El teorema del elemento primitivo

Facultad de Ciencias UNAM

Introducción

En esta sección reanudamos nuestro estudio de polinomios separables. El objetivo es demostrar un resultado conocido como el *teorema del elemento primitivo*. Este resultado sera útil cuando estudiemos teoría de Galois. Empezamos por presentar algunas definiciones básicas.

Campos separables

Definición

Supongamos que K/F es una extensión algebraica.

- Decimos que $\alpha \in K$ es **separable sobre** F si $m_{\alpha,F}(x)$ (su polinomio mínimo sobre F) es separable.
- Decimos que K/F es una **extensión separable** si todo $\alpha \in K$ es separable sobre F.

Notemos que como "polinomio irreducible $\implies$ polinomio separable" en campos con característica 0 y en campos finitos, entonces K/F es separable si F tiene característica 0 o F es finito. Esta es una de las razones por las que en futuras secciones a veces suponemos que todos los campos de esa sección tienen característica 0.

Toda extensión algebraica sobre un campo finito o sobre un campo con característica 0, es separable

Proposición 1

Supongamos que K/F es una extensión algebraica de campos.

1. Si $\mathrm{ch}(F) = 0$, entonces K es separable sobre F.
2. Si F finito, entonces K es separable sobre F.

Demostración. Por definición, hay que demostrar que $m_{\alpha,F}(x)$ es separable para toda $\alpha \in K$. Sin embargo, esto es consecuencia inmediata de los siguientes recordatorios.

- Para toda $\alpha \in K$, el polinomio $m_{\alpha,F}(x)$ es irreducible en $F[x]$.
- En campos con característica 0, irreducible $\implies$ separable (c.f. corolario 2.14.6).
- En campos finitos, irreducible $\implies$ separable (c.f. proposición 2.14.8).

□

El paso base del caso infinito del teorema del elemento primitivo

Lema 2

Supongamos que K/F es una extensión de campos y que K es infinito. Si $K = F(\beta, \gamma)$ con $\beta, \gamma \in K$ separables sobre F, entonces existe $\lambda \in F$ tal que

$$K = F(\beta, \gamma) = F(\beta + \lambda\gamma)$$

y $\beta + \lambda\gamma$ es separable sobre F.

Demostración. Supongamos que $\beta, \gamma \in K$ son separables sobre F, que $K = F(\beta, \gamma)$, y denotemos

$$f(x) = m_{\beta,F}(x), \quad g(x) = m_{\gamma,F}(x), \quad l = \deg f(x), \quad m = \deg g(x).$$

Si L es un campo de separación de $f(x)g(x)$, entonces existen

- $\beta_1, \ldots, \beta_l \in L$ distintas por pares y
- $\gamma_1, \ldots, \gamma_m \in L$ distintas por pares

tales que

$$f(x) = (x - \beta_1)(x - \beta_2) \cdots (x - \beta_l) \text{ y}$$
$$g(x) = (x - \gamma_1)(x - \gamma_2) \cdots (x - \gamma_m)$$

Ahora bien, como F es infinito, existe $\lambda \in F$ tal que

$$\lambda \neq \frac{\beta_i - \beta_r}{\gamma_s - \gamma_j} \quad \text{para toda} \quad 1 \leq r, i \leq l, \quad 1 \leq s, j \leq m, \quad s \neq j.$$

De donde,

$$\beta_r + \lambda\gamma_s \neq \beta_i + \lambda\gamma_j \text{ para } (r,s) \neq (i,j). \tag{1}$$

En particular, como $\beta = \beta_1$ y $\gamma = \gamma_1$, entonces

$$\beta + \lambda\gamma \neq \beta_i + \lambda\gamma_j \text{ para } 1 \leq i \leq l \text{ y } 2 \leq j \leq m. \tag{2}$$

En lo que sigue, veremos que $\beta + \lambda\gamma$ es el elemento primitivo[1] buscado. Específicamente, veremos que

$$F(\beta, \gamma) = F(\beta + \lambda\gamma)$$

La inclusión $\supset$ es consecuencia inmediata de la definición de $F(\beta + \lambda\gamma)$ y de que $F(\beta, \gamma)$ contiene a F y a $\beta + \lambda\gamma$.

De manera análoga, para la inclusión $\subset$, basta demostrar que $\beta, \gamma \in F(\beta + \lambda\gamma)$.

[1] Recuerda que si K/F es una extensión tal que $K = F(\alpha)$ para alguna $\alpha \in K$, entonces decimos que α es un elemento primitivo de la extensión.

Empecemos por ver que $\gamma \in F(\beta + \lambda\gamma)$. Primero, notemos que γ es raíz de los siguientes dos polinomios en $F(\beta + \lambda\gamma)[x]$.

$$g(x) \quad \text{y} \quad f(\beta + \lambda\gamma - \lambda x)$$

Supongamos que $h(x) \in F(\beta + \lambda\gamma)[x]$ es un mcd en $F(\beta + \lambda\gamma)[x]$ de estos dos polinomios y que además es un polinomio mónico. Como γ es raíz de ambos polinomios, entonces[2] γ también es raíz de $h(x)$. Como $h(x)$ es mónico, es fácil ver que tenemos la primera de las siguientes implicaciones.

$$\deg h(x) = 1 \implies h(x) = x - \gamma \implies \gamma \in F(\beta + \lambda\gamma)[x] \tag{3}$$

Donde la segunda implicación es consecuencia de que $h(x) \in F(\beta + \lambda\gamma)[x]$. Por eso, en lo que sigue demostraremos que $\deg h(x) = 1$. Para esto, veremos que los otros casos llevan a contradicciones.

[2] Recuerda que por definición de mcd, todo divisor común de $g(x)$ y $f(\beta + \lambda\gamma - \lambda x)$ también es divisor de $h(x)$.

Primero, veamos que $\deg h(x) \neq 0$. Si $\deg h(x) = 0$, entonces el 1 también es m.c.d y por lo tanto, existirían $A(x), B(x) \in F(\beta + \lambda\gamma)[x]$ tales que

$$A(x)g(x) + B(x)f(\beta + \lambda\gamma - \lambda x) = 1.$$

Evaluando en $x = \gamma$ obtendríamos $0 = 1$ y por lo tanto $\deg h(x) \neq 0$.

Ahora, veamos que $\deg h(x) \not> 1$. Supongamos que $\deg h(x) > 1$. Como $h(x)|g(x)$, entonces

- $h(x)$ es separable y
- toda raíz de $h(x)$ también es raíz de $g(x)$.

Usando esto y la suposición de que $\deg h(x) > 1$, es fácil ver que existe $i \in \{2, \ldots, m\}$ tal que γ_i es raíz de $h(x)$ (recuerda que las raíces de $g(x)$ son precisamente $\gamma = \gamma_1, \gamma_2, \ldots, \gamma_m$).

Pero $h(x)$ también divide a $f(\beta + \lambda\gamma - \lambda x)$ y por lo tanto, γ_i también es raíz de $f(\beta + \lambda\gamma - \lambda x)$ o equivalentemente, $\beta + \lambda\gamma - \lambda\gamma_i$ es raíz de $f(x)$. Pero como las raíces de $f(x)$ son precisamente $\beta = \beta_1, \beta_2, \ldots, \beta_l$, entonces

$$\beta + \lambda\gamma - \lambda\gamma_i = \beta_j \text{ para alguna } j \in \{1, \ldots, l\}.$$

Contradiciendo (2). Recordemos que ahí vimos que

$$\beta + \lambda\gamma \neq \beta_i + \lambda\gamma_j \text{ para } 1 \leq i \leq l \text{ y } 2 \leq j \leq m$$

y por lo tanto, $\deg h(x) \not> 1$.

Juntando esto con el hecho de que $\deg h(x) \neq 0$, obtenemos que $\deg h(x) = 1$ y por (3), también obtenemos $\gamma \in F(\beta + \lambda\gamma)[x]$.

En particular, como $\lambda \in F$, entonces $\lambda\gamma \in F(\beta + \lambda\gamma)$ y por lo tanto, $\beta = (\beta + \lambda\gamma) - \lambda\gamma \in F(\beta + \lambda\gamma)$.

Lo anterior completa nuestra demostración de que $F(\beta, \gamma) = F(\beta + \lambda\gamma)$.

Falta probar que $\beta + \lambda\gamma$ es separable sobre F. Queremos ver que el polinomio mínimo de $\beta + \lambda\gamma$ sobre F, el cual denotaremos por $p(x) \coloneqq m_{\beta+\lambda\gamma,F}(x)$, es separable. Para esto, demostraremos que existe un polinomio separable divisible por $p(x)$ (es fácil ver que todo divisor no constante de un polinomio separable es un polinomio separable).

Considera

$$s(x) \coloneqq \prod_{j=1}^{m} f(x - \lambda\gamma_j).$$

Como

$$f(x) = (x - \beta_1)(x - \beta_2)\cdots(x - \beta_l) = \prod_{i=1}^{l}(x - \beta_i),$$

entonces

$$s(x) = \prod_{j=1}^{m} \prod_{i=1}^{l} \Big((x - \lambda\gamma_j) - \beta_i \Big) = \prod_{j=1}^{m} \prod_{i=1}^{l} \Big(x - (\lambda\gamma_j + \beta_i) \Big).$$

Por lo tanto,

$$\{\lambda\gamma_j + \beta_i \mid j \in \{1, \ldots, m\} \text{ y } i \in \{1, \ldots, l\}\}$$

es el conjunto de raíces de $s(x)$ y como

$$\beta_r + \lambda\gamma_s \neq \beta_i + \lambda\gamma_j \text{ para } (r, s) \neq (i, j).$$

(c.f. (1)), entonces $s(x)$ es separable.

Ahora, veamos que $p(x)|s(x)$. Como $p(x) = m_{\beta+\lambda\gamma,F}(x)$, basta probar que $s(x)$ es un polinomio con coeficientes en F que tiene a $\beta + \lambda\gamma$ como raíz. La verificación de que $\beta + \lambda\gamma$ es raiz de $s(x)$ es muy sencilla y se la dejamos al lector.

Veamos que $s(x)$ es un polinomio con coeficientes en F. Para esto, supongamos que $x_1, \ldots, x_m$ son variables indeterminadas y considera

$$S(x_1, \ldots, x_m, x) \coloneqq \prod_{j=1}^{m} f(x - \lambda x_j) \in F[x_1, \ldots, x_m, x]$$

Recordemos que en la proposición 1.23.1 vimos que

$$F[x_1, \ldots, x_m, x] \cong \left(F[x_1, \ldots, x_m]\right)[x]$$

y por lo tanto, podemos escribir

$$S(x_1, \ldots, x_m, x) = \sum_{k=0}^{N} p_k(x_1, \ldots, x_m) x^k$$

para algunos $p_k(x_1, \ldots, x_m) \in F[x_1, \ldots, x_m]$ y alguna $N \in \mathbb{Z}_{\geq 0}$.

Veamos que $p_k(x_1, \ldots, x_m) \in F_{\text{sep}}[x_1, \ldots, x_n]$ para toda k. Para esto, notemos que si $\tau \in S_m$, entonces

$$\sum_{k=0}^{N} p_k(x_{\tau(1)}, \ldots, x_{\tau(m)})x^k = S(x_{\tau(1)}, \ldots, x_{\tau(m)}, x) = \prod_{j=1}^{m} f(x - \lambda x_{\tau(j)}) =$$

$$\prod_{j=1}^{m} f(x - \lambda x_j) = S(x_1, \ldots, x_m, x) = \sum_{k=0}^{N} p_k(x_1, \ldots, x_m)x^k$$

Comparando los coeficientes de estos elementos de $\left(F[x_1, \ldots, x_m]\right)[x]$ obtenemos $p_k(x_{\tau(1)}, \ldots, x_{\tau(m)}) = p_k(x_1, \ldots, x_m)$ o equivalentemente, $p_k(x_1, \ldots, x_m) \in F_{\text{sep}}[x_1, \ldots, x_n]$ para toda k.

Entonces como $\gamma_1, \ldots, \gamma_m$ son raíces de un polinomio mónico, el corolario 2.16.5 implica que

$$p_k(\gamma_1, \ldots, \gamma_m) \in F \text{ para toda } k.$$

Por lo tanto,

$$s(x) = \prod_{j=1}^{m} f(x - \lambda\gamma_j) = S(\gamma_1, \ldots, \gamma_m, x) = \sum_{k=0}^{N} p_k(\gamma_1, \ldots, \gamma_m) x^k \in F[x]$$

Como mencionamos anteriormente, esto implica que $p(x)|s(x)$ y por lo tanto, $p(x)$ divide a un polinomio separable. En particular, $p(x) = m_{\beta+\lambda\gamma,F}(x)$ es un polinomio separable o equivalentemente, $\beta + \lambda\gamma$ es un elemento separable.

□

El caso infinito del teorema del elemento primitivo

Proposición 3

Supongamos que K/F es una extensión de campos y que K es infinito. Si $K = F(\alpha_1, \ldots, \alpha_n)$ con $\alpha_1, \ldots, \alpha_n \in K$ separables sobre F, entonces existen $t_1, \ldots, t_n \in F$ tales que

$$K = F(\alpha_1, \ldots, \alpha_n) = F\left(t_1\alpha_1 + \cdots + t_n\alpha_n\right)$$

y $t_1\alpha_1 + \cdots + t_n\alpha_n$ es separable sobre F.

En particular, si K/F es una extensión finitamente generada por elementos separables, entonces K/F es una extensión simple generada por un elemento separable.

Demostración. Procedemos por inducción sobre n.

Paso base. $n = 2$.
Usando la notación del lema anterior y definiendo $\alpha_1 = \beta$, $\alpha_2 = \gamma$, $t_1 = 1$, $t_2 = \lambda$ obtenemos lo deseado.

Paso inductivo.
Supongamos que $n > 2$ y que $K = F(\alpha_1, \ldots, \alpha_n)$ con $\alpha_1, \ldots, \alpha_n \in K$ separables sobre F. Por hipótesis de inducción, existen $t_1, \ldots, t_{n-1} \in F$ tales que

$$F(\alpha_1, \ldots, \alpha_{n-1}) = F(t_1\alpha_1 + \cdots + t_{n-1}\alpha_{n-1})$$

y $t_1\alpha_1 + \cdots + t_{n-1}\alpha_{n-1}$ es separable. Mas aun, por el lema anterior, existe $\lambda \in F$ tal que

$$F(t_1\alpha_1 + \cdots + t_{n-1}\alpha_{n-1}, \alpha_n) = F\left((t_1\alpha_1 + \cdots + t_{n-1}\alpha_{n-1}) + \lambda\alpha_n\right)$$

y $(t_1\alpha_1 + \cdots + t_{n-1}\alpha_{n-1}) + \lambda\alpha_n$ es separable. Poniendo $t_n = \lambda$ obtenemos lo deseado. □

Comentario

En lo que sigue, demostraremos el caso finito del teorema del elemento primitivo. Claramente, el argumento ocupado en la base del caso infinito no nos sirve (recuerda que ocupamos la hipótesis de que F es infinito para encontrar un λ distinto a todos los $\frac{\beta_i - \beta_r}{\gamma_s - \gamma_j}$). La demostración que daremos para el caso finito es muy diferente y para ella necesitaremos el siguiente lema que lamentablemente no nos daremos el tiempo de demostrar[3].

Lema 4

Supongamos que F es un campo y que $F^* = F \setminus \{0\}$ es su grupo multiplicativo. Si G es un subgrupo finito de F^*, entonces G es cíclico.

[3] La razón por la que omitimos la demostración es que ocupa un resultado no trivial de la teoría de grupos abelianos. Al lector interesado lo referimos a Cox, Galois Theory, Proposition A.5.3.

El caso finito del teorema del elemento primitivo

Proposición 5

Supongamos que K/F es una extensión finita y que F es finito. Entonces existe $\alpha \in K$ tal que $L = F(\alpha)$ y α es separable sobre F.

Demostración. Supongamos que K/F es una extensión finita y que $n = [K : F] < \infty$. Por definición, existen $\alpha_1, \ldots, \alpha_n \in K$ tales que $\{\alpha_1, \ldots, \alpha_n\}$ es una F-base de K. En particular, todo elemento en K se escribe de manera única como

$$t_1\alpha_1 + \cdots + t_n\alpha_n, \qquad \text{con } t_1, \ldots, t_n \in F.$$

Por lo tanto, K es biyectable con el producto cartesiano de F n-veces, y en particular, K es finito.

Usando esto y el lema anterior, obtenemos que K^* es cíclico. Supongamos que $\alpha \in K^*$ es generador. Usando esto es fácil verificar que $K = F(\alpha)$.

Resta probar que α es separable sobre F. Demostraremos que α es separable demostrando que su polinomio mínimo divide a un polinomio separable.

Para esto, denotemos $m = |L| - 1$ y recordemos que como α es generador de K^*, entonces $\alpha^m = 1$. En particular,

$$(\alpha^k)^m = (\alpha^m)^k = 1^k = 1 \text{ para toda } k \in \{0, \ldots, m-1\}$$

o equivalentemente, α^i es raíz de $x^m - 1$ para toda $k \in \{0, \ldots, m-1\}$.
Por lo tanto,

$$x^m - 1 = (x-1)(x-\alpha)(x-\alpha^2)\cdots(x-\alpha^{m-1})$$

y en particular, $x^m - 1$ es un polinomio separable.

Finalmente, como α es raíz de $x^m - 1$, entonces (por definición de polinomio mínimo) $m_{\alpha,F}(x) | x^m - 1$. □

Terminamos esta sección enunciando la forma final del teorema del elemento primitivo. Como has de esperar, este resultado es simplemente consecuencia de juntar las proposiciones 3 y 5.

El teorema del elemento primitivo

Teorema 6

Supongamos que K/F es una extensión de campos. Si $K = F(\alpha_1, \ldots, \alpha_n)$ con $\alpha_1, \ldots, \alpha_n \in K$ separables sobre F, entonces existe $\alpha \in K$ separable sobre F tal que $K = F(\alpha)$.

Mas aun, si F es infinito, entonces podemos escoger α de manera que

$$\alpha = t_1\alpha_1 + \cdots + t_n\alpha_n$$

para algunas $t_1, \ldots, t_n \in F$.