CUERPOS DE DESCOMPOSICIÓN

ALGEBRA3 2017
CLASE 4 - 25/8/17 1

Proposición: Sea $f \in K[X]$ no cte. Existe un cuerpo E extensión de K que contiene (al menos) una raíz de f.

Demostración Spg podemos suponer f irreducible (de grado ≥ 1)

$K[X]/\langle f \rangle$ es cuerpo por ser $\langle f \rangle$ maximal

Consideramos
$$\pi_f : K[X] \to K[X]/\langle f \rangle$$
$$g \mapsto \pi_f(g) = \overline{g} = \overline{r_f(g)}$$

$(\overline{g} = \overline{h} \iff f \mid g-h)$

- $\pi_f(g+h) = \pi_f(g) + \pi_f(h)$ pues $\overline{g+h} = \overline{g} + \overline{h}$
- $\pi_f(gh) = \pi_f(g)\pi_f(h)$ pues $\overline{gh} = \overline{g}\,\overline{h}$
- $\pi_f(1) = \overline{1}$

Observar que $\forall a \in K$, $\pi_f(a) = \overline{a}$ satisface

$\pi_f(a) = \pi_f(b) \iff a = b$ pues $f \mid a-b \iff a = b$

luego $K \simeq \pi_f(K) \subseteq K[X]/\langle f \rangle$ $\therefore$ $K \hookrightarrow K[X]/\langle f \rangle$

Afirmación: Clase $\overline{x}$ de x satisface $f(\overline{x}) = \overline{0}$ en $K[X]/\langle f \rangle$

Si $g = \sum a_i x^i$, ent. $\pi_f(g) = \overline{g} = \overline{\sum a_i x^i} = \sum \overline{a_i}\, \overline{x}^i$

$= \sum a_i \overline{x}^i \Rightarrow$ $\overline{g(x)} = g(\overline{x})$.

Tenemos $\pi_f(f) = \underbrace{\overline{f(x)}}_{= \overline{0}} = f(\overline{x})$ $\therefore$ $f(\overline{x}) = \overline{0}$

$\overline{x}$ es raíz de f en el cuerpo $K[X]/\langle f \rangle$, extensión de f.

Observación

Sea $\alpha \in E$ raíz de $f \in K[X]$ irreducible.

Entonces $K[\alpha] \simeq K[X]/\langle f \rangle$

Demostración

$$K[X] \xrightarrow{\phi} K[\alpha]$$
$$X \longmapsto \alpha$$
$$g(X) \longmapsto g(\alpha)$$

$Ker(\phi) = \{ g \in K[X] / g(\alpha) = 0 \} = \langle f \rangle$ pues f irreducible

$\Rightarrow K[X]/\langle f \rangle \simeq K[\alpha]$.

Corolario: Si α, β son raíces del mismo pol $f \in K[X]$ irreducible,

entonces $K(\alpha) = K[\alpha] \simeq K[\beta] = K(\beta)$

pues $K[\alpha] \overset{\varphi}{\simeq} K[X]/\langle f \rangle \overset{\psi^{-1}}{\simeq} K[\beta]$

$\alpha \longmapsto \overline{X} \longmapsto \beta$

Este isomorfismo es un isomorfismo de cuerpos que además satisface $\sigma(a) = a, \forall a \in K$. Es lo que se llama K-morfismo (o K-inmersión para recalcar que siempre es mono)

Además $\sigma(\alpha) = \beta$ pues $\alpha \mapsto \beta$

Definición (K-morfismo o K-inmersión)

Sean E/K, F/K extensiones

$\sigma: E \to F$ es un K-morf (de cuerpos) o una K-inmersión

si σ es morfismo de cuerpos ($\sigma(1_E) = 1_F$, $\sigma(\alpha+\beta) = \sigma(\alpha) + \sigma(\beta)$ y $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$)

que además satisface $\sigma(a) = a, \forall a \in K$ (o sea $\sigma|_K = id_K$)

Las K-inmersiones $\sigma: E \to F$ se extienden en forma natural a $\sigma: E[X] \to F[X]$

Observación: Una K-inmersión es en particular una t.l de los K-ev E y F, o sea un morfismo de K-álgebras,

pues $\sigma(a\alpha) = \sigma(a)\sigma(\alpha) = a\,\sigma(\alpha)$, $\forall a \in K, \alpha \in E$

Satisface; para $\alpha \in E$, $f \in K[X]$, $f = \sum a_i x^i$

$$\sigma(f(\alpha)) = \sigma\left(\sum a_i \alpha^i\right) = \sum a_i \sigma(\alpha)^i = f(\sigma(\alpha)), \ \forall \alpha \in E$$

Corolario: Sea $\sigma : K(\alpha) \to F$ una K-~~mor~~ inm / $\sigma(\alpha) = \beta$

entonces σ queda determinado:

$$\sigma\left(\frac{f(\alpha)}{g(\alpha)}\right) = \frac{f(\beta)}{g(\beta)} \quad \text{donde } g(\beta) \neq 0 \text{ pues } g(\alpha) \neq 0 \text{ y } \sigma \text{ iny}$$

Teorema: Sean $\alpha, \beta \in E$ alg $/K$

$\exists$ una K-inmersión $\underset{K[\alpha] \to K[\beta]}{\sigma}$ / $\sigma(\alpha) = \beta \iff f(\alpha, K) = f(\beta, K)$

(y resulta un K-isomorfismo)

Demostración:

($\Rightarrow$) $\sigma(\alpha) = \beta \Rightarrow \sigma(f(\alpha)) = f(\beta)$

Sea $f = f(\alpha, K)$: $\sigma(f(\alpha)) = \sigma(0) = 0 = f(\beta)$

$\Rightarrow f(\beta, K) \mid f(\alpha, K)$ y recíprocamente.

($\Leftarrow$) Sup $f(\alpha, K) = f(\beta, K)$, ent. $K[\alpha] \simeq K[\beta]$ y $\sigma : \alpha \mapsto \beta$

Cuerpo de descomposición de un polinomio

Definición (cuerpo de descomposición) Sea $f \in K[X]$, $\mathrm{gr}(f) \geq 1$

Se dice que E/K es un cuerpo de descomposición de f si

1. f se factoriza linealmente en $E[X]$ (i.e. $f = a_d(X - \alpha_1) \dots (X - \alpha_d)$, con $\alpha_i \in E$, $1 \leq i \leq d$: E contiene todas las raíces de f)
2. Si $F \subseteq E$ es un cuerpo tq f se factoriza linealmente en $F[X]$, entonces $F = E$.

Se tiene $E = K(\alpha_1, .., \alpha_d) = K[\alpha_1, .., \alpha_d]$ y es por lo tanto finita.

$X^2+1/\mathbb{Q}$

$X^2+1/\mathbb{R}$

Ejemplos: $f = X^3 - 2 \in \mathbb{Q}[X]$: $E = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$, $f = X^p - 1$ $\quad (X^2-2)(X^2-3)/\mathbb{Q}$

Teorema (Existencia y unicidad del cuerpo de desc de f)

① Dado $f \in K(X)$, existe un cuerpo de desc de f

② Dos cuerpos de desc de f son K-isomorfos

Demostración

① Inducción en $gr(f)$.

$gr\, f = 1$ ✓ $\quad K(X)/_{\langle f \rangle} = K$

$gr\, f > 1$:

Sea $p | f$ irreducible. Entonces $K[X]/_{\langle p \rangle}$ contiene una raíz α_1 de f

$$K[X]/_{\langle p \rangle} = K[\alpha_1]$$

$$\begin{array}{c} K[\alpha_1] \\ | \\ K \end{array} \qquad f = \cancel{gk}\,(X-\alpha_1)\, g \text{ con } g \in K[\alpha_1][X] \text{ de grado } n-1$$

Existe un cuerpo de desc de g, E, sobre $K[\alpha_1]$

$\Rightarrow E = K[\alpha_1][\alpha_2, .., \alpha_d] = K[\alpha_1, .., \alpha_d]$ es cuerpo de desc de f/K.

② Usaremos la siguiente proposición (importante)

PROPOSICIÓN

Sea $\sigma: E_1 \to F_1$ iso de cuerpos.

Sea E cpo de desc de $f \in E_1[X] / E_1$ y F cualquier extensión de F_1 donde $\sigma(f)$ se factoriza linealmente.

Entonces existe $\bar{\sigma}: E \to F$ morf de cpos / $\bar{\sigma}|_{E_1} = \sigma$.

$$\begin{tikzcd} E = E_1[\alpha_2, .., \alpha_n] \arrow[r, dashed, "\bar{\sigma}"] \arrow[d, dash] & F \arrow[d, dash] \\ E_1 \arrow[r, "\sigma"'] & F_1 \end{tikzcd}$$

Demostración: Por inducción en $gr(f)$

- $gr(f) = 1 \Rightarrow E = E_1$ y $\bar{\sigma} = \sigma$
- $gr(f) > 1$:

Empieza abajo de doble raya:

$$\begin{tikzcd} E_1[X] \arrow[r, "\sigma"] \arrow[d, "\Pi_h"'] & F_1[X] \arrow[d, "\Pi_{\sigma(h)}"] \\ E_1[X]/\langle h\rangle \arrow[r, dashed, "\tilde\sigma"] & F_1[X]/\langle\sigma(h)\rangle \end{tikzcd} \quad (*)$$

Se define $\tilde\sigma(\Pi_h(g)) := \Pi_{\sigma(h)} \circ \sigma(g)$

¿bien definida?

$\Pi_h(g_1) = \Pi_h(g_2) \overset{\Rightarrow}{\Leftrightarrow} h \mid g_1 - g_2$

$\overset{\Rightarrow}{\Leftrightarrow} \sigma(h) \mid \sigma(g_1) - \sigma(g_2) \overset{\Rightarrow}{\Leftrightarrow} \Pi_{\sigma(h)} \circ \sigma(g_1) = \Pi_{\sigma(h)} \circ \sigma(g_2)$

por ser σ iso para vuelta

¿mono? Sea $\Pi_h(g) \in \ker \tilde\sigma$. qpq $\Pi_h(g) = 0$ o sea $h \mid g$.

$\tilde\sigma \circ \Pi_h(g) = \Pi_{\sigma(h)}(\sigma(g)) = 0$

$\Leftrightarrow$ ~~$\sigma(g)$~~ $\sigma(h) \mid \sigma(g) \underset{\sigma \text{ iso}}{\Leftrightarrow} h \mid g$

¿epi? Sea $\Pi_{\sigma(h)}(g') \in F_1[X]/\langle\sigma(h)\rangle$

Como σ epi, $\exists\, f \in E_1[X] / \ g' = \sigma(g)$

o sea $\Pi_{\sigma(h)}(g') = \Pi_{\sigma(h)} \sigma(g) = \tilde\sigma(\underbrace{\Pi_h(g)}) \checkmark$

Sea α raíz de f en E y $h \mid f \in E_1[X]$ un factor irreducible de f tq $h(\alpha) = 0$

Luego $\sigma(h)$ es irreducible en $F_1[X]$ (pues $E_1 \simeq F_1$)

y podemos considerar el diagrama de arriba $(*)$

Se tiene $\tilde\sigma$ iso, con $\tilde\sigma|_{E_1} = \sigma$

Así: sea $\beta = \sigma(\alpha)$ raíz de $\sigma(h)$.

Se tiene

$$E_1[\alpha] \simeq E_1[X]/_{h} \overset{\tilde{\sigma}}{\simeq} F_1[X]/_{\sigma(h)} \simeq F_1[\beta]$$

$\tilde{\varphi}$ satisface $\varphi|_{E_1} = \sigma$

Tenemos entonces

$$\begin{tikzcd} E \arrow[r, dashed, "\bar{\sigma}"] \arrow[d, no head] & F \arrow[d, no head] \\ E_1[\alpha] \arrow[r, "\tilde{\sigma}"'] \arrow[d, no head] & F_1[\beta] \arrow[d, no head] \\ E_1 \arrow[r, "\sigma"'] & F_1 \end{tikzcd}$$

E cpo de desc de $f_1 = f/x-\alpha$ sobre $E_1[\alpha]$, de grado $n-1$ y F contiene todas las raíces de $\tilde{\sigma}(f_1) = \tilde{\sigma}(f)/x-\beta$

$\Rightarrow$ $\tilde{\sigma}$ se extiende a $\bar{\sigma}: E \to F$ inmersión

~~PROPOSICIÓN Sea E cpo de desc de $f \in K[X]$ sobre K~~
~~y $\sigma: E \to E$ K-endomorfismo de E. Entonces~~
~~σ es K-automorfismo de E~~
~~(Veremos más adelante que vale para extensiones algebraicas)~~

~~Demostración~~

PROPOSICIÓN: Sea E/K ext. finita y $\sigma: E \to E$ K-endo de E.
Entonces σ es K-auto de E
(Veremos luego que vale para exts algs)

Demostración: Como σ es morf de K-e.v, entonces $\sigma(E)$ es subespacio de E pero $\sigma(E) \simeq E$, tiene la misma dimensión que E $\Rightarrow$ $\sigma(E) = E$ ∎

Unicidad del cuerpo de descomposición

En la prop sea F cpo de desc de $\sigma(f)$ sobre F_1. Entonces
$\sigma_1 : E \to F$ y $\sigma_2 : F \to E$

$\Rightarrow$ $\sigma_2 \circ \sigma_1$ es endo de E $\Rightarrow$ $\sigma_1 \circ \sigma_2$ es auto de E

y $\sigma_2 \circ \sigma_1$ auto de F $\Rightarrow$ σ_1, σ_2 isomorfismos

$$\begin{tikzcd} E \arrow[rr, "\cong"] & & F \\ & K \arrow[ul, dash] \arrow[ur, dash] & \end{tikzcd}$$

$E_1 = F_1 = K$, $\sigma = id_K$.

$\boxtimes$

Observación:

Sea E/K cpo de desc de $f \in K[X]$ de grado n

(1) Entonces $\forall \sigma : E \to E$ K-endo de E.

Entonces σ permuta las raíces de f

(2) $[E : K] \leq n!$

$$\begin{tikzcd} E = K[\alpha_1, \alpha_2, \ldots, \alpha_n] \arrow[d, dash, "\leq (n-1)!"] \\ K[\alpha_1] \arrow[d, dash, "\leq n"] \\ K \end{tikzcd}$$

Pensar si sale $[E : K] \mid n!$

Notaciones que vamos a adoptar

$\mathrm{Hom}(E/K, F/K) = \{\sigma : F \to K,\ K\text{-inmersiones}\}$

$\mathrm{End}(E/K) = \{\sigma : E \to E,\ K\text{-inmersiones}\}$

$\mathrm{Gal}(E/K) = \{\sigma : E \to E,\ K\text{-automorfismos}\}$

Vimos que si E/K es finita, entonces $\mathrm{End}(E/K) = \mathrm{Gal}(E/K)$.