3/19

Tuesday, March 19, 2019 11:33

Theorem Let φ be an isomorphism $F_1 \longrightarrow F_2$.

Let $f_1 \in F_1[x]$ be irreducible, let $f_2 = \varphi(f_1) \in F_2[x]$.

Let α_1 be a root of f_1 (in some K_1/F_1)

Let α_2 be a root of f_2 (in some K_2/F_2).

Then φ extends to an isomorphism

$$\begin{array}{ccc} F_1(\alpha_1) & \longrightarrow & F_2(\alpha_2) \\ | & & | \\ F_1 & \longrightarrow & F_2 \end{array}$$

s.t. $\varphi(\alpha_1) = \alpha_2$.

Proof: $F_1(\alpha_1) \cong F_1[x]/(f_1)$ with $\alpha_1 \longleftrightarrow x \bmod f_1$.

$F_2(\alpha_2) \cong F_2[x]/(f_2)$ with $\alpha_2 \longleftrightarrow x \bmod f_2$.

$\varphi: F_1[x] \xrightarrow{\sim} F_2[x]$, $(f_1) \longmapsto (f_2)$ so φ induces iso.

$$F_1[x]/(f_1) \xrightarrow{\sim} F_2[x]/(f_2)$$
$$x \longmapsto x$$

Defn Let K/F be an extension, $\alpha_1, \alpha_2 \in K$ are said to be *conjugate* over F if $m_{\alpha_1,F} = m_{\alpha_2,F}$ (this is so if α_1, α_2 are roots of the same irr. poly).

Examples (over $\mathbb{Q}$): i and $-i$.

$\sqrt{2}$ and $-\sqrt{2}$

$\sqrt[3]{2}$, $\omega \cdot \sqrt[3]{2}$, $\omega^2 \cdot \sqrt[3]{2}$ (where $\omega = e^{2\pi i/3}$).

α has at most $\deg_F \alpha$ conjugates in K/F (including itself).

Let $K/L/F$, $\alpha \in K$.

$$\{\text{Conjugates of } \alpha \text{ over } L\} \subseteq \{\text{Conjugates of } \alpha \text{ over } F\}.$$

since $m_{\alpha,F} \mid m_{\alpha,F}$.

Example $F = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2})$, $\alpha = \sqrt[4]{2}$.

Conjugates of α over F are roots of $x^4 - 2$

so they're $\{\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}\}$.

Conjugates of α over L are roots of $x^2 - \sqrt{2}$

So they're $\{\pm \sqrt[4]{2}\}$.

Splitting field of f.

Def Let $f \in F[x]$. An extension K/F is a splitting field of f if f completely splits in K:

$$f(x) = a(x-\alpha_1)\cdots(x-\alpha_n) \quad \text{where } \alpha_i \in K$$

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

If so, and E/K is an extension of K, then any root of f in E is in K as well.

(K contains "all roots of f").

Theorem: $\forall f \in F[x]$, a splitting field K/F exists and is unique up to isomorphism of extensions (that is, Id_F on F and maps roots of f to roots of f).

$[K:F] \leq n!$ where $n = \deg f$.

Example ① Splitting field of $x^2+1 \in \mathbb{R}[x]$ is $\mathbb{C} = \mathbb{R}(i)$.

② " " $x^2 - 2 \in \mathbb{Q}[x]$ is $\mathbb{Q}(\sqrt{2})$.

③ $f = x^n - 1 \in \mathbb{Q}[x]$. roots of f are $e^{2\pi i k/n}$ for $k = 0, \ldots, n-1$
$\qquad\qquad = \omega^k$ where $\omega = e^{2\pi i/n}$.

Splitting field is $\mathbb{Q}(\omega)$.

④ $f = x^n - 2 \in \mathbb{Q}[x]$. roots are $\omega^k \alpha$ for $k = 0, \ldots, n-1$.
$\alpha = \sqrt[n]{2}$.

Splitting field is $\mathbb{Q}(\alpha, \omega)$

⑤ $f = (x^n - 2)(x^n - 3)$. Splitting field is $\mathbb{Q}(\sqrt[n]{2}, \sqrt[n]{3}, \omega)$.

<u>proof</u>: Let $f = g_1 \cdots g_k$ where $g_i \in F[x]$ are irreducible.

Let α_1 be a root of g_1 (in some extension of F).

Then over $F(\alpha_1)$, $f(x) = (x - \alpha_1) f_1(x)$, $\deg f_1 = \deg f - 1$.

By induction on $\deg f$, $\exists$ a splitting field K of $f_1 \in F(\alpha_1)[x]$.

Over K, $f_1(x) = a(x - \alpha_2) \cdots (x - \alpha_n)$, so $f(x) = a(x - \alpha_1) \cdots (x - \alpha_n)$.

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

So K is a splitting field of f.

Let K_1, K_2 be splitting field of f (over F).

let $\alpha_1, \ldots, \alpha_n$ be roots of f in K_1
$\beta_1, \ldots, \beta_n$ be roots of f in K_2.

$$f(x) = a(x-\alpha_1)\cdots(x-\alpha_n)$$

$$= g_1(x)\cdot\cdots\cdot g_k(x) \longleftarrow \text{irr. over } F.$$

$$= a(x-\beta_1)\cdots(x-\beta_n)$$

Assume α_1 is a root of g_1

β_1 is a root of g_1

then $\exists\ \varphi : F(\alpha_1) \xrightarrow{\sim} F(\beta_1)$ s.t. $\alpha_1 \overset{\varphi}{\longmapsto} \beta_1$.

$$\begin{tikzcd} F(\alpha_1) \arrow[rr, "\sim"] & & F(\beta_1) \\ & F \arrow[ul, no head] \arrow[ur, no head] & \end{tikzcd}$$

Let $f(x) = (x-\alpha_1) f_1(x)$, $f_1 \in F(\alpha_1)[x]$.

$f(x) = (x-\beta_1)\tilde{f}_1(x)$, $\tilde{f}_1 \in F(\beta_1)[x]$.

Then $f_1 = \dfrac{f}{x-\alpha_1}$, $\tilde{f}_1 = \dfrac{f}{x-\beta_1}$,

So $\varphi : f_1 \longmapsto \tilde{f}_1$.

over $F(\alpha_1)$, $f_1 = h_1 \cdot\cdots\cdot h_\ell$

over $F(\beta_1)$, $\tilde{f}_1 = \tilde{h}_1 \cdot\cdots\cdot \tilde{h}_\ell$ s.t. $\tilde{h}_i = \varphi(h_i)$.

$\vdots$

Generalization

Let $\varphi : F_1 \xrightarrow{\sim} F_2$, $f_1 \in F_1[x]$, $f_2 = \varphi(f) \in F_2[x]$,

K_1 is a splitting field of f_1

K_2 is a splitting field of f_2.

Then $K_1 \cong K_2$ s.t.

$$\begin{tikzcd} K_1 \arrow[r] \arrow[d, dash] & K_2 \arrow[d, dash] \\ F_1 \arrow[r] & F_2 \end{tikzcd}$$

is commutative

& roots of F_1 go to roots of F_2.

⋮

Use induction on deg f with the generalization. □