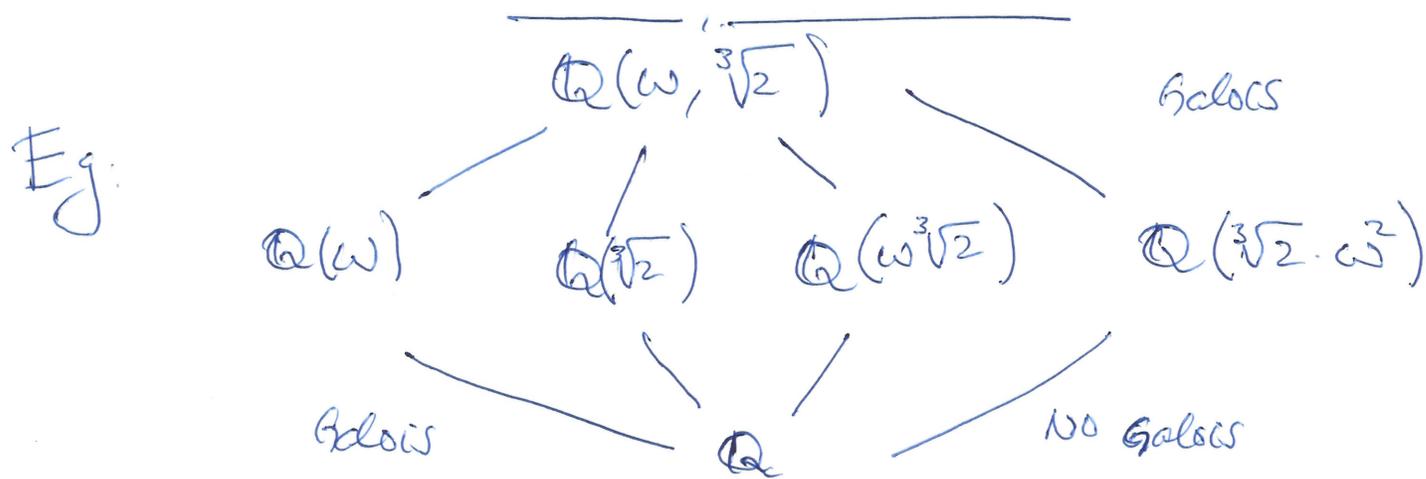


Algebra Moderna III : 12 noviembre

Clase pasada: Correspondencia de Galois: Campos fijados por subgrupos.

Hoy: Campos conjugados & subgp normales.



- $\mathbb{Q}(\omega)$ conjugado a si mismo

- $\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\omega^3 \sqrt[3]{2}), \mathbb{Q}(\omega^2 \sqrt[3]{2})$ conjugados

- $\text{Gal}(\mathbb{Q}(\omega, \sqrt[3]{2}) \setminus \mathbb{Q}) \cong \text{AGL}(\mathbb{F}_3)$

Lema: L
 $|$ extensiones de
 k campos finitos. Entonces
 $|$
 F a) $\text{Gal}(L \setminus k) < \text{Gal}(L \setminus F)$

b) si $\sigma \in \text{Gal}(L \setminus F)$, entonces

$$\text{Gal}(L \setminus \sigma k) = \sigma \text{Gal}(L \setminus k) \sigma^{-1} \text{ en } \text{Gal}(L \setminus F)$$

Demostración: a) EJERCICIO.

b)

$$\gamma \in \sigma \text{Gal}(L \setminus k) \sigma^{-1} \quad \beta \in \sigma \cdot k$$

$$\hookrightarrow \gamma = \sigma \cdot \tau \cdot \sigma^{-1} \quad \text{con } \tau \in \text{Gal}(L \setminus k)$$

$$\begin{aligned} \gamma(\beta) &= \sigma \circ \tau \circ \sigma^{-1}(\beta) \\ &= \sigma \circ \tau \circ \sigma^{-1}(\sigma(\alpha)) \\ &= \sigma \circ \tau(\alpha) \\ &= \sigma(\alpha) = \beta \end{aligned}$$

entonces

$$\sigma \text{Gal}(L \setminus K) \sigma^{-1} \subseteq \text{Gal}(L \setminus \sigma K)$$

para $\sigma|_K = \text{Id}$.

En la dirección opuesta $\sigma^{-1} \sigma(\alpha) = \sigma^{-1} \sigma(\alpha) = \alpha$.

Teoremas:



Extension de Galois

entonces las siguientes son equivalentes:

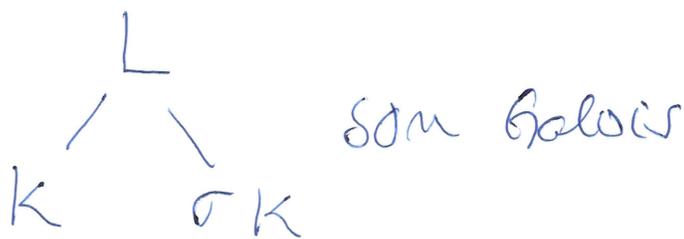
- a) $K = \sigma K \quad \forall \sigma \in \text{Gal}(L \setminus F)$
- b) $\text{Gal}(L \setminus K) \triangleleft \text{Gal}(L \setminus F)$
- c) $F \subseteq K$ es Galois.

Demostración: (a) \Rightarrow (b) Lema anterior

(b) \Rightarrow (a) si $\text{Gal}(L \setminus K) \triangleleft \text{Gal}(L \setminus F)$ &
 $\sigma \in \text{Gal}(L \setminus F)$ entonces (lema)

$$\text{Gal}(L \setminus K) = \sigma \text{Gal}(L \setminus K) \sigma^{-1} = \text{Gal}(L \setminus \sigma K)$$

pero



\Rightarrow

$K =$ campo fijado por $\text{Gal}(L \setminus K)$
 $\sigma \cdot K =$ " " " $\text{Gal}(L \setminus \sigma K)$

$\Rightarrow K = \sigma \cdot K$ como deseábamos.

(a) \Rightarrow (c) Tenemos que probar que K es
normal y separable $\begin{matrix} K \\ | \\ F \end{matrix}$

Campo de
 descomposición
 de $f \in F[X]$.

Tomemos $\alpha \in K$. Su polinomio minimal
 (hasta por mult. por una $\alpha \in F$)

$$\text{es } h(x) = \prod_{i=1}^r (x - \alpha_i)$$

II

$$\text{con } \alpha_i = \sigma_i(\alpha) \quad \sigma_i \in \text{Gal}(L/F)$$

observar $\sigma_i(\alpha) = \sigma_i(K) = K$ por hipótesis.

\Rightarrow todas las raíces de $h(x) \in F[x]$ están en K .

\Rightarrow K normal. Separable es claro.

$$(c) \Rightarrow (a) \quad \alpha \in K \quad \sigma \in \text{Gal}(L/F)$$

y tomemos su polinomio minimal $/F$.

$$\Rightarrow \sigma(\alpha) \in \sigma K \\ \in K \quad \leftarrow \text{por normalidad}$$

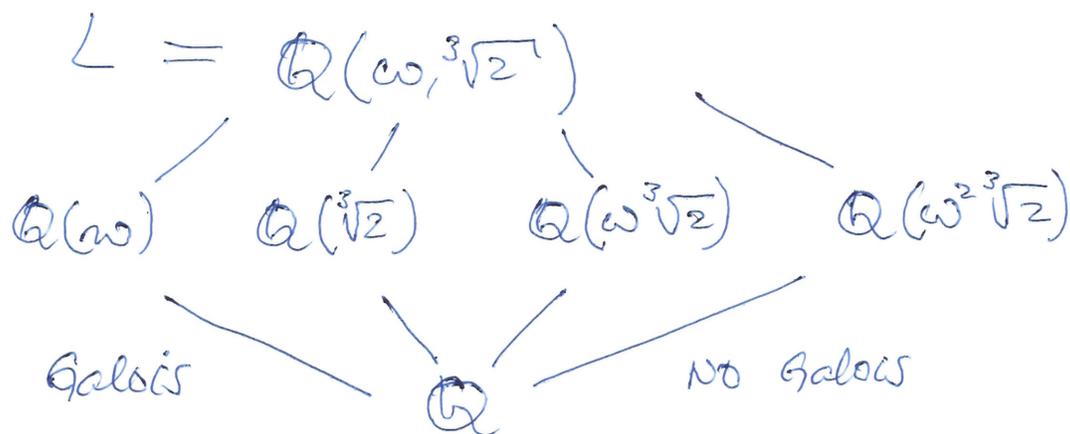
$$\Rightarrow \sigma K \subset K, \text{ pero } [K : \sigma K] = 1$$

$$\Rightarrow \sigma K = K \text{ como deseábamos}$$

(usamos separabilidad?)



Example



$$\text{Gal}(L \setminus \mathbb{Q}) \cong \mathbb{Z}_3 \rtimes \mathbb{Z}_3^* \cong \text{AGL}(\mathbb{Z}_3) = \{a\alpha + b \mid$$

$$\left. \begin{array}{l} a \in \mathbb{Z}_3^* \\ b \in \mathbb{Z}_3 \end{array} \right\}$$

orden 3

$$- \text{Gal}(L \setminus \mathbb{Q}(\omega)) \triangleleft \text{Gal}(L \setminus \mathbb{Q})$$

$$- \text{Gal}(L \setminus \mathbb{Q}(\sqrt[3]{2})) < \text{Gal}(L \setminus \mathbb{Q})$$

orden 2

↑ no es normal por el Testeana

orden 3

orden 2

$$\text{Sea } T = \{a\alpha + b \mid b \in \mathbb{Z}_3\} \quad D = \{a\alpha \mid a \in \mathbb{Z}_3^*\}$$

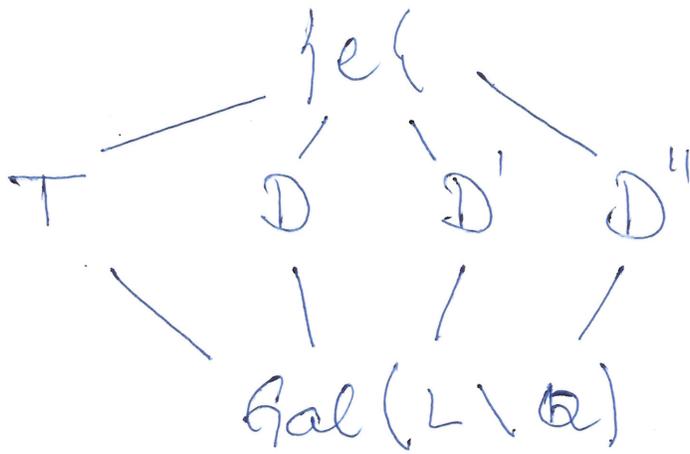
subgrupos en $\text{AGL}(\mathbb{Z}_3)$

$$T \triangleleft \text{Gal}(L \setminus \mathbb{Q})$$

D tiene 2 conjugados.

entonces

IV



Moraleja:

$\text{Gal}(L/\mathbb{Q})/T$ es un grupo

$\text{Gal}(L/\mathbb{Q})/D$ no es grupo.

$\text{Gal}(L/\mathbb{Q})/T = \{ a \in \mathbb{Z}_3^* \} = \text{ciclo}$
 $\cong \mathbb{Z}/2$

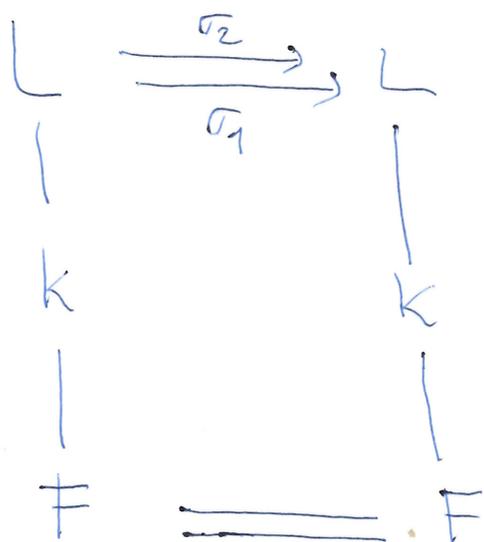
este isomorfismo

esta clase
en pasada

$\rightsquigarrow \cong \text{Gal}(\mathbb{Q}(\omega) / \mathbb{Q})$

dos automorfismos

$$\sigma_1, \sigma_2 \in \text{Gal}(L/F)$$



tal que

$$\sigma_1|_K = \sigma_2|_K$$

serán elementos de

¿Cuándo es esto un grupo? $\rightarrow \frac{\text{Gal}(L/F)}{\text{Gal}(L/K)}$

El teorema de arriba responde esta pregunta: este cociente es grupo

- (1) cuando la extensión K sobre F sea Galois
- (2) cuando el campo K sea igual a todos sus conjugados
- (3) cuando $\text{Gal}(L/K)$ sea un subgrupo normal de $\text{Gal}(L/F)$.