Splitting Fields

Defn Let $f \in F[x]$ have degree $n > 0$. Then an extn L/F is a splitting field of f over F if

(a) $f = c(x-\alpha_1)\cdots(x-\alpha_n)$, $c \in F$, $\alpha_i \in L$, and

(b) $L = F(\alpha_1, \ldots, \alpha_n)$.

Note Such L is the smallest field over which f splits completely

e.g. Splitting field of x^2+1 / $\mathbb{Q}$ is $\mathbb{Q}(i)$
/ $\mathbb{R}$ is $\mathbb{C}$
/ $\mathbb{C}$ is $\mathbb{C}$

e.g. Splitting field of x^4-2 / $\mathbb{Q}$ is $\mathbb{Q}(i, \sqrt[4]{2})$.

Thm Let $f \in F[x]$ have degree $n > 0$, and let L be a splitting field of f. Then $[L:F] \leq n!$.

Pf Proceed by induction on n. If $n=1$, $f = ax+b$ has root $-b/a \in F$, so $L = F$ and $[L:F] = 1 \leq 1!$.

Now suppose f has degree $n > 1$, $L = F(\alpha_1, \ldots, \alpha_n)$ a splitting field of f / F. If we write $f = (x-\alpha_1)g$, get $g \in F(\alpha_1)[x]$ and g has roots $\alpha_2, \ldots, \alpha_n$, so the splitting field of g over $F(\alpha_1)$ is L. By ind hyp, $[L:F(\alpha_1)] \leq (n-1)!$. Then $[L:F] = [L:F(\alpha_1)]\cdot[F(\alpha_1):F] \leq (n-1)![F(\alpha_1):F]$

But $[F(\alpha_1):F] = \deg(m_{\alpha_1, F})$ and $f(\alpha_1) = 0$ so $[F(\alpha_1):F] \leq n$

$\Rightarrow [L:F] \leq n!$. $\square$

Note The bound is sharp ($\mathbb{Q}(\omega, \sqrt[3]{2})$ / $\mathbb{Q}$ splits x^3-2) but not always realized ($\mathbb{Q}(\sqrt{2}, \sqrt{3})$ / $\mathbb{Q}$ splits $(x^2-2)(x^2-3)$ and $4 < 4!$).

Uniqueness:

$$\begin{array}{ccc} L_1 & & L_2 \\ | & & | \\ F_1 & \xrightarrow[\varphi]{\cong} & F_2 \end{array}$$

L_1 = splitting field of $f_1 \in F[x]$

L_2 = " " $f_2 \in F[x]$ where coeffs of f_2 are φ(coeffs f_1)

Thm $\exists$ iso $\bar{\varphi}: L_1 \to L_2$ with $\varphi = \bar{\varphi}|_{F_1}$.

Pf by ind'n on $n = \deg(f_1) = \deg(f_2)$. If $n=1$, $L_1 = F_1$, $L_2 = F_2$ and we can take $\bar{\varphi} = \varphi$. Now suppose $n > 1$. Then $L_1 = F(\alpha_1, \dots, \alpha_n)$ for α_i roots of f_1. Consider $F_1 \subseteq F_1(\alpha_1) \subseteq L_1$ where L_1 is a splitting field of $g_1 = f_1/(x-\alpha_1)$ over $F_1(\alpha_1)$.

Step 1 Let $h_1 \in F_1[x]$ be min poly of α_1 / F_1. Then

$$F_1(\alpha_1) = F_1[\alpha_1] \cong F_1[x]/(h_1), \quad \alpha_1 \mapsto x + (h_1).$$

Step 2 $\varphi: F_1 \cong F_2$ induces $\tilde{\varphi}: F_1[x] \cong F_2[x]$, $f_1 \mapsto f_2$, and $h_1 \mapsto h_2 := \tilde{\varphi}(h_1)$ irred factor of f_2. Roots of f_2 are $\beta_1, \dots, \beta_n \in L_2$ where β_1 is a root of h_2.

Step 3 Get $L_2 / F_2(\beta_1) / F_2$ with L_2 splitting $g_2 = f_2/(x-\beta_1)$.

Then $F_2(\beta_1) = F_2[\beta_1] \cong F_2[x]/(h_2)$, $\beta_1 \mapsto x + (h_2)$

Step 4 $\tilde{\varphi}$ induces $F_1[x]/(h_1) \cong F_2[x]/(h_2)$, $x + (h_1) \mapsto x + (h_2)$, so we get

$$\begin{array}{ccccc} L_1 & & & & L_2 \\ | & & & & | \\ F_1(\alpha_1) \cong F_1[x]/(h_1) & \cong & F_2[x]/(h_2) & \cong & F_2(\beta_1) \\ | & & & & \\ F_1 & \xrightarrow[\cong]{\varphi} & F_2 & & \end{array}$$

Step 5 Degree of $L_1 / F_1(\alpha_1)$ is $n-1$ so ind hyp produces $L_1 \cong L_2$ fitting into the diagram. $\square$

Cor If L_1, L_2 are splitting fields of $f \in F[x]$, then there is an iso $L_1 \xrightarrow{\cong} L_2$ which is the identity on F.

Pf Apply the thm to $\mathrm{id}: F \to F$. $\square$

Prop Let L be a splitting field of $f \in F[x]$, and suppose $h \in F[x]$ is irreducible with roots $\alpha, \beta \in L$. Then $\exists$ field iso $\sigma: L \to L$ that is identity on F, takes $\alpha \mapsto \beta$.

Pf Have $F(\alpha) = F[\alpha] \cong F[x]/(h) \cong F[\beta] = F(\beta)$

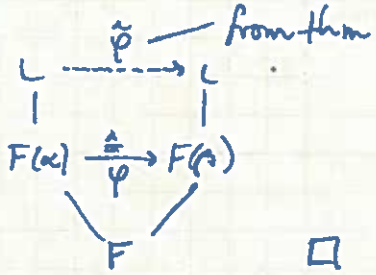
$\alpha \mapsto x + (h) \longleftarrow \beta$

φ

$\alpha \mapsto \beta$

id on F

Get the diagram of splitting fields



□

e.g. $L = \mathbb{Q}(\sqrt{2})$ is the splitting field of $x^2 - 2 \in \mathbb{Q}[x]$ which has roots $\pm\sqrt{2}$ so $\exists$ iso $L \to L$, $\sqrt{2} \mapsto -\sqrt{2}$, id on $\mathbb{Q}$.

Note Such σ is an elt of $Gal(L/F)$, the Galois group of L/F.

Normal Extensions

Q Given L/F, how can we tell if L is the splitting field of some $f \in F[x]$?

Prop Let L be the splitting field of $f \in F[x]$, and let $g \in F[x]$ be irred. If g has one root in L, then g splits completely over L.

Pf WLOG, f, g are monic. Then $L = F(\alpha_1, \dots, \alpha_n)$ where $f = (x-\alpha_1)\cdots(x-\alpha_n)$.

If $\beta \in L$ is a root of g, then g is the min'l poly of β/F since g is irred. & monic.

Have $L = F[\alpha_1, \dots, \alpha_n]$ so $\beta = h(\alpha_1, \dots, \alpha_n)$ for some $h \in F[x_1, \dots, x_n]$.

Now consider $s(x) = \prod_{\sigma \in \Sigma_n} (x - h(\alpha_{\sigma(1)}, \dots, \alpha_{\sigma(n)})) \in L[x]$.

Roots all in L, include β. Suffices to show $s \in F[x]$. TPS Why? (B/c then $g | s$, s splits completely.)

Consider $S(x) = \prod_{\sigma \in \Sigma_n} (x - h(x_{\sigma(1)}, \dots, x_{\sigma(n)}))$ with coeffs in $F[x_1, \dots, x_n]$.

This is clearly symmetric in $x_1, \dots, x_n$, so its expansion is of the form

$$S(x) = \sum_{i=0}^{n!} p_i(x_1, \dots, x_n) x^i$$

where each $p_i \in F[x_1, \dots, x_n]^{\Sigma_n}$. Since the α_i are roots of $f \in F[x]$, get $p_i(\alpha_1, \dots, \alpha_n) \in F$, so $S(x) \in F[x]$. □

e.g. $\mathbb{Q}(\sqrt[3]{2})$ is not the splitting field of any polynomial in $\mathbb{Q}[x]$:

$p_{\sqrt[3]{2}, \mathbb{Q}} = x^3 - 2$ is irred / $\mathbb{Q}$ but has roots $\omega\sqrt[3]{2}, \omega^2\sqrt[3]{2} \notin \mathbb{Q}(\sqrt[3]{2})$.

Defn An alg extn L/F is normal if every irred poly in $F[x]$ that has a root in L splits completely over L.

Aside Perhaps "equitable" would be a better term, but we are stuck with "normal."

HW L/F normal iff $m_{\alpha, F}$ splits completely $\forall \alpha \in L$.

Thm Suppose L/F. Then L is the splitting field of some $f \in F[x]$ iff L/F is normal and finite.

Pf ($\Rightarrow$) Finite by $n!$ bound on degree, just proved normal.

($\Leftarrow$) L/F normal and finite. By finiteness, $L = F(\alpha_1, \dots, \alpha_m)$ where each α_i alg / F. Let $p_i = m_{\alpha_i, F} \in F[x]$, set $f = p_1 \cdots p_m$.

Claim L is the splitting field of f.

Clearly f splits completely since each p_i has root α_i in L and L/F normal. Let L' be the subfield of L gen'd by F and the roots of f. Then $L = F(\alpha_1, \dots, \alpha_m) \subseteq L' \subseteq L$ so $L' = L$, and L is the splitting field of f over F. □