Cor. If α is algebraic over a field F, $\alpha \in F$,
Suppose $\psi : F(\alpha) \xrightarrow{\cong} E \subseteq F$ s.t.
$\psi(c) = c \ \forall c \in F$. Then $\psi(\alpha) = \beta$, β conj to α,
and $\psi = \psi_{\alpha,\beta}$.

Defn. An isomorphism $F \longrightarrow F$ is called
an <u>automorphism</u>.

If $\sigma : F \to F$ is an automorphism,
we say <u>σ fixes $a \in F$</u> if $\sigma(a) = a$.

We set $F_{\{\sigma_i\}} := \{a \in F : \sigma_j(a) = a \text{ for all } \sigma_j \in \{\sigma_i\}\}$.

$\uparrow$ collection of automorphisms of F $= \{a \in F : \sigma_j \text{ fixes } a \ \forall \sigma_j \in \{\sigma_i\}\}$.

$F_{\{\sigma_i\}}$ is called the
"<u>fixed field of $\{\sigma_i\}$ in F</u>".

Thm If $\{\sigma_i\}$ is <u>a</u> collection of automorphisms
of F, then $F_{\{\sigma_i\}}$ is a subfield of F.

Proof. If $a, b \in F_{\{\sigma_i\}}$.

$\boxed{\text{Note } 0 \in F_{\{\sigma_i\}}.}$ $\forall \sigma_j \in \{\sigma_i\}$, $\sigma_j(a+b) = \sigma_j(a) + \sigma_j(b) = a + b$. ✓
$\Rightarrow a + b \in F_{\{\sigma_i\}}$.

Similarly $a-b$, ab, $\frac{a}{b}$ if $b \neq 0$ are in $F_{\{\sigma_i\}}$.

Thm Let $\mathrm{Aut}(E) = \{\text{automorphisms } \sigma: E \to E\}$.
Then $\mathrm{Aut}(E)$ is a group (composition = group operation)

Pf. Identity $I: E \to E$ is an automorphism,
so $\mathrm{Aut}(E) \neq \emptyset$. Note if $\sigma_1, \sigma_2, \sigma_3$ are automorphisms
of E, then $\sigma_1 \circ \sigma_2$ is automorphism. ✓

$$(\sigma_1 \circ \sigma_2) \circ \sigma_3 = \sigma_1 \circ (\sigma_2 \circ \sigma_3). ✓$$

Identity I is an automorphism and,

$$I \circ \sigma_3 = \sigma_3 \circ I = \sigma_3. ✓$$

$\forall \ \sigma \in \mathrm{Aut}(E) \quad \sigma^{-1} \in \mathrm{Aut}(E)$.

and $\sigma \circ \sigma^{-1} = I$. ✓

Notation: Suppose $F \leq E$ are fields. Let $G(E/F) = \{\psi: E \to E$ automorphisms such that ψ fixes $F\}$.
(called group of E over F)

Thm $G(E/F)$ is a subgroup of $\mathrm{Aut}(E)$, and
$$F \leq E_{G(E/F)}.$$

Proof: I fixes $F \Rightarrow I \in G(E/F)$.

$\forall \ \sigma, \tau \in G(E/F)$,

$\sigma \circ \tau \in \mathrm{Aut}(E)$ and $\forall a \in F$,

$$(\sigma \circ \tau)(a) = \sigma(\tau(a)) = \sigma(a) = a$$

so $\sigma \circ \tau \in G(E/F)$.

If $\tau: E \to E$ fixes F, then

$\tau(a) = a \ \forall \ a \in F$.

Apply τ^{-1}: $\quad \tau^{-1}(\tau(a)) = \tau^{-1}(a)$

$$\Rightarrow \quad a = \tau^{-1}(a)$$

$$\Rightarrow \tau^{-1} \in G(E/F).$$

$$\therefore G(E/F) < \mathrm{Aut}(E). \boxtimes$$

Next suppose $a \in F$. Then

$\forall \tau \in G(E/F)$, $\tau(a) = a \Rightarrow a \in E_{G(E/F)}$.

$\therefore F \leq E_{G(E/F)}$. $\boxtimes$

Example: Consider $E = \mathbb{Q}(\sqrt{2}, \sqrt{5})$ over $\mathbb{Q} = F$.

define $\sigma_1 : E \to E$ by

$E = \{ c_1 + c_2\sqrt{2} + c_3\sqrt{5} + c_4\sqrt{10} \}$
$c_j \in \mathbb{Q}$

$$\sigma_1(c_1 + c_2\sqrt{2} + c_3\sqrt{5} + c_4\sqrt{10}) = c_1 - c_2\sqrt{2} + c_3\sqrt{5} - c_4\sqrt{10}$$

We can check that $\sigma \in G(E/F)$.

Define $\sigma_2 : E \to E$ by

$$\sigma_2(c_1 + c_2\sqrt{2} + c_3\sqrt{5} + c_4\sqrt{10}) = c_1 + c_2\sqrt{2} - c_3\sqrt{5} - c_4\sqrt{10}$$

is also in $G(E/F)$.

$\sigma_1\sigma_2$:

$$(c_1, c_2, c_3, c_4) \to (c_1, -c_2, -c_3, c_4)$$

It turns out.

$$E_{\{\sigma_1\}} = \mathbb{Q}(\sqrt{5})$$

$$E_{\{\sigma_2\}} = \mathbb{Q}(\sqrt{2})$$

$$E_{\underbrace{\{I, \sigma_1, \sigma_2, \sigma_1\sigma_2\}}_{= G(E/F) \cong \mathbb{Z}_2 \times \mathbb{Z}_2}} = \mathbb{Q}.$$

believe me

<u>Quiz:</u> (1) What is your favorite kind of cake?

(2) Let $F \subseteq \overline{\mathbb{Z}_p}$ be a field of order p^n.

<u>Finish</u>: Then F is the set of zeros of

________________ over $\mathbb{Z}_p$.

(3) If $a \in \mathbb{R}$ is a constructible number then $[\mathbb{Q}(a) : \mathbb{Q}]$ must be ________.

(4) State the known fact about $F^* = F \setminus \{0\}$, if F is a finite field.