El grupo de Galois de un campo de descomposición

Facultad de Ciencias UNAM

Introducción

En esta sección estudiaremos el grupo de Galois de un campo de descomposición. Específicamente, estudiaremos a $\mathrm{Gal}(E/F)$ donde E es un campo de descomposición sobre F. Empezamos por recordar un resultado presentado anteriormente.

Recordatorio amistoso

En el teorema 2.10.1 demostramos el siguiente resultado:

Supongamos que F, F' son campos, que $\phi : F \to F'$ es un isomorfismo de campos, que $\Phi : F[x] \to F'[x]$ es el isomorfismo entre anillos de polinomios inducido por ϕ, que $f(x) \in F[x]$, y que $f'(x) := \Phi(f(x))$.

Si E es un campo de descomposición de $f(x)$ sobre F y E' es un campo de descomposición de $f'(x)$ sobre F', entonces existe un isomorfismo $\sigma : E \to E'$ que extiende a ϕ.

En otras palabras, tenemos el siguiente diagrama conmutativo donde las flechas horizontales son isomorfismos y las flechas verticales son inclusiones.

$$\begin{array}{ccc} E & \xrightarrow{\sigma} & E' \\ \uparrow & & \uparrow \\ F & \xrightarrow{\phi} & F' \end{array}$$

En lo que sigue, usaremos este resultado para acotar a $\left|\mathrm{Gal}(E/F)\right|$.

El numero de isomorfismos que extienden a un isomorfismo dado

Proposición 1

Supongamos que F, F' son campos, que $\phi : F \to F'$ es un isomorfismo de campos, que $\Phi : F[x] \to F'[x]$ es el isomorfismo entre anillos de polinomios inducido por ϕ, que $f(x) \in F[x]$, y que $f'(x) := \Phi(f(x))$.

Si E es un campo de descomposición de $f(x)$ sobre F y E' es un campo de descomposición de $f'(x)$ sobre F', entonces

$$\left|\{\sigma : E \to E' \mid \sigma \text{ es un isomorfismo extiende a } \phi\}\right| \leq [E : F]$$

y la desigualdad se convierte en igualdad cuando $f(x)$ es separable.

Demostración. Procedemos por inducción sobre $[E : F]$.

Paso base. Si $[E : F] = 1$, entonces $E = F$, $E' = F'$, y $\sigma = \phi$. Por lo tanto,

$$\left|\{\sigma : E \to E' \mid \sigma \text{ es un isomorfismo extiende a } \phi\}\right| = 1 = [E : F].$$

Paso inductivo. Sea $n > 1$, E/F tal que $[E : F] = n$, y supongamos la hipótesis de inducción para cualquier L/K con $[L : K] < n$ (donde L es un campo de descomposición sobre K). Específicamente, supongamos el siguiente enunciado:

> *Supongamos que K, K' son campos, que $\psi : K \to K'$ es un isomorfismo de campos, que $\Psi : K[x] \to K'[x]$ es el isomorfismo entre anillos de polinomios inducido por ψ, que $g(x) \in K[x]$, y que $g'(x) := \Psi(g(x))$.*
>
> *Si L es un campo de descomposición de $g(x)$ sobre K, L' es un campo de descomposición de $g'(x)$ sobre K', y $[L : K] < n$, entonces*
>
> $$\left|\{\theta : L \to L' \mid \theta \text{ es un isomorfismo extiende a } \psi\}\right| \leq [L : K]$$
>
> *y la desigualdad se convierte en igualdad cuando $g(x)$ es separable.*

Como $[E : F] > 1$, entonces existe un factor irreducible de $f(x)$ con grado > 1, digamos $p(x)$ (de lo contrario, todos los factores irreducibles de $f(x)$ tienen grado 1, lo cual implicaría que todas las raíces de $f(x)$ viven en F, lo cual implicaría $E = F$, contradiciendo $[E : F] > 1$). También, denotemos por $p'(x)$ al correspondiente factor irreducible de $f'(x)$, es decir, $p'(x) := \Phi(p(x))$.

Ahora bien, sea $\alpha_0 \in E$ una raíz fija de $p(x)$ y denotemos $\alpha_0' := \phi(\alpha_0)$. Es fácil verificar que α_0' es una raíz de $p'(x)$. Por el teorema 2.5.4 existe un isomorfismo $\tau : F(\alpha_0) \to F'\left(\phi(\alpha_0)\right)$ que extiende a ϕ. Es decir, tenemos el siguiente diagrama conmutativo

$$\begin{array}{ccc} F(\alpha_0) & \xrightarrow{\tau} & F'(\alpha_0') \\ \uparrow & & \uparrow \\ F & \xrightarrow{\phi} & F' \end{array}$$

Por otro lado, es fácil verificar que E es campo de descomposición de $f(x)$ sobre $E(\alpha_0)$ y que E' es campo de descomposición de $f'(x)$ sobre $F'\left(\phi(\alpha_0)\right)$. Entonces por el teorema 2.10.1 existe $\sigma : E \to E'$ isomorfismo tal que el siguiente diagrama es conmutativo

$$\begin{array}{ccc} E & \xrightarrow{\sigma} & E' \\ \uparrow & & \uparrow \\ F(\alpha_0) & \xrightarrow{\tau} & F'(\alpha_0') \end{array}$$

Juntando estos dos diagramas obtenemos el siguiente diagrama

$$\begin{array}{ccc} E & \xrightarrow{\sigma} & E' \\ \uparrow & & \uparrow \\ F(\alpha_0) & \xrightarrow{\tau} & F'(\alpha_0') \\ \uparrow & & \uparrow \\ F & \xrightarrow{\phi} & F' \end{array}$$

Denotemos

$$A = \left\{\tau : F(\alpha_0) \to F'(\alpha_0') \mid \tau \text{ es un isomorfismo que extiende a } \phi\right\}$$

y veamos que

$$\{\sigma : E \to E' \mid \sigma \text{ es un isomorfismo extiende a } \phi\} = \bigcup_{\tau \in A} \left\{\sigma : E \to E' \mid \sigma \text{ es un isomorfismo que extiende a } \tau\right\}.$$

$\subset$) Si $\sigma : E \to E'$ es un isomorfismo que extiende a ϕ, entonces σ extiende a $\sigma \restriction_{F(\alpha_0)} \in A$.

$\supset$) Es consecuencia inmediata de que toda $\tau \in A$ extiende a ϕ.

Usando la ecuación anterior obtenemos que

$$\left|\{\sigma : E \to E' \mid \sigma \text{ es un isomorfismo extiende a } \phi\}\right| =$$

$$\left|\bigcup_{\tau \in A} \{\sigma : E \to E' \mid \sigma \text{ es un isomorfismo que extiende a } \tau\}\right| =$$

$$\sum_{\tau \in A} \left|\{\sigma : E \to E' \mid \sigma \text{ es un isomorfismo que extiende a } \tau\}\right| \qquad (1)$$

Ahora bien, sea $\tau \in A$. Como

- τ es un isomorfismo de $F(\alpha_0)$ en $F'(\alpha_0')$,
- E es un campo de descomposición de $f(x)$ sobre $F(\alpha_0)$,
- E' es un campo de descomposición de $f'(x)$ sobre $F'(\alpha_0')$, y
- $[E : F(\alpha_0)] < [E : F] = n$ (pues $[E : F] = [E : F(\alpha_0)][F(\alpha_0) : F]$ y $[F(\alpha_0) : F] > 1$),

entonces la hipótesis de inducción implica que

$$\left|\{\sigma : E \to E' \mid \sigma \text{ es un isomorfismo que extiende a } \tau\}\right| \leq [E : F(\alpha_0)] \qquad (2)$$

y la desigualdad se convierte en igualdad cuando $f(x)$ es separable.

Juntando (1) y (2) obtenemos

$$\begin{aligned}\Big|\{\sigma : E \to E' \mid \sigma \text{ es un isomorfismo extiende a } \phi\}\Big| &\leq \sum_{\tau \in A} [E : F(\alpha_0)] \\ &= |A| \cdot [E : F(\alpha_0)] \qquad (3)\end{aligned}$$

y la desigualdad se convierte en igualdad cuando $f(x)$ es separable.

Por otro lado, notemos que si $\tau \in A$ (es decir, $\tau : F(\alpha_0) \to F'(\alpha_0')$ es un isomorfismo que extiende a ϕ), entonces τ queda completamente determinado por su valor en α_0. Como $\tau(\alpha_0)$ es necesariamente una raíz de $p(x)$, entonces hay tantos τ's como hay raíces de $p(x)$. Mas aun, como α es raíz de $p(x)$ y $p(x)$ es irreducible, entonces el corolario 2.5.2 implica que $[F(\alpha) : F] = \deg p(x)$. Juntando todo esto obtenemos

$$\begin{aligned}|A| &= \Big|\big\{\tau : F(\alpha_0) \to F'(\alpha_0') \mid \tau \text{ es iso que extiende a } \phi\big\}\Big| \\ &= \Big|\{\text{raíces de } p(x)\}\Big| \leq \deg p(x) = [F(\alpha) : F] \qquad (4)\end{aligned}$$

Notemos que la desigualdad anterior se convierte en igualdad cuando $p(x)$ tiene $\deg p(x)$ raíces distintas o equivalentemente, cuando $p(x)$ es separable.

Juntando (3) y (4) obtenemos

$$\left|\{\sigma : E \to E' \mid \sigma \text{ es un isomorfismo extiende a } \phi\}\right| \leq$$
$$|A| \cdot [E : F(\alpha_0)] \leq [F(\alpha_0) : F][E : F(\alpha_0)] = [E : F]$$

y la primera desigualdad se convierte en igualdad cuando $f(x)$ es separable y la segunda desigualdad se convierte en igualdad cuando $p(x)$ es separable. En particular, como $p(x)$ es un factor de $f(x)$, entonces ambas desigualdades se convierten en igualdades cuando $f(x)$ es separable. $\square$

$\left|\mathrm{Gal}(E/F)\right| \leq [E : F]$ si E es un campo de descomposición sobre F

Corolario 2

Supongamos que F es un campo y que $f(x) \in F[x]$. Si E es un campo de descomposición de $f(x)$ sobre F, entonces

$$\left|\mathrm{Gal}(E/F)\right| \leq [E : F]$$

y la desigualdad se convierte en igualdad si $f(x)$ es separable.

Demostración. Poniendo $F' := F$ y $\phi := \mathrm{id}_E$ en la proposición anterior obtenemos

$$\begin{aligned}\left|\mathrm{Gal}(E/F)\right| &= \left|\{\sigma : E \to E \mid \sigma \text{ es un isomorfismo extiende a } \mathrm{id}_E\}\right| \\ &= \left|\{\sigma : E \to E' \mid \sigma \text{ es un isomorfismo extiende a } \phi\}\right| \leq [E : F]\end{aligned}$$

donde la primera igualdad es consecuencia inmediata de la definición de $\mathrm{Gal}(E/F)$. □

Grupo de Galois de un polinomio

Definición

Supongamos que F es un campo, que $f(x) \in F[x]$, y que E es un campo de descomposición de $f(x)$ sobre F. Definimos **el grupo de Galois de** $f(x)$ **sobre** F como $\mathrm{Gal}(E/F)$.

Como

- cualesquiera dos campos de descomposición de $f(x)$ sobre E son isomorfos y
- $\mathrm{Gal}(K/F) \cong \mathrm{Gal}(L/F)$ si $K \cong L$,

entonces la definición anterior no depende (salvo isomorfismo) del campo de descomposición que escojamos.

El grupo de Galois de un polinomio es isomorfo a un subgrupo de S_n, $n =$ numero de raíces del polinomio

Proposición 3

Supongamos que F es un campo y que $f(x) \in F[x]$. Si E es un campo de descomposición de $f(x)$ sobre F y $f(x)$ tiene n raíces distintas, entonces $\mathrm{Gal}(E/F)$ es isomorfo a un subgrupo de S_n.

Demostración. Como es de esperarse, demostraremos que existe un homomorfismo inyectivo de $\mathrm{Gal}(E/F)$ en S_n. Para esto, empecemos por suponer que $\alpha_1, \ldots, \alpha_n$ son las n distintas raíces de $f(x)$. Cabe recalcar que en lo que sigue, el orden/numeración que acabamos de darle a las raíces es importante y esta fijo.

Con esto en mente, supongamos que $\sigma \in \mathrm{Gal}(E/F)$. Como los elementos de $\mathrm{Gal}(E/F)$ mapean raíces de $f(x)$ en raíces de $f(x)$, entonces para cada $i \in \{1, \ldots, n\}$ existe un único[1] $\theta_\sigma(i) \in \{1, \ldots, n\}$ tal que $\sigma(\alpha_i) = \alpha_{\theta_\sigma(i)}$.

[1] Si no fuera único, σ ni si quiera seria una función bien definida.

Veamos que para cada $\sigma \in \mathrm{Gal}(E/F)$ la correspondencia $i \mapsto \theta_\sigma(i)$ es una función biyectiva.

- θ_σ *es una función bien definida*: Supongamos que $\alpha_i = \alpha_j$, entonces $\sigma(\alpha_i) = \sigma(\alpha_j)$. Supongamos que $\sigma(\alpha_i) = \alpha_k = \sigma(\alpha_j)$. Por definición de θ_σ lo anterior implica que $\theta_\sigma(i) = k = \theta_\sigma(j)$.
- θ_σ *es inyectiva*: Si $\theta_\sigma(i) = \theta_\sigma(j)$, entonces

$$\sigma(\alpha_i) = \alpha_{\theta_\sigma(i)} = \alpha_{\theta_\sigma(j)} = \sigma(\alpha_j).$$

  Como σ es un automorfismo, lo anterior implica que $\alpha_i = \alpha_j$ y como supusimos que $\alpha_1, \ldots, \alpha_n$ son distintas, entonces $i = j$.
- θ_σ *es suprayectiva*: Supongamos que $j \in \{1, \ldots, n\}$. Como $\sigma \in \mathrm{Aut}(E/F)$, entonces $\sigma^{-1} \in \mathrm{Aut}(K/F)$. Por lo tanto, $\sigma^{-1}(\alpha_j) \in \{\alpha_1, \ldots, \alpha_n\}$. En particular, existe $i \in \{1, \ldots, n\}$ tal que $\sigma^{-1}(\alpha_j) = \alpha_i$. De donde, $\alpha_j = \sigma(\alpha_i)$. Por definición de θ_σ, lo anterior implica que $\theta_\sigma(i) = j$.

Por definición de S_n, lo anterior es equivalente a que $\theta_\sigma \in S_n$ para cada $\sigma \in \mathrm{Gal}(E/F)$.

Sea $\Theta : \mathrm{Gal}(E/F) \to S_n$ tal que $\Theta(\sigma) = \theta_\sigma$.

Veamos que Θ es un homomorfismo de grupos inyectivo.

- Θ *es un homomorfismo*: Supongamos que $\sigma_1, \sigma_2 \in \mathrm{Gal}(E/F)$. Entonces para cada $i \in \{1, \ldots, n\}$ tenemos que

$$\begin{aligned} \alpha_{\theta_{\sigma_1 \circ \sigma_2}(i)} = \sigma_1 \circ \sigma_2(\alpha_i) = \sigma_1\left(\sigma_2(\alpha_i)\right) = \sigma_1\left(\alpha_{\theta_{\sigma_2}(i)}\right) &= \alpha_{\theta_{\sigma_1}\left(\theta_{\sigma_2}(i)\right)} \\ &= \alpha_{\left(\theta_{\sigma_1} \circ \theta_{\sigma_2}\right)(i)} \end{aligned}$$

  De donde, $\theta_{\sigma_1 \circ \sigma_2}(i) = \left(\theta_{\sigma_1} \circ \theta_{\sigma_2}\right)(i)$ para toda i. Por lo tanto,

$$\Theta(\sigma_1 \circ \sigma_2) = \theta_{\sigma_1 \circ \sigma_2} = \theta_{\sigma_1} \circ \theta_{\sigma_2} = \Theta(\sigma_1) \circ \Theta(\sigma_2)$$

- Θ *es inyectivo*: Supongamos que $\theta_{\sigma_1} = \theta_{\sigma_2}$. Queremos ver que $\sigma_1 = \sigma_2$. Como $E = F(\alpha_1, \ldots, \alpha_n)$, entonces existen $m_1, \ldots, m_n \in \mathbb{Z}_{\geq 0}$ tales que

$$\left\{ \alpha_1^{j_1} \alpha_2^{j_2} \cdots \alpha_m^{j_m} \mid j_l \in \{0, 1 \ldots, m_i - 1\} \text{ para cada } l \in \{1, 2, \ldots, k\} \right\}$$

  es una F-base de E. Por lo tanto, basta probar que $\sigma_1(\alpha_i) = \sigma_2(\alpha_i)$ para toda i. Pero por definición para toda i tenemos

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

Comentario

En lo que sigue, usaremos la misma notación que en la proposición anterior. Por el teorema de Lagrange[2], la proposición anterior implica que

$$\left|\mathrm{Gal}(E/F)\right| \text{ divide a } |S_n| = n!$$

Mas aun, si suponemos que $f(x)$ es separable, entonces

- $n =$ numero de raíces del polinomio $= \deg f(x)$ y
- $\left|\mathrm{Gal}(E/F)\right| = [E : F]$.

Por lo tanto, tenemos el siguiente resultado:

Corolario 4

Si E es el campo de descomposición de $f(x)$ sobre F y $f(x)$ es separable, entonces $[E : F]$ divide a $n!$ donde $n = \deg f(x)$.

Concluimos esta sección con mas aplicaciones de la proposición anterior.

[2] Una de las consecuencias del teorema de Lagrange es que si G es un grupo y H es un subgrupo de G, entonces $|H|$ divide a $|G|$.

El grupo de Galois de $(x^2-2)(x^2-3)$ sobre $\mathbb{Q}$

El campo de descomposición de $(x^2-2)(x^2-3)$ sobre $\mathbb{Q}$ es $\mathbb{Q}(\sqrt{2},\sqrt{3})$. Como $(x^2-2)(x^2-3)$ tiene 4 raíces distintas, entonces (por la proposición 3) $\mathbb{Q}(\sqrt{2},\sqrt{3})$ es isomorfo a un subgrupo de S_4. Determinemos explícitamente a este subgrupo. Para esto, recordemos que en el la sección anterior vimos que

$$\mathbb{Q}(\sqrt{2},\sqrt{3}) = \{1, \sigma, \tau, \sigma\tau\}$$

donde

$$\sigma : \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{cases} \qquad \tau : \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases}$$

Denotemos

$$\alpha_1 = \sqrt{2}, \quad \alpha_2 = -\sqrt{2}, \quad \alpha_3 = \sqrt{3}, \quad \alpha_4 = -\sqrt{3}.$$

Como σ fija a α_3, α_4 e intercambia a α_1, α_2, entonces (usando la notación de la proposición 3) $\theta_\sigma = (12)$. De manera análoga $\theta_\tau = (34)$. Por lo tanto,

$$\mathbb{Q}(\sqrt{2},\sqrt{3}) \cong \{\mathrm{id}, (12), (34), (12)(34)\} \subset S_4.$$

El grupo de Galois de $x^3 - 2$ es isomorfo a S_3

En la sección anterior vimos que si K es el campo de descomposición de $x^3 - 2$, entonces

$$\mathrm{Gal}(K/F) = \left\{1, \sigma, \sigma^2, \tau, \sigma\tau, \tau\sigma\right\}$$

donde

$$\sigma : \begin{cases} \sqrt[3]{2} \mapsto \zeta\sqrt[3]{2} \\ \zeta \mapsto \zeta \end{cases} \qquad \tau : \begin{cases} \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ \zeta \mapsto \zeta^2 \end{cases}$$

y $\zeta = \frac{-1+i\sqrt{3}}{2}$.

Por otro lado, como $x^3 - 2$ tiene 3 raíces distintas, entonces $\mathrm{Gal}(K/F)$ es isomorfo a un subgrupo de S_3. Pero $\left|\mathrm{Gal}(K/F)\right| = 6 = 3! = |S_3|$ y por lo tanto, $\mathrm{Gal}(K/F) \cong S_3$.