F (i.e., $\phi(c) = c$, $\forall c \in F$).

Since $f(x)$ has no repeated roots, $p(x)$ has no repeated roots. $\therefore$ roots of $p(x) = \{\beta_1, \dots, \beta_d\} \subset E$.

$\therefore$ exactly d isomorphisms $\phi_i : F(\alpha) \to F(\beta_i)$

Consider diagrams of the form

$$\begin{tikzcd}
E \arrow[r, dashed, "\psi"] \arrow[d] & E \arrow[d] \\
F(\alpha) \arrow[r, "\phi_i"] \arrow[d] & F(\beta_i) \arrow[d] \\
F \arrow[r, "id"] & F
\end{tikzcd}$$

$|G(E/F)|$ counts the possibilities for this diagram

From above, d possibilities for this square.

Here, $\psi \in G(E/F(\alpha))$. i.e., we count possibilities for top square by counting $|G(E/F(\alpha))|$.

But $E \supset F(\alpha)$ is the S.F. for $q(x)$, so I.H.

Says $|G(E/F(\alpha))| = [E:F(\alpha)] < [E:F]$.

So there are

$$[E:F(\alpha)] \cdot d = [E:F(\alpha)][F(\alpha):F]$$
$$= [E:F]$$

ways to complete the square. $\blacksquare$

<u>Ex</u>. $H = \{id, \sigma, \tau, \sigma\tau\} \subseteq G(E/F)$,

where $E = \mathbb{Q}(\sqrt{3}, \sqrt{5})$ & $F = \mathbb{Q}$.

But E is the S.F. of $f(x) = (x^2-3)(x^2-5)$, which has no repeated roots, so

$$|G(E/F)| = [E:F] = [\mathbb{Q}(\sqrt{3},\sqrt{5}):\mathbb{Q}(\sqrt{3})]\cdot[\mathbb{Q}(\sqrt{3}):\mathbb{Q}]$$
$$= 2\cdot 2 = 4.$$

$\therefore\ H = G(E/F).$

So $G(f(x)) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Separability

Let $E \supset F$ be the S.F. of $f(x) \in F[x]$ and write

$$f(x) = \prod_{i=1}^{r} (x-\alpha_i)^{n_i} = (x-\alpha_1)^{n_1} \cdot \ldots \cdot (x-\alpha_r)^{n_r}.$$

The **multiplicity** of α_i as a root is n_i.

If $n_i = 1$, α_i is a **simple root**.

Call $f(x)$ **separable** if all roots are simple.

Call $E \supset F$ a **separable extension** if every elt of E is a root of some separable polynomial in $F[x]$.

Prop. Over a field of characteristic 0, every irreducible polynomial is separable.

Rmk Char $\mathbb{Q} = 0$, so for us all irreducibles will be separable.

$(x^2-2)(x^2-2)$ has repeated roots
has no roots in $\mathbb{Q}$
NOT irreducible

Def. If $E \supset F$ can be written as $E = F(\alpha)$, for some $\alpha \in E$, call α a **primitive element**.

<u>Primitive Element Theorem</u>. If $E \supset F$ is a finite, separable extension, $\exists\, \alpha \in E$ s.t. $E = F(\alpha)$.

<u>Cor</u> Any S.F. of an irreducible in $\mathbb{Q}[x]$ is a simple extension.

<u>Fixed fields</u>

Recall: $G(E/F) \subseteq \mathrm{Aut}(E)$; $\mathrm{Aut}(E) \circlearrowright E$

Given a subgroup $G \subseteq \mathrm{Aut}(E)$, define

$$E_G := \{\alpha \in E \mid \sigma(\alpha) = \alpha, \forall \sigma \in G\}.$$

<u>Exercise</u>. E_G is a field.

We call E_G the fixed field of G.

<u>Example</u>: $H := \{id, \sigma\} \subsetneq G(E/F)$ from above.

Check: $E_H = \mathbb{Q}(\sqrt{5})$.

<u>Prop</u>. Let $E \supset F$ be the S.F. for a separable polynomial over F. Then $E_{G(E/F)} = F$.

(Proof.) From def'n, $F \subseteq E_{G(E/F)}$.

$E \supset F$ a S.F. $\Longrightarrow$ $E \supset E_{G(E/F)}$ is a S.F.

$$G(E/F) = G(E/E_{G(E/F)}). \ *$$

Thm above: as S.F. of separable polynomial,

$$[E : E_{G(E/F)}] = |G(E/E_{G(E/F)})|$$
$$= |G(E/F)|$$
$$= [E:F].$$

So $F = E_{G(E/F)}$. ∎

<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.

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

⋱