El polinomio universal y su grupo de Galois

Facultad de Ciencias UNAM

Introducción

En esta sección definiremos a un polinomio particularmente importante llamado el polinomio universal. Calcularemos su campo de descomposición (sobre el campo mas chico que contiene a sus coeficientes) y veremos su grupo de Galois (sobre el mismo campo) es isomorfo a S_n. Antes de hacer esto, recordamos el concepto de campos de fracciones.

Supongamos que $(R, +, \times)$ es un dominio entero con unidad. El campo de fracciones de R, es el campo $(L_R, \oplus, \otimes)$ donde

$$L_R = \left\{ \frac{a}{b} \mid a \in R, b \in R \setminus \{0\} \right\},$$

$$\frac{a}{b} \oplus \frac{c}{d} = \frac{(a \times d) + (b \times c)}{b \times d},$$

$$\frac{a}{b} \otimes \frac{c}{d} = \frac{a \times c}{b \times d},$$

donde $\frac{a}{b}$ es la clase de equivalencia de la pareja ordenada (a, b) bajo la relación $(a, b) \sim (c, d) \iff a \times d = b \times c$.

En palabras, L_R es el campo que tiene como elementos a los cocientes de elementos de R y las operaciones son análogas a las de $\mathbb{Q}$.

El campo de funciones racionales en varias variables

Definición

Supongamos que F es un campo y que $x_1, \ldots, x_n$ son variables indeterminadas. Como $F[x_1, \ldots, x_n]$ es un dominio entero, podemos definir su campo de fracciones

$$F(x_1, \ldots, x_n) = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in F[x] \text{ y } g(x) \neq 0 \right\}.$$

La extensión de un isomorfismo de campos $R \to R$ a un automorfismo de su campo de fracciones

Lema 1

Supongamos que R es un dominio entero y que K es su campo de fracciones. Si $\phi : R \to R$ es un isomorfismo de anillos, entonces existe un único isomorfismo de campos $\Phi : K \to K$ tal que $\Phi \restriction_R = \phi$.

En particular, como $F(x_1, \ldots, x_n)$ es el campo de fracciones de $F[x_1, \ldots, x_n]$, entonces todo isomorfismo de anillos $\phi : F[x_1, \ldots, x_n] \to F[x_1, \ldots, x_n]$ se extiende a un isomorfismo de campos $\Phi : F(x_1, \ldots, x_n) \to F(x_1, \ldots, x_n)$.

Demostración. Naturalmente, definimos

$$\begin{aligned} \Phi : K &\to K \\ \frac{a}{b} &\mapsto \frac{\phi(a)}{\phi(b)} \end{aligned}$$

El lector podrá fácilmente verificar que de esta manera, Φ satisface lo deseado. □

El polinomio universal

Definición

Supongamos que F es un campo y que $x_1, \ldots, x_n, x$ son variables indeterminadas. Definimos el **polinomio universal de** $F[x_1, \ldots, x_n, x]$ por

$$\tilde{f}(x_1, \ldots, x_n, x) = (x - x_1)(x - x_2) \cdots (x - x_n) \in F[x_1, \ldots, x_n, x].$$

Por otro lado, recordemos que

$$F[x_1, \ldots, x_n, x] = \left(F[x_1, \ldots, x_n]\right)[x]$$

y por lo tanto, podemos ver a $\tilde{f}(x_1, \ldots, x_n, x)$ como un polinomio en x con coeficientes en $F[x_1, \ldots, x_n]$. En lo que sigue, veremos que podemos decir todavía mas acerca de los coeficientes de $\tilde{f}(x_1, \ldots, x_n, x)$.

$\tilde{f}(x_1, \ldots, x_n, x) \in \big(F(\sigma_1, \ldots, \sigma_n)\big)[x]$

Supongamos que $\sigma_1, \ldots, \sigma_n$ son los polinomios simétricos elementales de $F[x_1, \ldots, x_n]$. Específicamente, supongamos que

$$\sigma_j(x_1, \ldots, x_n) = \sum_{1 \leq i_1 < \cdots < i_j \leq n} x_{i_1} x_{i_2} \cdots x_{i_j}$$

En la proposición 2.16.1 demostramos que

$$(x - x_1) \cdots (x - x_n) = x^n - \sigma_1 x^{n-1} + \cdots + (-1)^j \sigma_j x^{n-j} + \cdots + (-1)^n \sigma_n$$

donde $\sigma_j = \sigma_j(x_1, \ldots, x_n)$ y por lo tanto,

$$\tilde{f}(x_1, \ldots, x_n, x) \in \big(F(\sigma_1, \ldots, \sigma_n)\big)[x].$$

Cabe recalcar que en lo anterior $F(\sigma_1, \ldots, \sigma_n)$ es (como has de esperar) el subcampo de $F(x_1, \ldots, x_n)$ generado por F y $\sigma_1, \ldots, \sigma_n$.

Mas aun, cuando consideremos a $\tilde{f}(x_1, \ldots, x_n, x)$ como elemento de $\big(F(\sigma_1, \ldots, \sigma_n)\big)[x]$, lo denotamos por $\tilde{f}(x)$.

El campo de descomposición del polinomio universal

Proposición 2

Supongamos que F es un campo y que $x_1, \ldots, x_n, x$ son variables indeterminadas. Entonces el campo de descomposición de $\tilde{f}(x)$ sobre[1] $F(\sigma_1, \ldots, \sigma_n)$ es $F(x_1, \ldots, x_n)$.

Demostración. Obviamente, $\tilde{f}(x) = (x - x_1) \cdots (x - x_n)$ se descompone en $F(x_1, \ldots, x_n)/F$. Resta probar que no existe L campo tal que $F(\sigma_1, \ldots, \sigma_n) \subset L \subsetneq F(x_1, \ldots, x_n)$ en donde $\tilde{f}(x)$ se descompone. Como es usual, supongamos lo contrario y denotemos por L a este campo. Como $\tilde{f}(x)$ se descompone en L/F, existen $a_1, \ldots, a_n \in L$ tales que

$$\tilde{f}(x) = (x - a_1) \cdots (x - a_n).$$

Pero como (i) $\tilde{f}(x) = (x - x_1) \cdots (x - x_n)$ y (ii) $\left(F(\sigma_1, \ldots, \sigma_n)\right)[x]$ es un DFU, entonces (después de un reacomodo) $a_i = x_i$ para toda $i = 1, \ldots, n$. Esto implica $F(x_1, \ldots, x_n) \subset L$, contradiciendo $L \subsetneq F(x_1, \ldots, x_n)$. □

[1] Recuerda que $\tilde{f}(x) = \tilde{f}(x_1, \ldots, x_n, x) \in \left(F(\sigma_1, \ldots, \sigma_n)\right)[x]$.

Comentario

En lo que sigue, veremos que el grupo de Galois de $\tilde{f}(x)$ sobre $F(\sigma_1, \ldots, \sigma_n)$ es isomorfo a S_n. Específicamente, veremos que

$$\mathrm{Gal}\left(F(x_1, \ldots, x_n)/F(\sigma_1, \ldots, \sigma_n)\right) \cong S_n.$$

Antes de esto, introducimos un poquito de notación.

El isomorfismo ϕ_τ

Definición

Supongamos que F es un campo y que $x_1, \ldots, x_n$ son variables indeterminadas. Para cada $\tau \in S_n$, definimos

$$\phi_\tau : F[x_1, \ldots, x_n] \to F[x_1, \ldots, x_n]$$

como el homomorfismo de anillos que satisface

$$a \mapsto a \text{ si } a \in F \quad \text{y} \quad x_i \mapsto x_{\tau(i)} \text{ para toda } i = 1, \ldots, n.$$

En palabras, $\phi_\tau\left(f(x_1, \ldots, x_n)\right)$ es el polinomio[2] obtenido a través de permutar las variables de $f(x_1, \ldots, x_n)$ usando a τ. Mas aun, el lector podrá fácilmente verificar que ϕ_τ es de hecho un isomorfismo.

Por ejemplo, si $F = \mathbb{Q}$, $n = 3$, y $f(x) = 3x_1x_2x_3 + 5x_1$, entonces

$$\phi_\tau\left(f(x_1, x_2, x_3)\right) = \phi_\tau(3x_1x_2x_3 + 5x_1) = 3x_{\tau(1)}x_{\tau(2)}x_{\tau(3)} + 5x_{\tau(1)}.$$

[2] Cabe recalcar que si seguimos con nuestra notación usual de polinomios y funciones, deberíamos de escribir $\left(\phi_\tau\left(f(x_1, \ldots, x_n)\right)\right)(x_1, \ldots, x_n)$ en vez de $\phi_\tau\left(f(x_1, \ldots, x_n)\right)$, pero por brevedad preferimos esta notación.

El grupo de Galois de $\tilde{f}(x)$ sobre $F(\sigma_1, \ldots, \sigma_n)$ es S_n

Teorema 3

Supongamos que F es un campo y que $x_1, \ldots, x_n, x$ son variables indeterminadas. Entonces el grupo de Galois de $\tilde{f}(x)$ sobre $F(\sigma_1, \ldots, \sigma_n)$ es isomorfo a S_n.

Demostración. Como $F(x_1, \ldots, x_n)$ es el campo de descomposición de $\tilde{f}(x)$ sobre $F(\sigma_1, \ldots, \sigma_n)$, entonces el resultado deseado es equivalente a que

$$\text{Gal}\left(F(x_1, \ldots, x_n)/F(\sigma_1, \ldots, \sigma_n)\right) \cong S_n.$$

Para ver este isomorfismo, recordemos que en la sección anterior demostramos que el grupo de Galois de un polinomio es isomorfo a un subgrupo de S_n donde $n =$ numero de raíces del polinomio. Mas aun, recordemos que para demostrar esto, demostramos la existencia de un homomorfismo inyectivo del grupo de Galois del polinomio en S_n. En lo que sigue, veremos que con las hipótesis adicionales de esta proposición, este homomorfismo también es suprayectivo.

Antes que nada, recordemos como esta definido (anteriormente, lo habíamos definido en el caso general, pero ahora lo vamos a definir usando la notación del caso en el que estamos). Por brevedad, en lo que sigue, denotamos

$$K = F(\sigma_1, \ldots, \sigma_n) \quad \text{y} \quad L = F(x_1, \ldots, x_n).$$

Ahora si, dado un elemento de $\mathrm{Gal}(L/K)$, vamos a construir un elemento de S_n. Supongamos que $\sigma \in \mathrm{Gal}(L/K)$. Como (i) los elementos de $\mathrm{Gal}(E/F)$ mapean raíces de $\tilde{f}(x)$ en raíces de $\tilde{f}(x)$ y (ii) las raíces de $\tilde{f}(x)$ son $x_1, \ldots, x_n$, entonces para cada $i \in \{1, \ldots, n\}$ existe un único $\theta_\sigma(i) \in \{1, \ldots, n\}$ tal que $\sigma(x_i) = x_{\theta_\sigma(i)}$.

En la sección anterior demostramos que la correspondencia $i \overset{\theta_\sigma}{\longmapsto} \theta_\sigma(i)$ es una biyeccion y por lo tanto, pertenece a S_n. Finalmente, el homomorfismo buscado es

$$\begin{aligned} \Theta : \mathrm{Gal}(L/K) &\to S_n \\ \sigma &\mapsto \theta_\sigma. \end{aligned}$$

En palabras, $\Theta(\sigma)$ es la permutación en los índices de las x_i inducida por σ.

Para ver que en este caso Θ es suprayectivo, supongamos que $\tau \in S_n$ y considera el isomorfismo de anillos

$$\phi_\tau : F[x_1, \ldots, x_n] \to F[x_1, \ldots, x_n]$$

(definido justo antes de este teorema).

Por el lema 1, existe un (único) isomorfismo de campos

$$\Phi_\tau : F(x_1, \ldots, x_n) \to F(x_1, \ldots, x_n)$$

que extiende a ϕ_τ.

En lo que sigue, veremos que $\Phi_\tau \in \mathrm{Gal}(L/K)$ y que $\Theta(\Phi_\tau) = \tau$. Como Φ_τ es un isomorfismo de campos de $L = F(x_1, \ldots, x_n)$ en si mismo, para ver que $\Phi_\tau \in \mathrm{Gal}(L/K)$, solo resta probar que Φ_τ fija a $K = F(\sigma_1, \ldots, \sigma_n)$. Primero notemos que para toda $j = 1, \ldots, n$ tenemos que

$$\begin{aligned}\Phi_\tau(\sigma_j) = \phi_\tau(\sigma_j) &= \phi_\tau\left(\sum_{1 \le i_1 < \cdots < i_j \le n} x_{i_1} x_{i_2} \cdots x_{i_j}\right) \\ &= \sum_{1 \le i_1 < \cdots < i_j \le n} x_{\tau(i_1)} x_{\tau(i_2)} \cdots x_{\tau(i_j)} = \sum_{1 \le i_1 < \cdots < i_j \le n} x_{i_1} x_{i_2} \cdots x_{i_j} = \sigma_j.\end{aligned}$$

En palabras, Φ_τ fija a todos los σ_j. Por otro lado, recordemos que existen $m_1, \ldots, m_n \in \mathbb{Z}$ tales que

$$\left\{ \sigma_1^{j_1} \sigma_2^{j_2} \cdots \sigma_m^{j_m} \mid j_i \in \{0, 1 \ldots, n_i - 1\} \text{ para cada } i \in \{1, \ldots, n\} \right\}$$

es una F-base de $F(\sigma_1, \ldots, \sigma_n)$ (c.f. proposición 2.7.6). Juntando esto con el hecho de que Φ_τ fija a todos los σ_j, obtenemos que Φ_τ fija a $F(\sigma_1, \ldots, \sigma_n) = K$. Como mencionamos anteriormente, esto implica que $\Phi_\tau \in \mathrm{Gal}(L/K)$.

Resta probar que $\Theta(\Phi_\tau) = \tau$.

Por definición, Φ_τ satisface $x \mapsto x_{\tau(i)}$ para toda i. En palabras, la permutación en los índices de las x_i inducida por Φ_τ es τ. Pero (también por definición) $\Theta(\Phi_\tau)$ es la permutación en los índices de las x_i inducida por Φ_τ, pero (también por definición). Por lo tanto, $\Theta(\Phi_\tau) = \tau$.

Lo anterior implica que $\Theta : \mathrm{Gal}(L/K) \to S_n$ es suprayectivo y como ya sabíamos que es un homomorfismo inyectivo, entonces $\mathrm{Gal}(L/K) \cong S_n$. $\square$