MATH 403/503 L34

Splitting Fields [Judson §21.2]

Def Let $p(x) \in F[x]$ be nonconstant. An extension field E of F is a splitting field of $p(x)$ (over F) if there exist $\alpha_1, \ldots, \alpha_n \in E$ such that

i) $p(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$

ii) $E = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$

If i) holds we say $p(x)$ splits over E.

Example x^2-2 splits over $\mathbb{R}$ since

$x^2-2 = (x-\sqrt{2})(x+\sqrt{2})$

But $\mathbb{R}$ is not ~~the~~ a splitting field for x^2-2 over $\mathbb{Q}$, because ii) does not hold. However $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt{2}, -\sqrt{2})$ is a splitting field for x^2-2 over $\mathbb{Q}$.

<u>Example</u> Let $p(x) = x^4 + 2x^2 - 8 \in \mathbb{Q}[x]$.
Then $p(x)$ has irreducible factors
$x^2 - 2$ and $x^2 + 4$ (check!)
So $\mathbb{Q}(\sqrt{2}, i)$ is a splitting field
for $p(x)$ over $\mathbb{Q}$.
$\left(\mathbb{Q}(\sqrt{2}, -\sqrt{2}, \sqrt{2}i, -\sqrt{2}i) = \mathbb{Q}(\sqrt{2}, i)\right)$

<u>Example.</u> Let $p(x) = x^3 - 2 \in \mathbb{Q}[x]$.
Then $p(x)$ has a root in the
field $\mathbb{Q}(\sqrt[3]{2})$. However, it is <u>not</u>
a splitting field for $p(x)$ since
the complex cube roots

$$\sqrt[3]{2}\,\varepsilon, \quad \sqrt[3]{2}\,\varepsilon^2$$

(where $\varepsilon = \exp(2\pi i/3) = -\frac{1}{2} + \frac{\sqrt{3}}{2} i$)
are not in $\mathbb{Q}(\sqrt[3]{2})$ since $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$.
Instead, a splitting field for $p(x)$ is
$\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\,\varepsilon, \sqrt[3]{2}\,\varepsilon^2) = \mathbb{Q}(\sqrt[3]{2}, \varepsilon)$
which has degree 6 over $\mathbb{Q}$.
$\left(m_{\varepsilon,\mathbb{Q}}(x) = x^2 + x + 1, \quad m_{\sqrt[3]{2}}(x) = p(x) = x^3 - 2 \right)$

Theorem 21.31 Let $p(x) \in F[x]$ be nonconstant. Then there exists a splitting field for $p(x)$ over F.

Proof Induction on $n := \deg p(x)$.

If $n=1$: Then $p(x)$ already splits in F

so $E = F$ is a splitting field for $p(x)$.

If $n > 1$: WLOG $p(x)$ is irreducible,

optional

otherwise $p(x) = f_1(x) \cdots f_k(x)$ and

$\exists\, E_i = E_{i-1}(\alpha_{i1}, \dots, \alpha_{ik_i})$ splitting field for $f_i(x)$ over E_{i-1}, $E_0 = F$ by induction hypothesis.

Then $E := F(\alpha_{ij})$ is a splitting field for $p(x)$ ~~WLOG regarding all~~

When $p(x)$ is irreducible, we let K be a field in which $p(x)$ has a root α_1 (eg $K = F[x]/(p(x))$). Thus

$p(x) = (x - \alpha_1)\, q(x)$; for some $q(x) \in K[x]$.

$\deg q(x) = (\deg p(x)) - 1$ so by induction hypothesis there is a splitting field $E \supseteq K$ for $q(x)$.

$E = K(\alpha_2, \dots, \alpha_n) = F(\alpha_1, \alpha_2, \dots, \alpha_n)$.

Lemma

Let $\phi : F_1 \to F_2$ be an isomorphism of fields.

Let $p_1(x) \in F_1[x]$ be irreducible and $p_2(x) = \phi(p_1(x))$.

Let E_i ~~$\supseteq F_i$~~ be an extension of F_i containing a root α_i of $p_i(x)$.

Then $\exists !$ isomorphism

$$\Phi : F_1(\alpha_1) \to F_2(\alpha_2)$$

s.t $\Phi|_{F_1} = \phi$ & $\Phi(\alpha_1) = \alpha_2$.

Pf

$$F_1(\alpha_1) \cong \frac{F_1[x]}{(p_1(x))} \overset{\tilde{\phi}}{\cong} \frac{F_2[x]}{(p_2(x))} \cong F_2(\alpha_2)$$

$$\alpha_1 \longleftarrow \bar{x} \qquad \bar{x} \longmapsto \alpha_2$$

$\blacksquare$

<u>Theorem</u> Let $\phi : F_1 \to F_2$ be an isomorphism of fields.
Let $p_1(x) \in F_1[x]$ be nonconstant.
Let $p_2(x) = \phi(p_1(x)) \in F_2[x]$ be the corresponding pol over F_2.
Let E_i be a splitting field for $p_i(x)$ over F_i, for $i = 1, 2$.
Then ϕ extends to an isomorphism
$\Phi : E_1 \to E_2$.

<u>Proof</u> Induction on $n := \deg p_1(x)$:

<u>$n=1$</u>: Then $E_1 = F_1$ and $E_2 = F_2$ so can take $\Phi = \phi$.

<u>$n>1$</u>: If $p_1(x)$ is reducible, say $p_1(x) = f_1(x)\, g_1(x)$ where f_1, g_1 are nonconstant, then E_1 contains a splitting field for $f_1(x)$, $\tilde{E}_1$ say, and E_2 contains a splitting field $\tilde{E}_2$ for $f_2(x) := \phi(f_1(x))$.

By the induction hypothesis, ϕ extends to an isomorphism $\tilde{\phi} : \tilde{E}_1 \longrightarrow \tilde{E}_2$

Then regard $g_1(x) \in \tilde{E}_1[x]$, $g_2(x) = \tilde{\phi}(g_1(x)) \in \tilde{E}_2[x]$

E_1 is ~~the~~ a splitting field for $g_1(x)$ over $\tilde{E}_1$. So $\tilde{\phi}$ extends to an isomorphism $\Phi : E_1 \longrightarrow E_2$.

If $p_1(x)$ is irreducible, let $\alpha_1 \in E_1$ be a root, and write

$$p_1(x) = (x - \alpha_1) q_1(x)$$

where $q_1(x) \in F_1(\alpha_1)[x]$

Let $\alpha_2 \in E_2$ be a root of $p_2(x)$ so

$$p_2(x) = (x - \alpha_2) q_2(x)$$

By Lemma, ϕ extends to an isomorphism $\bar{\phi} : F_1(\alpha_1) \longrightarrow F_2(\alpha_2)$

$$\alpha_1 \longmapsto \alpha_2$$

Now E_1 is a splitting field for $q_1(x)$ over $F_1(\alpha_1)$. By Induction Hypothesis, $\bar{\phi}$ extends to an isomorphism $\Phi : E_1 \to E_2$.

Example Let E be ~~the~~ the splitting field for $p(x) = x^3 - 2$ over $\mathbb{Q}$.

$\mathbb{Q}(\sqrt[3]{2}, \varepsilon)$ $\varepsilon = \exp \frac{2\pi i}{3}$

Consider $\mathrm{Id} : \mathbb{Q} \longrightarrow \mathbb{Q}$

$p(x) = x^3 - 2 \qquad q(x) = x^3 - 2$

~~Then~~ Pick $\alpha = \sqrt[3]{2} \qquad \beta = \sqrt[3]{2}\,\varepsilon$

Then lift Id to an isom

$\mathbb{Q}(\sqrt[3]{2}) \longrightarrow \mathbb{Q}(\sqrt[3]{2}\,\varepsilon)$

Next factor pols

$p(x) = x^3 - 2 = (x - \sqrt[3]{2})\underbrace{(x - \sqrt[3]{2}\,\varepsilon)(x - \sqrt[3]{2}\,\varepsilon^2)}_{\tilde{p}(x)}$ still irr/$\mathbb{Q}$

$q(x) = x^3 - 2 = (x - \sqrt[3]{2}\,\varepsilon)\underbrace{(x - \sqrt[3]{2})(x - \sqrt[3]{2}\,\varepsilon^2)}_{\tilde{q}(x)}$.

Pick new roots

$\tilde{\alpha} = \sqrt[3]{2}\,\varepsilon \qquad \tilde{\beta} = \sqrt[3]{2}$

$\Rightarrow \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\,\varepsilon) \longrightarrow \mathbb{Q}(\sqrt[3]{2}\,\varepsilon, \sqrt[3]{2})$

$\sqrt[3]{2} \longmapsto \sqrt[3]{2}\,\varepsilon$

$\sqrt[3]{2}\,\varepsilon \longmapsto \sqrt[3]{2}$

We're done.

$\sqrt[3]{2} \longmapsto \sqrt[3]{2}\,\varepsilon$

$\varepsilon \longmapsto \varepsilon^{-1} = \varepsilon^2$