Álgebra III - 2do C. 2020 - Clase 11 - 6/10/2020

Recapitulando la correspondencia de Galois

Sea E/K Galois *finita*, entonces

$$\begin{array}{ccc} E & \longleftrightarrow & \{\mathrm{id}_E\} \\ | & & \wedge \\ F & \longrightarrow & \mathrm{Gal}(E/F) \\ \| & \circlearrowleft & \| \\ E^H & \longleftarrow & H \\ | & & \wedge \\ K & \longleftrightarrow & \mathrm{Gal}(E/K) \end{array}$$

Propiedades

Sean $K \subset F, L \subset E$ con E/K Galois, y $H, H' < \mathrm{Gal}(E/K)$.

- $E^{\mathrm{Gal}(E/F)} = F$ (inyectividad de $\to$ siempre)
- $\mathrm{Gal}(E/E^H) = H$ cuando E/K *finita* (inyectividad de $\leftarrow$ en el caso finito)
- $F \subset L \implies \mathrm{Gal}(E/F) > \mathrm{Gal}(E/L)$, pues
  $\mathrm{Gal}(E/L) = \{\sigma \in \mathrm{Gal}(E/K) \text{ tq } \sigma|_L = \mathrm{id}\} \subset \{\sigma \in \mathrm{Gal}(E/K) \text{ tq } \sigma|_F = \mathrm{id}\} = \mathrm{Gal}(E/F)$.
- $H < H' \implies E^H \supset E^{H'}$, pues
  $E^{H'} = \{x \in E \text{ tq } \sigma(x) = x, \forall\, \sigma \in H'\} \subset \{x \in E \text{ tq } \sigma(x) = x, \forall\, \sigma \in H\} = E^H$.
- $F \subset L \iff \mathrm{Gal}(E/F) > \mathrm{Gal}(E/L)$,
  pues para la vuelta
  $$F = E^{\mathrm{Gal}(E/F)} \subset E^{\mathrm{Gal}(E/L)} = L.$$
- Si E/K finita, $H < H' \iff E^H \supset E^{H'}$,
  pues para la vuelta
  $$H = \mathrm{Gal}(E/E^H) < \mathrm{Gal}(E/E^{H'}) = H'.$$

Correspondencia de Galois y normalidad

Vamos a desarrollar ahora la relación entre subextensiones normales de E/K y subgrupos normales de $\mathrm{Gal}(E/K)$: con razón el nombre de extensión normal ¿no?

Recuerdo que $H \lhd G \;\Leftrightarrow\; \forall\, \sigma \in G\,,\ \sigma\, H\, \sigma^{-1} = H$
y en ese caso el conjunto de coclases G/H tiene estructura de grupo.

Lema 8.2.7 (Subextensiones normales e inmersiones)
Sea E/K algebraica y F/K subextensión. Entonces

$$F/K \ \textit{normal} \quad \Longleftrightarrow \quad \sigma(F) = F,\, \forall\, \sigma \in \mathrm{Hom}(E/K, \overline{K}/K).$$

Prueba.–

$$\begin{aligned} F/K \ \text{ normal} \quad &\underset{\text{def}}{\Longleftrightarrow} \quad \psi(F) = F,\, \forall\, \psi \in \mathrm{Hom}(F/K, \overline{K}/K) \\ &\Longleftrightarrow \quad \sigma(F) = F,\, \forall\, \sigma \in \mathrm{Hom}(E/K, \overline{K}/K), \end{aligned}$$

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

■

Lema 8.2.8 (Subextensiones y conjugación)
Sea E/K Galois, F/K subextensión y $\sigma \in \mathrm{Gal}(E/K)$. Entonces

1. *$\sigma(F)$ también es subextensión de E/K,*
2. $\mathrm{Gal}(E/\sigma(F)) = \sigma\, \mathrm{Gal}(E/F)\, \sigma^{-1}$

Prueba.–
(1) $\sigma(F)$ es cuerpo y $K \subset \sigma(F) \subset E$:

(2)

$$\begin{aligned}
\tau \in \mathrm{Gal}(E/\sigma(F)) &\iff \tau(\sigma(\alpha)) = \sigma(\alpha),\ \forall\, \alpha \in F \\
&\iff \sigma^{-1} \circ \tau \circ \sigma(\alpha) = \alpha,\ \forall\, \alpha \in F \\
&\iff \sigma^{-1} \circ \tau \circ \sigma \in \mathrm{Gal}(E/F) \\
&\iff \exists\, \psi \in \mathrm{Gal}(E/F) \ \text{ tq } \ \psi = \sigma^{-1} \circ \tau \circ \sigma \\
&\iff \exists\, \psi \in \mathrm{Gal}(E/F) \ \text{ tq } \ \tau = \sigma \circ \psi \circ \sigma^{-1} \\
&\iff \tau \in \sigma\, \mathrm{Gal}(E/F)\, \sigma^{-1}.
\end{aligned}$$

■

Proposición 8.2.9 (Galois y normalidad)
Sea E/K Galois. Entonces

1. *F/K normal (i.e. Galois)* $\iff$ $\mathrm{Gal}(E/F) \lhd \mathrm{Gal}(E/K)$,
   y en ese caso $\mathrm{Gal}(F/K) \simeq \mathrm{Gal}(E/K)/\mathrm{Gal}(E/F)$.
2. *Si E/K es finita, $H \lhd \mathrm{Gal}(E/K)$* $\iff$ *E^H/K Galois.*

Prueba.–
(1)

$$\begin{aligned}
F/K \ \text{ normal} &\iff \sigma(F) = F,\ \forall\, \sigma \in \mathrm{Gal}(E/K) \\
&\iff \mathrm{Gal}(E/\sigma(F)) = \mathrm{Gal}(E/F),\ \forall\, \sigma \in \mathrm{Gal}(E/K) \\
&\iff \sigma\, \mathrm{Gal}(E/F)\, \sigma^{-1} = \mathrm{Gal}(E/F),\ \forall\, \sigma \in \mathrm{Gal}(E/K) \\
&\iff \mathrm{Gal}(E/F) \lhd \mathrm{Gal}(E/K),
\end{aligned}$$

donde la vuelta de la segunda equivalencia vale porque

$$\sigma(F) = E^{\mathrm{Gal}(E/\sigma(F))} = E^{\mathrm{Gal}(E/F)} = F.$$

En ese caso consideramos el morfismo de grupos

$$\begin{array}{rccc}
\Psi: & \mathrm{Gal}(E/K) & \longrightarrow & \mathrm{Gal}(F/K) \\
& \sigma & \longmapsto & \sigma|_F.
\end{array}$$

- Ψ es sobreyectiva pues toda $\psi \in \mathrm{Gal}(F/K)$ se extiende a $\sigma \in \mathrm{Gal}(E/K)$.
- $\mathrm{Nu}(\Psi) = \{\sigma \in \mathrm{Gal}(E/K) \,:\, \sigma|_F = \mathrm{id}_F\} = \mathrm{Gal}(E/F)$.

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

(2) En el caso E/K finita, como $H = \mathrm{Gal}(E/E^H)$,

$$H \lhd \mathrm{Gal}(E/K) \iff \mathrm{Gal}(E/E^H) \lhd \mathrm{Gal}(E/K) \iff E^H/K \text{ normal.}$$

■

Dejo el resto de esta página libre para que cada uno se arme sus mejores diagramas para resumir toda la información sobre la correspondencia de Galois.

Correspondencia de Galois vs. compuestos e intersecciones

Proposición 8.2.10 (Grupos de Galois, intersecciones y compuestos)
Sean $K \subset F, L \subset E$ *con* E/K *Galois,* $H, H' < \mathrm{Gal}(E/K)$. *Entonces*

1. $\mathrm{Gal}(E/F) \cap \mathrm{Gal}(E/L) = \mathrm{Gal}(E/FL)$.
2. *Sea* G *el menor subgrupo de* $\mathrm{Gal}(E/K)$ *que contiene tanto a* H *como a* H', *o sea* $G = \langle H \cup H' \rangle$.

   Entonces $E^H \cap E^{H'} = E^G$.

Prueba.–
(1)

$$\begin{aligned} \sigma \in \mathrm{Gal}(E/F) \cap \mathrm{Gal}(E/L) &\iff \sigma|_F = \mathrm{id}_F \text{ y } \sigma|_L = \mathrm{id}_L \\ &\iff \sigma|_{FL} = \mathrm{id}_{FL} \iff \sigma \in \mathrm{Gal}(E/FL) \end{aligned}$$

(2)

$$\begin{aligned} x \in E^H \cap E^{H'} &\iff \sigma(x) = x, \forall\, \sigma \in H \text{ y } \forall\, \sigma \in H' \\ &\iff \sigma(x) = x, \forall\, \sigma \in \langle H \cup H' \rangle \iff x \in E^G \end{aligned}$$

■

Investigar qué valdría y en qué condiciones para $\mathrm{Gal}(E/F \cap L)$ y para $E^H\, E^{H'}$.

Veamos ahora una consecuencia de la propiedad $E^{\mathrm{Gal}(E/K)} = K$, que en el caso de extensiones Galois, corrige la anormalidad que habíamos visto que podía pasar que $[FL : L] \neq [F : F \cap L]$ (Proposición 3.2.2):

Proposición 8.2.11 (Compuesto para Galois finita)
Sean $K \subset F, L \subset E$ *con* F/K *Galois* finita *y* L/K *arbitraria. Entonces*

1. $\mathrm{Gal}(FL/L) \simeq \mathrm{Gal}(F/F \cap L)$, *y por lo tanto* $[FL : L] = [F : F \cap L]$.
2. $[FL : L] \,|\, [F : K]$.

Prueba.–

1. Sabemos que FL/L y $F/F\cap L$ son ambas Galois (no hace falta aquí F/K finita).

   Definimos el mapa

   $$\begin{array}{rccc} \Psi: & \mathrm{Gal}(FL/L) & \longrightarrow & \mathrm{Gal}(F/F\cap L) \\ & \sigma & \longmapsto & \sigma|_F. \end{array}$$

   Probemos que está bien definido, y que es un isomorfismo de grupos.

   - <u>Buena definición</u> $\quad \sigma\in\mathrm{Gal}(FL/L) \Rightarrow \sigma|_F\in\mathrm{Gal}(F/F\cap L)$:

     Por un lado, como $\sigma|_L=\mathrm{id}_L$, $\sigma|_{F\cap L}=\mathrm{id}_{F\cap L}$.

     Por otro lado, como F/K es normal, $\sigma|_F$ es $(F\cap L)$-automorfismo.

   - <u>Ψ isomorfismo de grupos</u>
     - Primero, Ψ es morfismo de grupos está ok, ¿no?
     - Segundo, Ψ mono:

       Si $\Psi(\sigma)=\mathrm{id}_F$, i.e., si $\sigma|_F=\mathrm{id}_F$, sabiendo que $\sigma|_L=\mathrm{id}_L$ se concluye que $\sigma|_{FL}=\mathrm{id}_{FL}$.
     - Tercero, Ψ epi:

       Sabemos que $H:=\mathrm{Im}(\mathrm{Gal}(FL/L))<\mathrm{Gal}(F/F\cap L)$.
       Qpq son iguales.

       Para ello probemos que $F^H=F\cap L$ porque así por la correspondencia de Galois en el caso finito, tendremos

       $$H=\mathrm{Gal}(F/F^H)=\mathrm{Gal}(F/F\cap L).$$

       $F^H\subset F\cap L$:

       Sea $x\in F^H=\{x\in F:\tau(x)=x,\,\forall\tau\in H\}$, qpq $x\in F\cap L$,
       o sea me falta probar $x\in L$.

       Para ello, como $x\in F\subset FL$,
       vamos a probar que $x\in(FL)^{\mathrm{Gal}(FL/L)}=L$.

       Sea entonces $\sigma\in\mathrm{Gal}(FL/L)$, qpq $\sigma(x)=x$.

       Pero $\sigma|_F=:\tau\in H=\mathrm{Im}(\mathrm{Gal}(FL/L))$ y por lo tanto

       $$x\in F^H \quad\Longrightarrow\quad \tau(x)=x \quad\Longrightarrow\quad \sigma(x)=x.$$

$F^H \supset F \cap L$:

Sea $x \in F \cap L$, qpq $x \in F^H = \{x \in F : \tau(x) = x, \forall\, \tau \in H\}$.

Sea entonces $\tau \in H = \mathrm{Im}(\mathrm{Gal}(FL/L))$. Pero

$$\exists\, \sigma \in \mathrm{Gal}(FL/L) \ \text{ tq } \ \tau = \sigma|_F \quad \Longrightarrow \quad \tau(x) = \sigma(x) = x \ \text{ pues } \ x \in L$$
$$\Longrightarrow \quad x \in F^H.$$

2. Por (1) sabemos que $[FL : L] = [F : F \cap L]$,

   y también vale $[F : F \cap L] \,|\, [F : K]$.

   Por lo tanto $[FL : L] \,|\, [F : K]$.

■

Otra equivalencia de ser Galois

Probaremos ahora que en realidad la propiedad $E^{\mathrm{Gal}(E/K)} = K$ caracteriza la propiedad de ser Galois, no es solo una consecuencia de ello, y en muchos lados se da esa propiedad como definición de extensión Galois.

Recuerdo que me tomé la libertad de notar por $\mathrm{Gal}(E/K)$ el conjunto de todos los K-automorfismos de E, aún cuando la extensión no es Galois.

Teorema 8.2.12 (Otra equivalencia de Galois)
Sea E/K algebraica. Entonces

$$E/K \ \textit{ Galois (normal y separable)} \quad \Longleftrightarrow \quad E^{\mathrm{Gal}(E/K)} = K.$$

Prueba.–

($\Rightarrow$) Esto ya lo vimos, es la proposición 8.2.5.

($\Leftarrow$) Quiero probar que E/K es separable, es decir que $\forall\, \alpha \in E$, α es separable, y también que E/K es normal, es decir que $\forall\, \sigma \in \mathrm{Hom}(E/K, \overline{K}/K)$ se tiene que $\sigma(\alpha) \in E$ (así las inmersiones son endos, y por lo tanto autos).

Sea entonces $\alpha \in E$. Como $K(\alpha)/K$ es finita, $\mathrm{Hom}(K(\alpha)/K, \overline{K}/K)$ es finita, y en particular el conjunto de los *distintos* valores en

$$\{\sigma(\alpha) \,:\, \sigma \in \mathrm{Gal}(E/K)\}$$

es finito. Sean entonces $\sigma_1, \ldots, \sigma_n \in \mathrm{Gal}(E/K)$ tales que

$$\{\sigma(\alpha) \,:\, \sigma \in \mathrm{Gal}(E/K)\} = \{\sigma_1(\alpha), \ldots, \sigma_n(\alpha)\},$$

que, repito, son todos valores distintos entre sí.
Defino

$$f = \prod_{1\leq \imath \leq n} \big(X - \sigma_i(\alpha)\big) \quad \in \ E[X], \ \text{ pues } \sigma_i(\alpha) \in E.$$

Se tiene

- $f(\alpha) = 0$ pues para $\sigma = \mathrm{id}_E$, $\sigma(\alpha) = \alpha$ es uno de los valores tomados.
- $f \in E^{\mathrm{Gal}(E/K)}[X]$ pues si $\sigma \in \mathrm{Gal}(E/K)$, se tiene

$$\sigma(f) = \prod_{1\leq \imath \leq n} \big(X - \sigma \circ \sigma_i(\alpha)\big) = \prod_{1\leq \imath \leq n} \big(X - \sigma_i(\alpha)\big) = f,$$

  dado que son todos automorfismos y

$$\{\sigma_1(\alpha), \ldots, \sigma_n(\alpha)\} = \{\sigma \circ \sigma_1(\alpha), \ldots, \sigma \circ \sigma_n(\alpha)\}$$

  pues esos son todos los valores posibles de evaluar los automorfismos de E en α.

Por lo tanto $f \in E^{\mathrm{Gal}(E/K)}[X] = K[X]$ por hipotesis.
Así, α es raíz del polinomio $f \in K[X]$ que tiene todas sus raíces distintas: α es separable.
Notar además que $f(\alpha, K) \,|\, f$, o sea todas las raíces del minimal de f son de la forma $\sigma_i(\alpha)$ para algunos i, donde σ_i es automorfismo de E. Es decir todas las raíces de $f(\alpha, K)$ pertenecen a E.
Esto implica que $\forall\, \sigma \in \mathrm{Hom}(E/K, \overline{K}/K)$ se tiene que $\sigma(\alpha) \in E$, pues obligatoriamente $\sigma(\alpha)$ es una raíz de $f(\alpha, K)$.

■