Álgebra Moderna III: 16 octubre

Clase pasada: Grupo de Galois

Hoy: Permutaciones de raíces de $f \in F[x]$

↳ ¿Qué permutaciones se permiten?

Supongamos $f \in F[x]$ y sea L su campo de descomposición.

entonces en $L[x]$

$$f = a_0(x-\alpha_1)\cdots(x-\alpha_n), \quad a_0 \neq 0$$

$\alpha_1, \ldots, \alpha_n \in L$ distintos

así

$$\mathrm{Gal}(L \setminus F) \longrightarrow S_n$$

$$\sigma \longmapsto \{\alpha_1, \ldots, \alpha_n\} \longmapsto \{\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}\}$$

donde $\sigma(\alpha_i) = \alpha_{\overline{\sigma}(i)}$ para algún $\overline{\sigma}(i) \in \{1, \dots, n\}$

$$\overline{\sigma} : \{1, \dots, n\} \longrightarrow \{1, \dots, n\}$$

es injectiva pues las raíces son todas distintas (Extensión Separable).

Propo: $Gal(L \setminus F) \longrightarrow S_n$ es un homomorfismo de grupos injectivo.

Demostración: $*$ homomorfismo:

$$\sigma_1 \circ \sigma_2 (\alpha_i) = \sigma_1 (\alpha_{\sigma_2(i)}) = \alpha_{\sigma_1 \sigma_2 (i)}$$

$*$ es injectivo pues ψ está determinado por su efecto en $\alpha_1, \ldots, \alpha_n$ pues $L = F(\alpha_1, \ldots, \alpha_n)$. ☐

Corolario: $|Gal(L \setminus F)|$ divide a $n!$

¿Qué relación hay entre $[L:F]$ y $|Gal(L \setminus F)|$?

Teorema: L campo de descomposición de un polinomio $f \in F[x]$ separable. Entonces

$$|Gal(L \setminus F)| = [L:F]$$

Demostración: Sabemos $L = F(\alpha_1, \ldots, \alpha_n)$

con α_i's raíces de $f \in F[x]$.

SUPONGAMOS EXISTE $\beta \in L$ tal que

$L = F(\beta)$. (además separable)

Sea $h \in F[x]$ el polinomio minimal de β.

$\Rightarrow [L:F] = \text{grado}(h)$, denotemoslo por m, necesitamos demostrar que $|Gal(L \setminus F)|$ ~~tiene~~ es igual a grado(h).

Observar $\{\beta = \beta_1, \ldots, \beta_m\} = \underset{\text{de } h}{\text{raíces}} \in L$

por normalidad de L.

Más aún, existe $\varphi_i : L \longrightarrow L$ tal que
Isomorfismo

$$\varphi_i(\beta) = \beta_i \quad \text{y} \quad \varphi_i|_F = Id.$$

$$\Rightarrow \{\varphi_1, \dots, \varphi_m\} \leq Gal(L \setminus F)$$

$$\Rightarrow |Gal(L \setminus F)| \geq m. \quad \text{Sin embargo,}$$

Sea $\tau \in Gal(L \setminus F)$, entonces

$\tau(\beta)$ determina totalmente a τ

y además $\tau(\beta) \in \{\beta_1, \dots, \beta_m\}$

$$\Rightarrow \tau = \varphi_k \quad \text{para algún } k \in \{1, \dots, m\}$$

$$\Rightarrow |Gal(L \setminus F)| = [L : F]$$

El resultado crucial aquí es que existe $\beta \in L$, tal que

$$L(\alpha_1, \ldots, \alpha_m) = L(\beta).$$

Regresaremos a este teorema en una clase (o dos).

OBSERVACIÓN: L campo de descomposición de $f \in F[x]$ / F

$\Rightarrow [F\,L]$ divide a $n!$ donde

$n = \text{grado}(f)$.

Retomando: ¿Qué permutaciones de las raíces de $f \in F[x]$ se permiten?

más aún, ¿qué tipo de subgrupo es $Gal(L\backslash F)$ de S_n?

Teorema (Jordan 1870). Sea L el campo de descomposición de $f \in F[x]$ un polinomio separable de grado n. Entonces

$Gal(L\backslash F) < S_n$ es transitivo

sii f es irreducible/F.

Demostración: ($\Leftarrow$) f irreducible

$$\Rightarrow F[x]/\langle f\rangle \cong F(\alpha) \cong F(\beta) \cong F[x]/\langle f\rangle$$

con α & β raíces de f

y existe $\varphi \in Gal(L\backslash F)$ tal que $\alpha \mapsto \beta$.

$\Rightarrow$) $Gal(L \setminus F) < S_n$ transitivo

Supongamos h es un factor no trivial de f.

$\Rightarrow \exists\ \alpha$ raíz de f que anula también a h. i.e $h(\alpha) = 0$.

para cualquier $j \in \{1, \dots, n\}$ $n = \text{grado}(f)$

existe $\varphi_j(\alpha) \in \{\text{raíces de } h\}$ con $\varphi_j \in Gal(L \setminus F)$

$\Rightarrow$ grado$(h) \geq$ grado(f)

$\Rightarrow h = af \quad a \in F^*$

$\Rightarrow f$ irreducible pues solo tiene factores triviales. $\blacksquare$