# Álgebra III - 2do C. 2020 - Clase 10 - 2/10/2020

**Proposición 8.1.4** (Galois vs. torres y compuestos)

1. *Torres:* *Sea* $E/F/K$ *torre.*
   - $E/K$ *Galois* $\Rightarrow$ $E/F$ *Galois:*
   - *¿* $E/K$ *Galois* $\Rightarrow$ $F/K$ *Galois?*
   - *¿* $E/F$ *y* $F/K$ *Galois* $\Rightarrow$ $E/K$ *Galois ?*
2. *Compuestos e intersecciones:* *Sean* $K \subset F, L \subset E$.
   - $F/K$ *Galois* $\Rightarrow$ $FL/L$ *Galois*
   - $F, L$ *Galois sobre* $K$ $\Rightarrow$ $FL/K$ *Galois*
   - *¿* $FL/K$ *Galois* $\Rightarrow$ $F, L$ *Galois sobre* $K$ *?*
   - *¿* $F, L$ *Galois sobre* $K$ $\Rightarrow$ $F \cap L/K$ *Galois?*

**Proposición 8.1.5** ($\mathrm{Gal}(f,K) < S_n$ para $f$ separable)
*Sea $f \in K[X]$ un polinomio separable de grado $n$. Entonces $\mathrm{Gal}(f,K) < S_n$, el grupo de permutaciones de $n$ elementos.*

Prueba.–
Sea $K(f) = K(\alpha_1, \ldots, \alpha_n)$ con $\alpha_1, \ldots, \alpha_n$ distintos, raíces de $f$,
y sea $A = \{\alpha_1, \ldots, \alpha_n\}$.
Para todo $\sigma \in \mathrm{Gal}(f,K)$, $\sigma(A) = A$. Entonces

$$\mathrm{Gal}(f,K) \ \to \ S(A) = S_n \ , \ \sigma \ \mapsto \ \sigma|_A$$

es un morfismo de grupos, que es monomorfismo, pues $\sigma|_A = \mathrm{id} \ \Rightarrow \ \sigma = \mathrm{id}_K$.
Por lo tanto $\mathrm{Gal}(f,K)$ es (isomorfo a) un subgrupo de $S_n$.

■

## 8.2 Correspondencia de Galois

Ya podemos empezar a construir de a poco la correspondencia de Galois.

**Observación 8.2.1** (Subextensiones $E/F$ y subgrupos de $\mathrm{Gal}(E/K)$)
*Sea $E/F/K$ torre y $E/K$ Galois. Entonces,*

- *$E/F$ Galois,*
- $\mathrm{Gal}(E/F) < \mathrm{Gal}(E/K)$*:* $\mathrm{Gal}(E/F)$ *es un* subgrupo *del grupo* $\mathrm{Gal}(E/K)$.

*Más aún, si $E/K$ Galois* finita*, entonces* $|\mathrm{Gal}(E/F)| = [E:F]$,
*y si $K \subset F, L \subset E$, entonces*

$$\mathrm{Gal}(E/F) = \mathrm{Gal}(E/L) \ \Rightarrow \ F = L.$$

*Prueba.–*
Ya sabemos $E/F$ Galois (¡Ojo, $F/K$ no tiene porque serlo!)
Claramente, $\mathrm{Gal}(E,F)$ es un subconjunto de $\mathrm{Gal}(E/K)$ que es un grupo también, con lo cual $\mathrm{Gal}(E/F) < \mathrm{Gal}(E/K)$.
Ahora bien, en el caso $E/K$ Galois finita, $E = K(\theta)$ y si $K \subset F, L \subset E$, se tiene

$$\begin{aligned} \mathrm{Gal}(E/F) = \mathrm{Gal}(E/L) \ &\Rightarrow \ \prod_{\sigma \in \mathrm{Gal}(E/F)} \big(X - \sigma(\theta)\big) = \prod_{\sigma \in \mathrm{Gal}(E/L)} \big(X - \sigma(\theta)\big) \\ &\Rightarrow \ f(\theta, F) = f(\theta, L) \\ &\Rightarrow \ F = L. \end{aligned}$$

■

**Ejemplo** (Subextensiones de $\mathbb{Q}(\sqrt[3]{2},\omega)/\mathbb{Q}$)

$$\mathbb{Q}(\sqrt[3]{2},\omega)=\mathbb{Q}(f) \text{ con } f=(X-\sqrt[3]{2})(X-\sqrt[3]{2}\omega)(X-\sqrt[3]{2}\omega^2)$$

donde vamos a numerar las raíces:

$$\alpha_1=\sqrt[3]{2} \quad , \quad \alpha_2=\sqrt[3]{2}\omega \quad , \quad \alpha_3=\sqrt[3]{2}\omega^2.$$

Notemos $E=\mathbb{Q}(\sqrt[3]{2},\omega)$. Se tiene

$$\mathrm{Gal}(E/\mathbb{Q})=\{\sigma_1,\ldots,\sigma_6\}\simeq S_3=\{1,(12),(13),(23),(123),(132)\},$$

con la identificación

$$\begin{array}{lcl}
\sigma_1=\mathrm{id}_E & \leftrightarrow & 1\\
\sigma_2:\ \sqrt[3]{2}\mapsto\sqrt[3]{2},\omega\mapsto\omega^2 & \leftrightarrow & (23) \text{ pues } \alpha_1\mapsto\alpha_1,\alpha_2\mapsto\alpha_3,\alpha_3\mapsto\alpha_2\\
\sigma_3:\ \sqrt[3]{2}\mapsto\sqrt[3]{2}\omega,\omega\mapsto\omega & \leftrightarrow & (123) \text{ pues } \alpha_1\mapsto\alpha_2,\alpha_2\mapsto\alpha_3,\alpha_3\mapsto\alpha_1\\
\sigma_4:\ \sqrt[3]{2}\mapsto\sqrt[3]{2}\omega,\omega\mapsto\omega^2 & \leftrightarrow & (12) \text{ pues } \alpha_1\mapsto\alpha_2,\alpha_2\mapsto\alpha_1,\alpha_3\mapsto\alpha_3\\
\sigma_5:\ \sqrt[3]{2}\mapsto\sqrt[3]{2}\omega^2,\omega\mapsto\omega & \leftrightarrow & (132) \text{ pues } \alpha_1\mapsto\alpha_3,\alpha_2\mapsto\alpha_1,\alpha_3\mapsto\alpha_2\\
\sigma_6:\ \sqrt[3]{2}\mapsto\sqrt[3]{2}\omega^2,\omega\mapsto\omega^2 & \leftrightarrow & (13) \text{ pues } \alpha_1\mapsto\alpha_3,\alpha_2\mapsto\alpha_2,\alpha_3\mapsto\alpha_1
\end{array}$$

Subgrupos de $S_3$: Hay 6

$$\{1\}\ ,\ \langle(12)\rangle\ ,\ \langle(13)\rangle\ ,\ \langle(23)\rangle\ ,\ \langle(123)\rangle\ ,\ S_3$$

que se corresponden con los subgrupos de $\mathrm{Gal}(E/\mathbb{Q})$:

$H_1=\{\mathrm{id}_E\}$ , $H_2=\langle\sigma_4\rangle$ , $H_3=\langle\sigma_6\rangle$ , $H_4=\langle\sigma_2\rangle$ , $H_5=\langle\sigma_3\rangle=\langle\sigma_5\rangle$ , $H_6=\mathrm{Gal}(E,\mathbb{Q})$.

Para cada subextensión $F/\mathbb{Q}$ de $E/\mathbb{Q}$, $E/F$ define un subgrupo $\mathrm{Gal}(E/F)$ en forma inyectiva, y ya conocemos 6 subxtensiones de $E/\mathbb{Q}$:

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

¡Así que las tenemos todas! ¿Pero cómo se corresponden?
Notar que $[E:F]=|\mathrm{Gal}(E/F)|$ así que esa información limita la búsqueda por suerte... Recordar también que $\sigma\in\mathrm{Gal}(E/F)$ implica que $\sigma|_F=\mathrm{id}_F$, ayuda:

$$\begin{array}{lcl}
\mathrm{Gal}(E/F_1)=H_1=\{\mathrm{id}_E\} & \Longrightarrow & [E:F_1]=1 \ \text{ y } \ F_1=E,\\
\mathrm{Gal}(E/F_2)=H_2=\langle\sigma_4\rangle & \Longrightarrow & [E:F_2]=2 \ \text{ y } \ F_2=\mathbb{Q}(\sqrt[3]{2}\omega^2),\\
\mathrm{Gal}(E/F_3)=H_3=\langle\sigma_6\rangle & \Longrightarrow & [E:F_3]=2 \ \text{ y } \ F_3=\mathbb{Q}(\sqrt[3]{2}\omega),\\
\mathrm{Gal}(E/F_4)=H_4=\langle\sigma_2\rangle & \Longrightarrow & [E:F_4]=2 \ \text{ y } \ F_4=\mathbb{Q}(\sqrt[3]{2}),\\
\mathrm{Gal}(E/F_5)=H_5=\langle\sigma_3\rangle & \Longrightarrow & [E:F_5]=3 \ \text{ y } \ F_5=\mathbb{Q}(\omega),\\
\mathrm{Gal}(E/F_6)=H_6=\mathrm{Gal}(E/\mathbb{Q}) & \Longrightarrow & [E:F_6]=6 \ \text{ y } \ F_6=\mathbb{Q},
\end{array}$$

pues $\sigma_4(\sqrt[3]{2}\omega^2)=\sqrt[3]{2}\omega\cdot\omega^4=\sqrt[3]{2}\omega^2$ y $\sigma_6(\sqrt[3]{2}\omega)=\sqrt[3]{2}\omega^2\cdot\omega^2=\sqrt[3]{2}\omega$.

¿Quiénes son las subextensiones normales de $E/\mathbb{Q}$? La única (salvo las triviales) es $\mathbb{Q}(\omega)$.

¿Quiénes son los subgrupos normales de $S_3$? El único (salvo los triviales) es $\langle\sigma_3\rangle = \langle\sigma_5\rangle$ que se corresponde con $A_3 = \langle(123)\rangle$, que tiene índice 2.

En este ejemplo, $F/K$ subextensión normal de $E/K \iff \mathrm{Gal}(E/F) \lhd \mathrm{Gal}(E/K)$.

---

Rdo: Sea $H < G$ grupo, entonces $H$ es *normal* en $G$:

$$\begin{aligned} H \lhd G &\iff ghg^{-1} \in H,\ \forall\, h \in H,\ \forall\, g \in G \\ &\iff gHg^{-1} = H,\ \ \forall\, g \in G \end{aligned}$$

Por ejemplo $\langle(12)\rangle \not\lhd S_3$ pues $(132)(12)(123) = (13)$.

Los subgrupos normales son los que permiten cocientar y darle a $G/H$ una estructura de grupo.

---

La correspondencia de Galois que veremos a continuación sistematiza esta búsqueda que hicimos en forma medio desprolija a mano, además de que permite encontrar todas las subextensiones aún cuando uno no las conoce a priori como en este ejemplo.

**Teorema 8.2.2** (Correspondencia de Galois - I)
*Sea $E/K$ Galois.*

$$\begin{array}{ccc} E & \longmapsto & \mathrm{Gal}(E/E) = \{\mathrm{id}_E\} \\ | & & \wedge \\ F & \longmapsto & \mathrm{Gal}(E/F) = \{\sigma \in \mathrm{Gal}(E/K) \,:\, \sigma|_F = \mathrm{id}_F\} \\ | & & \wedge \\ K & \longmapsto & \mathrm{Gal}(E/K) \end{array}$$

*Sea*

$$\begin{array}{rccc} \Phi: & \textit{Subextensiones de } E/K & \longrightarrow & \textit{Subgrupos de } \mathrm{Gal}(E/K) \\ & F/K & \longmapsto & \mathrm{Gal}(E/F). \end{array}$$

*Entonces*

1. $\Phi$ *es inyectiva*
2. *Si $E/K$ es Galois* finita, $\Phi$ *es sobreyectiva, con*

$$\Phi^{-1}(H) = E^H := \{x \in E \,:\, \sigma(x) = x,\ \forall\, \sigma \in H\} \ \subset\ E.$$

Vamos a ir haciendo la prueba de a poquito, a través de los resultados que siguen.

**Lema 8.2.3** (El cuerpo fijo por un subgrupo)
*Sea $E/K$ Galois, y $H < \mathrm{Gal}(E/K)$, y sea*

$$E^H := \{x \in E \,:\, \sigma(x) = x,\ \forall\, \sigma \in H\} \subset E.$$

*Entonces,*
*$E^H$ es una subextensión de $E/K$, que se llama el* cuerpo fijo de $E$ por $H$.

*Prueba.–*
Primero notamos que $K \subset E^H \subset E$ pues si $x \in K$, $\sigma(x) = x$, $\forall\, \sigma \in H$ (pues $\sigma(x) = x$, $\forall\, \sigma \in \mathrm{Gal}(E/K)$ y $H \subset \mathrm{Gal}(E/K)$).
Segundo $E^H$ es un cuerpo: $0, 1 \in E^H$ y $x, y \in E^H \ \Rightarrow\ x \pm y, xy, 1/x \in E^H$ debido a que $\sigma \in H$ es inmersión de cuerpos: $\forall\, \sigma \in H$ y $x, y \in E^H$ se tiene

$$\begin{cases} \sigma(x \pm y) = \sigma(x) \pm \sigma(y) = x \pm y, \\ \sigma(xy) = \sigma(x)\sigma(y) = xy \\ \sigma(1/x) = 1/\sigma(x) = 1/x \end{cases}$$

■

**Observación 8.2.4** ( $E^{\{\mathrm{id}_E\}} = E$ )
*Sea* $E/K$ *Galois y* $H = \{\mathrm{id}_E\}$. *Entonces* $E^H = E$.

**Proposición 8.2.5** ( $\Phi$ es inyectiva)
*Sea* $E/K$ *Galois. Entonces* $E^{\mathrm{Gal}(E/K)} = K$.
*En particular* $\Phi$ *es inyectiva.*

*Prueba.–*
Ya sabemos que $K \subset E^{\mathrm{Gal}(E/K)}$, que es una subextensión de $E/K$.
Falta probar que $E^{\mathrm{Gal}(E/K)} \subset K$,
o equivalentemente, que si $\alpha \notin K$, entonces $\alpha \notin E^{\mathrm{Gal}(E/K)}$.
Para ello probamos que si $\alpha \notin K$, entonces existe $\sigma \in \mathrm{Gal}(E/K)$ tal que $\sigma(\alpha) \neq \alpha$:
Pero si $\alpha \notin K$, $\mathrm{gr}(f(\alpha, K)) \geq 2$ y como el polinomio es separable, existe $\beta \neq \alpha$ raíz de $f(\alpha, K)$ también.
Por lo tanto, como ya usamos varias veces, por ser $E/K$ normal, existe $\sigma \in \mathrm{Gal}(E/K)$ que extiende al isomorfismo $K(\alpha) \to K(\beta)$, $\alpha \mapsto \beta$. O sea $\sigma(\alpha) \neq \alpha$, como se quería probar.

Esto implica que $\Phi$ es inyectiva ya que si $F/K$ y $L/K$ son dos subextensiones de $E/K$, entonces $E/F$ y $E/L$ son Galois, y

$$\Phi(F) = \Phi(L) \;\Leftrightarrow\; \mathrm{Gal}(E/F) = \mathrm{Gal}(E/L) \;\Rightarrow\; E^{\mathrm{Gal}(E/F)} = E^{\mathrm{Gal}(E/L)} \;\Leftrightarrow\; F = L.$$

Esto prueba (1) en el teorema 8.2.2.

■

Notar que el Teorema Fundamental de los polinomios simétricos elementales implica que si $E = K(f)$ con $\mathrm{gr}(f) = n$, entonces $E^{S_n} = K$, donde por $E^{S_n}$ se entiende el cuerpo fijo por todas las permutaciones de las raíces de $f$, independientemente de las relaciones que existan entre ellas. Esto es por la *Consecuencia esencial para nosotros* que vimos en la primera clase, y es el argumento que usaron Vandermonde y Lagrange para resolver las ecuaciones de grado 3 y 4. Lo brillante de Galois fue darse cuenta de tomar en cuenta las relaciones entre las raíces, que son las que determinan el grupo de Galois: no hace falta quedar fijo por todo el grupo simétrico (tratando a las raíces como variables independientes) sino por el grupo de Galois, que es el que refleja las relaciones que existen entre las raíces.

Tratamos ahora la sobreyectividad de $\Phi$ en el caso que $E/K$ es Galois *finita*.

**Proposición 8.2.6** ( $\Phi$ es sobreyectiva si $E/K$ finita)
*Sea* $E/K$ *Galois* finita. *Entonces, para todo* $H < \mathrm{Gal}(E/K)$, $\mathrm{Gal}(E/E^H) = H$.
*En particular* $\Phi$ *es sobreyectiva.*

*Prueba.–*
(1) $\underline{H \subset \mathrm{Gal}(E/E^H)}$:
Sea $\tau \in H$. Qpq $\tau \in \mathrm{Gal}(E/E^H)$, es decir que $\tau$ es un automorfismo de $E$ que satisface que $\tau(\alpha) = \alpha$, $\forall\, \alpha \in E^H$.
Pero por definición, $E^H = \{\alpha \in E : \psi(\alpha) = \alpha, \forall\, \psi \in H\}$.
En particular, como $\tau \in H$, $\tau(\alpha) = \alpha$, $\forall\, \alpha \in E^H$.
(Notar que aquí no hemos usado que $E/K$ es finita: siempre vale $H \subset \mathrm{Gal}(E/E^H)$.)
(1) $\underline{\mathrm{Gal}(E/E^H) = H}$:
Como ambos subgrupos son subrupos del grupo finito $\mathrm{Gal}(E/K)$, y como ya sabemos que $H \subset \mathrm{Gal}(E/E^H)$, alcanza con probar que $|H| = |\mathrm{Gal}(E/E^H)|$. Y en realidad alcanza con probar que $|H| \geq |\mathrm{Gal}(E/E^H)|$.
Probemos entonces que $|H| \geq |\mathrm{Gal}(E/E^H)|$:
Como $E/E^H$ es Galois finita, hay un elemento primitivo $\theta \in E$ tq

$$E = E^H(\theta) \quad \text{y} \quad |\mathrm{Gal}(E/E^H)| = \mathrm{gr}(f(\theta, E^H)).$$

Definamos

$$f = \prod_{\tau \in H} \big(X - \tau(\theta)\big) \quad \in \; E[X],$$

que tiene grado $|H|$.
Si probamos que $f \in E^H[X]$, entonces $f(\theta, E^H) \,|\, f$, lo que implica

$$|\mathrm{Gal}(E/E^H)| \;=\; \mathrm{gr}(f(\theta, E^H)) \;\leq\; \mathrm{gr}(f) \;=\; |H|,$$

como se quería probar.
Pero $f \in E^H[X]$, efectivamente, pues $\forall\, \psi \in H$, se tiene

$$\psi(f) = \psi\Big(\prod_{\tau \in H} \big(X - \tau(\theta)\big)\Big) = \prod_{\tau \in H} \big(X - \psi \circ \tau(\theta)\big) = \prod_{\tau \in H} \big(X - \tau(\theta)\big) = f$$

ya que $H$ es un grupo y $\psi \in H$ implican $\{\psi \circ \tau,\, \tau \in H\} = \{\tau,\, \tau \in H\}$.

Esto implica que $\Phi$ es sobreyectiva (cuando $E/K$ es finita) ya que si $H < \mathrm{Gal}(E/K)$, entonces $\exists\, F/K$ subextensión de $E/K$ tq $\Phi(F) = H$: Simplemente $F = E^H$ pues

$$\Phi(E^H) \;= \mathrm{Gal}(E/E^H) = H.$$

Esto prueba (2) en el teorema 8.2.2.

■