ALGEBRA 3 2017
CLASE 11
19/9/17 (1)

Teorema de correspondencia de Galois

E/K Galois:

$$
\begin{array}{ccc}
E & \longleftrightarrow & \mathrm{Gal}(E/E) = \{id\} \\
| & & \cap \\
E^{\mathrm{Gal}(E/F)} = F & \longmapsto & \mathrm{Gal}(E/F) \\
E^{H} & \longleftarrow\!\shortmid & H = \mathrm{Gal}(E/E^{H}) \text{ si } E/K \text{ finita} \\
| & & \cap \\
K & \longleftrightarrow & \mathrm{Gal}(E/K)
\end{array}
$$

E/K Galois finita:

$$
\begin{array}{ccc}
E & \longleftrightarrow & \mathrm{Gal}(E/E) = \{id\} \\
| & & \cap \\
E^{H'} \cancel{\mathrm{Gal}(E/L)} = L & \longleftrightarrow & H' = \mathrm{Gal}(E/L) \\
| & & \cap \\
E^{H} = F & \longleftrightarrow & H = \mathrm{Gal}(E/F) \\
| & & \cap \\
K & \longleftrightarrow & \mathrm{Gal}(E/K)
\end{array}
$$

Propiedades 1) E/K Galois Entonces

$$\mathrm{Gal}(E/F) \cap \mathrm{Gal}(E/L) = \mathrm{Gal}(E/FL)$$

Demostración

$(\subseteq)$ $\sigma \in \mathrm{Gal}(E/F) \cap \mathrm{Gal}(E/L) \Rightarrow \sigma$ fija a F y $L \Rightarrow$
σ fija a $FL \Rightarrow \sigma \in \mathrm{Gal}(E/FL)$

$(\supseteq)$ $\sigma \in \mathrm{Gal}(E/FL) \Rightarrow \sigma|_{FL} = id \Rightarrow \sigma|_F = id$ y $\sigma|_L = id$
$\Rightarrow \sigma \in \mathrm{Gal}(E/F) \cap \mathrm{Gal}(E/L)$

Propiedades 2) Sea E/K Galois

Sea G el menor subgrupo de $Gal(E/K)$ que contiene tanto a H y a H' ($H, H' < Gal(E/K)$). Entonces

$E^G = E^H \cap E^{H'}$ (generado por los eltos de $H \cup H'$)

Demostración

$(\subseteq)$ $x \in E^G \Rightarrow \sigma(x) = x, \forall \sigma \in G \Rightarrow \sigma(x) = x, \forall \sigma \in H, \forall \sigma \in H'$

$\Rightarrow x \in E^H$ y $x \in E^{H'} \Rightarrow x \in E^H \cap E^{H'}$

$(\supseteq)$ $x \in E^H \cap E^{H'} \Rightarrow \sigma(x) = x, \forall \sigma \in H$ y $\forall \sigma \in H' \Rightarrow$

$\sigma(x) = x \Rightarrow \sigma(x) = x, \forall \sigma \in \langle H \cup H' \rangle = G \Rightarrow x \in E^G$ ⊠

Investigar que valdría y en qué condiciones para

$Gal(E/F \cap L)$

y para $E^H \cdot E^{H'}$.

Correspondencia de Galois y normalidad

Rdo: $H \triangleleft G \underset{\text{def}}{\iff} \forall \sigma \in G, \ \sigma H \sigma^{-1} = H$

y en ese caso el cjto de coclases G/H tiene estructura de grupo.

Lema: Sea E/K algebraica y F/K subextensión. Entonces

$$F/K \text{ normal} \iff \sigma(F) = F, \ \forall \sigma : E \xrightarrow[K]{} \overline{K}$$

Demostración

$$F/K \text{ normal} \iff \psi(F) = F, \ \forall \psi \in \mathrm{Hom}(F/K, \overline{K}/K)$$
$$\iff \sigma(F) = F, \ \forall \sigma \in \mathrm{Hom}(E/K, \overline{K}/K)$$

pues todo $\psi \in \mathrm{Hom}(F/K, \overline{K}/K)$ se extiende a $\sigma \in \mathrm{Hom}(E/K, \overline{K}/K)$
y $\sigma|_F \in \mathrm{Hom}(F/K, \overline{K}/K)$.

Lema: Sea E/K Galois y $\sigma \in \mathrm{Gal}(E/K)$.
Sea F/K subextensión. Entonces $\sigma(F)/K$ también es subextensión

y $\mathrm{Gal}(E/\sigma(F)) = \sigma \,\mathrm{Gal}(E/F)\, \sigma^{-1}$

Demostración $\sigma(F)$ cpo y $K \subseteq \sigma(F) \subseteq E$.

$$\Big(\underset{\substack{\cap \\ F}}{\sigma(x)} + \underset{\substack{\cap \\ F}}{\sigma(y)} = \underset{\substack{\cap \\ F}}{\sigma(x+y)} \quad \text{y} \quad \sigma(x)\sigma(y) = \sigma(xy) \Big)$$

$$\tau \in \mathrm{Gal}(E/\sigma(F)) \iff \tau(\sigma(\alpha)) = \sigma(\alpha), \ \forall \alpha \in F$$
$$\iff \tau \circ \sigma(\alpha) = \sigma(\alpha) \ \forall \alpha \in F \iff \sigma^{-1} \circ \tau \circ \sigma(\alpha) = \alpha, \ \forall \alpha \in F$$
$$\iff \sigma^{-1} \circ \tau \circ \sigma \in \mathrm{Gal}(E/F) \iff \exists \psi \in \mathrm{Gal}(E/F) : \psi = \sigma^{-1} \circ \tau \circ \sigma$$
$$\iff \tau = \sigma \circ \psi \circ \sigma^{-1} \iff \tau \in \sigma \,\mathrm{Gal}(E/F)\, \sigma^{-1}$$

PROPOSICIÓN Sea E/K Galois. Entonces

① F/K normal (i.e. Galois) $\iff \mathrm{Gal}(E/F) \triangleleft \mathrm{Gal}(E/K)$
y en ese caso $\mathrm{Gal}(F/K) \simeq \mathrm{Gal}(E/K)/\mathrm{Gal}(E/F)$

(2) Si E/K finita: $H \triangleleft \mathrm{Gal}(E/K) \iff E^H/K$ Galois

Demostración

① F/K normal $\iff \sigma(F)=F,\ \forall \sigma\in \mathrm{Gal}(E/K)$

$$\iff \mathrm{Gal}(E/\sigma(F)) = \mathrm{Gal}(E/F),\quad \forall \sigma \in \mathrm{Gal}(E/K)$$

(pues $(\Rightarrow)$ obvio y $(\Leftarrow)$ pues $\sigma(F) = E^{\mathrm{Gal}(E/\sigma(F))} = E^{\mathrm{Gal}(E/F)} = F$)

$$\iff \sigma\, \mathrm{Gal}(E/F)\, \sigma^{-1} = \mathrm{Gal}(E/F),\ \forall \sigma\in \mathrm{Gal}(E/K)$$

$$\iff \mathrm{Gal}(E/F) \trianglelefteq \mathrm{Gal}(E/K)$$

y en ese caso:

$$\mathrm{Gal}(E/K) \xrightarrow{\ \Psi\ } \mathrm{Gal}(F/K)$$
$$\sigma \longmapsto \sigma|_F$$

Sobreyectiva pues todo $\tau \in \mathrm{Gal}(F/K)$ se extiende a σ

$$\ker(\Psi) = \{\sigma\in \mathrm{Gal}(E/K) \,/\, \sigma|_F = id_F\} = \mathrm{Gal}(E/F)$$

Por lo tanto $\quad \mathrm{Gal}(F/K) \simeq \mathrm{Gal}(E/K)/\mathrm{Gal}(E/F)$

② Caso finito:

$$H \trianglelefteq \mathrm{Gal}(E/K) \iff \mathrm{Gal}(E/E^H) \trianglelefteq \mathrm{Gal}(E/K)$$
$$H = \mathrm{Gal}(E/E^H)$$
$$\iff E^H \text{ normal} / K \quad (\text{o sea Galois}) \ \boxtimes$$

Proposición

E/K Galois, F/K arbitraria $\quad (E, F\subseteq L)$

Entonces: EF/F Galois
$E/E\cap F$ Galois

$$\begin{tikzcd}[column sep=small] & EF \arrow[dl, dash] \arrow[dr, dash] & \\ E \arrow[dr, dash] & & F \arrow[dl, dash] \\ & E\cap F \arrow[d, dash] & \\ & K & \end{tikzcd}$$

y si E/K finita,

$$\mathrm{Gal}(EF/F) \simeq \mathrm{Gal}(E/E\cap F)$$

(o sea aquí los grados coinciden !)

Demostración

Ya vimos EF/F y $E/E\cap F$ Galois.

Sea $\psi: \mathrm{Gal}(EF/F) \longrightarrow \mathrm{Gal}(E/E\cap F)$
$\sigma \longmapsto \sigma|_E$

Vamos a probar que ψ está bien def, es homomorfismo de grupos y es isomorfismo.

bien def: $\sigma|_F = id_F \Rightarrow \sigma|_{E\cap F} = id_{E\cap F}$ ✓

σ homomorfismo ✓

σ monomorfismo: $\sigma|_E = id_E \Rightarrow \sigma|_{EF} = id_{EF}$
$\sigma|_F = id_F$

σ epimorfismo:

$$\mathrm{Im}(\mathrm{Gal}(EF/F)) < \mathrm{Gal}(E/E\cap F)$$
$$\overset{\circ\circ}{\|}$$
$$H < \mathrm{Gal}(E/E\cap F)$$

Qpq $E^H = E\cap F$ ya que así tendremos $H = \mathrm{Gal}(E/E^H)$
$= \mathrm{Gal}(E/E\cap F)$

$(\supseteq)$
Sea $x \in E\cap F$, y sea $\tau \in H$, i.e $\exists\, \sigma \in \mathrm{Gal}(EF/F) / \tau = \sigma|_E$

luego $\tau(x) = \sigma(x) = x$ pues $x \in F \Rightarrow x \in E^H$.

$(\subseteq)$ Sea $x \in E^H$, i.e. $\tau(x) = x$, $\forall\, \tau \in H = \mathrm{Im}(\mathrm{Gal}(EF/F))$

i.e $\tau = \sigma|_E$ para $\sigma \in \mathrm{Gal}(EF/F)$

$\Rightarrow$ ~~$x \in E$ y $x \in F$ pues~~ $x \in E\cap F$
pues $\sigma(x) = x$, $\forall\, \sigma \in \mathrm{Gal}(EF/F)$ $\boxtimes$

$\Rightarrow x \in E$ y $x \in EF^{\mathrm{Gal}(EF/F)} = F$

Corolario E/K Galois finita. Entonces $[EF:F] \mid [E:K]$, $\forall\, F/K$
y $[EF:F] = [E:E\cap F]$ (pues $|\mathrm{Gal}(EF/F)| = |\mathrm{Gal}(E/E\cap F)|$)

Lema de Artin

Sea E cuerpo y $G < Aut(E)$ un subgrupo finito de automorfismos de E. Sea $K := E^G$. Entonces E/K es Galois finita y $Gal(E/K) = G$.

Obs: la demostración de la Correspondencia de Galois es directa a partir de esto (para E/K Galois finita)

Sea $G = Gal(E/K)$: entonces

$$Gal(E/E^{Gal(E/K)}) = Gal(E/K)$$

Sea $H < Gal(E/K)$ y $F := E^H$

entonces $Gal(E/E^H) = H$

$$\left.\begin{array}{l} y \quad E^{Gal(E/E^H)} = E^{Gal(E/F)} \\ \qquad \overset{\|}{H} = F. \end{array}\right] ?$$

Lema auxiliar para el lema de Artin

Sea E/K separable y supongamos que existe n / $[K[\alpha]:K] \leq n$, $\forall \alpha \in E$.

Entonces E/K es finita y por lo tanto monógena:
$\exists\, \theta \in E$ / $E = K[\theta]$ y se tiene $[E:K] \leq n$ también.

Demostración

Sea $\theta \in E$ con $[K[\theta]:K] \leq n$ máximo. Entonces $E = K[\theta]$ pues sino $\exists\, \beta \notin K[\theta]$ / $K[\theta,\beta]$ es finita separable.
$\Rightarrow K[\theta,\beta] = K[\gamma]$ y $[K[\gamma]:K] >$ máximo.

Absurdo. ☒

Demostración del lema de Artin

Dado $\alpha \in E$. Qpq α es separable $/K$.

Como G es finito, considero los finitos $\sigma_i(\alpha)$, con $\sigma \in G$,

o sea $\{\sigma_1(\alpha), \dots, \sigma_m(\alpha)\} = \{\sigma(\alpha), \sigma \in G\}$

Sea $f = \prod_{1 \leq i \leq m} (X - \sigma_i(\alpha)) \in E[X]$ pues $\sigma_i \in \mathrm{Aut}(E)$

Probemos que $f \in E^G[X] = K[X]$:

$\forall \sigma \in G$, $\sigma(f) = \prod (X - \sigma \circ \sigma_i(\alpha)) = f$.

$\Rightarrow$ α es raíz de un polinomio separable en $K[X]$.

Pero además $\forall \alpha \in E$, $[K[\alpha] : K] \leq |G| \Rightarrow$

E/K es finita de grado $\leq |G|$, y $E = K[\theta]$

donde $f(\theta, K) = \prod_{\substack{\sigma \in G \\ \sigma(\theta) \neq \sigma'(\theta)}} (X - \sigma(\theta))$ tiene todas sus raíces en E

$\Rightarrow$ E/K es el cuerpo de descomposición de un pol. separable

$\Rightarrow$ E/K Galois finita.

Mas aún, $[E : K] \leq |G|$, i.e. $|\mathrm{Gal}(E/K)| \leq |G|$

Pero por otro lado
$G \subseteq \mathrm{Gal}(E/K)$:

$\forall \sigma \in G$, $\forall \alpha \in K = E^G$, $\sigma(\alpha) = \alpha$ por def

(También se puede ver que en realidad
$f(\theta, K) = \prod_{\sigma \in G} (X - \sigma(\theta))$) $\boxtimes$