<u>Recall</u>: Splitting fields exist. i.e., given $f(x) \in F[x]$, we constructed a splitting field $E \supset F$ for $f(x)$.

Are they unique?

<u>Lemma</u>. Suppose we have

1. an isomorphism of fields $\phi : E \to F$;
2. extension fields $K \supset E$ & $L \supset F$;
3. an algebraic elt $\alpha \in K$ w/ min. poly. $p(x) \in E[x]$;
4. a root $\beta \in L$ of $\phi(p(x)) \in F[x]$.

Then ϕ extends to a unique isom. $\overline{\Phi} : E(\alpha) \longrightarrow F(\beta)$ s.t.

$$\begin{tikzcd}
K \arrow[d] & L \arrow[d] \\
E(\alpha) \arrow[r, dashed, "\overline{\Phi}", "\exists!"'] \arrow[d] & F(\beta) \arrow[d] \\
E \arrow[r, "\phi"] & F
\end{tikzcd}$$

(Proof idea.) Keys: $E(\alpha) \cong E[x]/\langle p(x) \rangle$

$F(\beta) \cong F[x]/\langle \phi(p(x)) \rangle$

linear algebra. $\blacksquare$

Thm. Suppose we have

1. an isomorphism of fields $\phi : E \to F$;
2. a nonconstant polynomial $p(x) \in E[x]$;
3. a splitting field $K \supset E$ of $p(x)$ and a splitting field $L \supset F$ of $\phi(p(x))$.

Then ϕ extends to an isom. $\psi : K \to L$.

(Proof.) Induction on $\deg p(x)$.

Base: $\deg p(x) = 1 \Rightarrow K = E$; $L = F$, so we let $\psi = \phi$.

Inductive step: Assume theorem holds for poly. of degree k, $1 \le k < n$, $n := \deg p(x)$.

Assume $p(x)$ irreducible.

Take a root $\alpha \in K$ of $p(x)$ and a root $\beta \in L$ of $\phi(p(x))$.

Lemma $\Rightarrow$

$$\begin{tikzcd} E(\alpha) \arrow[r, "\Phi"] & F(\beta) \\ E \arrow[u, hookrightarrow, leftarrow] \arrow[r, "\phi"] & F \arrow[u, leftarrow] \end{tikzcd}$$

In $E(\alpha)[x]$, $p(x) = (x-\alpha)f(x)$, for some $f(x) \in E(\alpha)[x]$.

$\phi(p(x)) = (x-\beta)g(x)$, for some $g(x) \in F(\beta)[x]$.

$K \supset E(\alpha)$ is a splitting field for $f(x) \in E(\alpha)[x]$

$L \supset F(\beta)$ is a splitting field for

$$g(x) = \overline{\Phi}(f(x)) \in F(\beta)[x].$$

So inductive hypothesis gives

$$\begin{array}{ccc} K & \xrightarrow{\psi} & L \\ \downarrow & & \downarrow \\ E(\alpha) & \xrightarrow{\overline{\Phi}} & F(\beta). \end{array}$$

$\blacksquare$

<u>Cor.</u> Let F be a field and fix $p(x) \in F[x]$. There exists a splitting field of $p(x)$, unique up to isomorphism

---

Towards Galois theory

For any field F, let $\mathrm{Aut}(F)$ denote the collection of automorphisms of F:

$$\mathrm{Aut}(F) := \{\sigma : F \to F \mid \sigma \text{ is an isomorphism of rings}\}.$$

<u>Prop.</u> For any field F, $\mathrm{Aut}(F)$ is a group under composition.

<u>Prop.</u> Let $E \supset F$ be a field extension. Then

$$G(E/F) := \{\sigma \in \mathrm{Aut}(E) \mid \sigma(\alpha) = \alpha, \forall \alpha \in F\} \leq \mathrm{Aut}(E)$$

is a subgroup of $\mathrm{Aut}(E)$.

(Proof.) Exercise using subgroup criteria. $\blacksquare$

Def. For any field extension $E \supset F$, we call $G(E/F)$ the Galois group of E over F. If $f(x) \in F[x]$ and E is its splitting field, then $G(E/F)$ is the Galois group of $f(x)$ over F.

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

Define $\sigma, \tau \in \mathrm{Aut}(E)$ by

$$\sigma(a + b\sqrt{3}) = a - b\sqrt{3}, \text{ where } a, b \in \mathbb{Q}(\sqrt{5})$$
$$\tau(c + d\sqrt{5}) = c - d\sqrt{5}, \text{ where } c, d \in \mathbb{Q}(\sqrt{3}).$$

Note that σ, τ fix $\mathbb{Q}$.

Soon: $G(E/F) = \{id, \sigma, \tau, \sigma\tau\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Given $f(x) \in F[x]$ and $\sigma \in G(E/F)$, with $E =$ S.F. of $f(x)$, the coefficients of $f(x)$ are fixed by $\sigma : E \to E$. But there could be a root $\alpha \in E$ of $f(x)$ with $\alpha \notin F$, and we could have $\sigma(\alpha) \neq \alpha$. Where can σ take α?

Prop. Let $E \supset F$ be a field extension, $f(x) \in F[x]$ a polynomial. Then any automorphism in $G(E/F)$ permutes those roots of $f(x)$ which lie in E.

(Proof.) Let $\alpha \in E$ be a root of $f(x)$, $\sigma \in G(E/F)$.

We NTS $\sigma(\alpha)$ is a root of $f(x)$.

Write $f(x) = a_0 + a_1 x + \cdots + a_n x^n$.

Then
$$\begin{aligned} 0 = \sigma(0) &= \sigma(f(\alpha)) \\ &= \sigma(a_0 + a_1\alpha + \cdots + a_n\alpha^n) \\ &= a_0 + a_1\sigma(\alpha) + \cdots + a_n(\sigma(\alpha))^n \\ &= f(\sigma(\alpha)). \end{aligned}$$

σ is a homom.
$\sigma(a_i) = a_i$

$\blacksquare$

So $G(E/F)$ is a group, and it acts on the finite set $\{\alpha \in E \mid f(\alpha) = 0\}$.

<u>Def.</u> Let $E \supset F$ be an algebraic field extension. Call $\alpha, \beta \in E$ conjugate over F if α, β have the same minimal polynomial over F.

<u>Prop.</u> Let $E \supset F$ be an algebraic field extension, $\alpha, \beta \in E$ conjugate elements over F. Then there is an isom. $\sigma : F(\alpha) \to F(\beta)$ which restricts to the identity on F.

(Proof.) Apply Lemma from start of today. $\blacksquare$

So the orbits of $G(E/F) \circlearrowright E$ are the conjugacy classes of E, provided E is algebraic over F.

If $E \supset F$ is the S.F. of $f(x) \in F[x]$, we can use the action $G(E/F) \curvearrowright \{\alpha \in E \mid f(\alpha) = 0\}$ to learn things about $G(E/F)$.

<u>Thm</u>. 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 tomorrow.