Álgebra Moderna III : 11 Septiembre

Clase pasada: Campos de descomposición

$$\begin{tikzcd} L \arrow[r, dotted, "\overline{\varphi}"] \arrow[d, dash] & M \arrow[d, dash] \\ F \arrow[r, equal, "id."'] & F \end{tikzcd}$$

$\exists$ isomorfismo $\overline{\varphi}_{|F} = Id.$

Hoy: Extensiones normales

$$\begin{matrix} L \\ | \\ F \end{matrix}$$ campo de descomposición de algún polinomio

Pregunta:

¿Cuántos automorfismos

$$\begin{tikzcd} L \arrow[rr, "\cong"] \arrow[dr, dash] & & L \arrow[dl, dash] \\ & F & \end{tikzcd}$$

$\varphi: L \xrightarrow{\cong} L$ t.q. $\varphi_{|F} = Id$

existen?

¿Existe un número finito de ellos?

¿Qué le haces a las raíces de polinomios?

↳ i.e. ¿raíces van a raíces?

Una respuesta parcial es:

Proposición: $\begin{array}{c} L \\ | \\ F \end{array}$ campo de descomposición de f.

Supongamos $h \in F[x]$ irreducible y con raíces α y β en L. Entonces, existe un automorfismo $\varphi : L \xrightarrow{\cong} L$ t.q. $\varphi_{|F} = Id$. y manda $\alpha \mapsto \beta$.

Demostración: h es el polinomio mínimal de α y β, de ahí

$$\begin{tikzcd} F(\beta) \arrow[r, phantom, "\cong"] & F[x]/h \arrow[r, phantom, "\cong"] & F(\alpha) \arrow[ll, bend right, "\varphi"'] \\ \beta \arrow[r, mapsto] & x+h & \alpha \arrow[l, mapsto] \end{tikzcd} \quad \left.\right\} \quad \begin{array}{l} \varphi(\alpha) = \beta \\ \varphi_{|F} = Id. \end{array}$$

si
$$\begin{tikzcd} L \arrow[r, dashed, "\bar{\varphi}"] & L \arrow[d, dash] \\ F(\alpha) \arrow[u, dash] \arrow[r, "\varphi"'] & F(\beta) \end{tikzcd}$$
campo de descomposición de $f/F(\alpha)$ ó $/F(\beta)$

entonces el teorema pasado nos dá el isomorfismo que buscamos.

(Raíces vana Raíces)

---

si en $\begin{matrix} L \\ | \\ F \end{matrix}$ campo de descomposición de $g \in F[x]$ y $\alpha \in L$ es raíz de un polinomio irreducible $f \in F[x]$

¿es posible que ninguna otra raíz de f esté en L?

si este es el caso, para un $\varphi : \begin{tikzcd} L \arrow[rr, "\cong"] & & L \\ & F \arrow[ul, dash] \arrow[ur, dash] & \end{tikzcd}$

tal que $\varphi|_F = Id$ ¿Qué pasa con $\varphi(\alpha)$? ...

Respuesta:

<u>Teorema</u>:

$$\begin{array}{c} L \\ | \\ F \end{array}$$

campos de descomposición de $f \in F[x]$.

Si $g \in F[x]$ es irreducible y tiene una raíz en L,

entonces todas sus raíces están en L.

<u>Demostración</u>:

$$f = (x-\alpha_1)\cdots(x-\alpha_n) \text{ en } L$$

$$g(\beta) = 0 \quad \text{con } \beta \in L = F[\alpha_1, \dots, \alpha_n]$$

por demostrar que toda raíz de g está en L.

$$S(x) = \prod_{\sigma \in S_n} (x - h(\alpha_{\sigma(1)} \cdots \alpha_{\sigma(n)}))$$

$$= \prod_{\sigma \in S_n} (x - h(\alpha_{\sigma(1)}, \dots, \alpha_{\sigma(n)}))$$

◆◆◂

$\sigma = id$ dice

$$x - h(\alpha_1,\dots,\alpha_n) = x - \beta$$

asumamos por notación.

$$S(\beta) = 0 \Longrightarrow$$

$g \mid S(x)$ pues g es el polinomio minimal de β.

pero $S(x) = (x - h(\alpha_1,\dots,\alpha_n))(x - h(\alpha_{\sigma_1(1)}\cdots\alpha_{\sigma_1(n)}))\cdots$

evidentemente factoriza en L.

$\Rightarrow$ g factoriza en L. $\blacksquare$

EJER: Esta prueba tiene un <u>hueco</u>.
¿Cuál es?

¡Resolverlo!

<u>Def.</u> Una $\begin{array}{c} L \\ | \\ F \end{array}$ extensión se dice NORMAL si todo polinomio irreducible$/F$ que tenga una raíz en L, factoriza en términos lineales en L.

CORO: $\begin{array}{c} L \\ | \\ F \end{array}$ extensión campo de descomposición. $\Longleftrightarrow$ normal & finita.

Demostración: $\Rightarrow$ ✓

$\Leftarrow$) finita (grado n) : $L = F(\alpha_1, \ldots, \alpha_n)$ α_i alg$/F$.

Sea

$P_i(x) =$ polinomio minimal de α_i $\Rightarrow$

$f = P_1 \cdots P_n$ & L es el campo de descomposición de f.

Cada

* p_i factoriza en términos lineales en L (normalidad)

$\Rightarrow$ f factoriza en términos lineales en L.

*

$$L = F(\alpha_1, \dots, \alpha_n) < K < L$$

$\boxed{\text{campo } F \oplus \text{ raíces de } f.}$

$$\Rightarrow \quad K = F(\alpha_1, \dots, \alpha_n)$$

$\Rightarrow$ $K = L$ campo de descomposición.

Pregunta: si f es irreducible$/F$ & α una raíz de f en L. ¿Puede α tener multiplicidad mayor a 1?