

Existencia de raíces en una extensión

Facultad de Ciencias UNAM

Introducción

El objetivo de esta sección es demostrar y estudiar el siguiente resultado:

Supongamos que F es un campo y que $p(x) \in F[x]$. Si $p(x)$ es irreducible en $F[x]$, entonces existe una extensión de campos K/F tal que $p(x)$ tiene una raíz en K .

Para tener un ejemplo específico en mente, considera $F = \mathbb{R}$ y $p(x) = x^2 + 1$. Obviamente, en este caso $K = \mathbb{C}$ cumple lo deseado.

Existencia de raíces en una extensión

Teorema 1

Supongamos que F es un campo y que $p(x) \in F[x]$. Si $p(x)$ es irreducible en $F[x]$, entonces existe un campo K tal que

1. K contiene una copia isomorfa de F , es decir, existe un homomorfismo inyectivo $\phi : F \rightarrow K$.
2. Si $\Phi : F[x] \rightarrow K[x]$ es tal que

$$\Phi(a_nx^n + \cdots + a_1x + a_0) = \phi(a_n)x^n + \cdots + \phi(a_1)x + \phi(a_0),$$

entonces $\Phi(p(x)) \in K[x]$ tiene una raíz en K .

Demostración. Supongamos que F es un campo y que $p(x) \in F[x]$ es irreducible en $F[x]$. Definimos

$$K := F[x]/(p(x))$$

Como $p(x)$ es irreducible, la proposición 1.24.5 implica que K es un campo. Por otro lado, denotemos por π a la proyección canónica de $F[x]$ en $F[x]/(p(x)) = K$.

1. Veamos que la restricción

$$\phi := \pi \upharpoonright_F: F \rightarrow K$$

es un homomorfismo inyectivo.

Debería de ser claro que ϕ es un homomorfismo de anillos y como $\varphi(1_F) = \pi(1_F) = 1_F + (p(x))$, entonces es un homomorfismo de campos. La inyectividad es consecuencia de que todo homomorfismo de campos es inyectivo (c.f. proposición 2.3.1).

2. Supongamos que

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

y que $\Phi : F[x] \rightarrow K[y]$ es el homomorfismo entre anillos de polinomios inducido por ϕ .

Cabe recalcar que la razón por la que introducimos la variable y es simplemente por claridad (pues $K = F[x]/(p(x))$). De esta manera, las x son elementos en F y las y son elementos en K .

Si todavía hay confusión, recuerda que Φ es (por definición) el homomorfismo que satisface

$$ax^k \in F[x] \mapsto \varphi(a)y^k \in K[y]$$

para toda $a \in F$ y toda $k \in \mathbb{Z}_{\geq 0}$.

Ahora si, calculando directamente, obtenemos

$$\begin{aligned}\Phi(p(x)) &= \Phi\left(a_nx^n + a_{n-1}x^{n-1} \cdots + a_1x + a_0\right) \\&= \phi(a_n)y^n + \phi(a_{n-1})y^{n-1} + \cdots + \phi(a_1)y + \phi(a_0) \\&= \pi(a_n)y^n + \pi(a_{n-1})y^{n-1} \cdots + \pi(a_1)y + \pi(a_0)\end{aligned}$$

Como este es un polinomio sobre $K = F[x]/(p(x))$, es decir, es un elemento de $K[y] = (F[x]/(p(x))) [y]$, entonces podemos evaluarlo en el elemento $\pi(x) \in F[x]/(p(x)) = K$. Calculando directamente, obtenemos

$$\begin{aligned}\Phi(p(x))(\pi(x)) &= \pi(a_n)(\pi(x))^n + \pi(a_{n-1})(\pi(x))^{n-1} + \cdots + \pi(a_1)\pi(x) + \pi(a_0) \\&= \pi\left(a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0\right) \text{ (pues } \pi \text{ es homomorfismo)} \\&= \pi(p(x)) = 0_K\end{aligned}$$

Por lo tanto, $\pi(x)$ es una raíz de $\Phi(p(y))$ en K .

Comentario

Si identificamos a F con su imagen bajo ϕ , es decir, si hacemos la convención $a = \phi(a)$ para toda $a \in F$, entonces

$$\begin{aligned}\Phi(a_nx^n + \cdots + a_1x + a_0) &= \phi(a_n)x^n + \cdots + \phi(a_1)x + \phi(a_0) \\ &= a_nx^n + \cdots + a_1x + a_0.\end{aligned}$$

y la proposición anterior se puede escribir de la siguiente manera:

Supongamos que F es un campo y que $p(x) \in F[x]$. Si $p(x)$ es irreducible en $F[x]$, entonces existe una extensión de campos K/F tal que $p(x)$ tiene una raíz en K .

En otras palabras, dado un polinomio irreducible sobre un campo, existe una extensión en donde el polinomio tiene una raíz.

En lo que sigue, (por conveniencia) siempre adoptamos esta convención.

Comentario

Por la demostración de la proposición anterior, es natural interesarse en entender mejor el campo $F[x]/(p(x))$. Tal vez recuerdes que ya lo habíamos estudiado un poquito en la sección 1.24. Ahí encontramos una forma de describir explícitamente al conjunto $F[x]/(p(x))$. En la demostración de la siguiente proposición volvemos a presentar este resultado con el objetivo de dar otra forma de describir explícitamente a $F[x]/(p(x))$.

Antes de continuar, notemos que [podemos ver a \$F\[x\]/\(p\(x\)\)\$ como espacio vectorial sobre \$F\$](#) . En efecto, la suma es la usual y la multiplicación por escalares la definimos por

$$\alpha \cdot (a(x) + (p(x))) = \alpha a(x) + (p(x))$$

para toda $\alpha \in F$ y toda $a(x) \in F[x]$.

Finalmente, recordemos la famosa notación de barra: para toda $a(x) \in F[x]$ denotamos $\overline{a(x)} = a(x) + (p(x))$. De esta manera, la multiplicación por escalares se convierte en $\alpha \cdot \overline{a(x)} = \overline{\alpha a(x)}$.

El cociente $F[x]/(p(x))$

Proposición 2

Supongamos que F es un campo y que $p(x) \in F[x]$ es irreducible en $F[x]$ con $n = \deg p(x) \geq 1$. Denotemos

$$K = F[x]/(p(x)) \quad \text{y} \quad \theta = \bar{x} = x + (p(x)) \in K.$$

Entonces el conjunto

$$\left\{ 1, \theta, \theta^2, \dots, \theta^{n-1} \right\}$$

es una base de K considerado como espacio vectorial sobre V . En particular,

$$F[x]/(p(x)) = \left\{ a_0 + a_1\theta + a_2\theta^2 + \cdots + a_{n-1}\theta^{n-1} \mid a_0, a_1, a_2, \dots, a_{n-1} \in F \right\}.$$

En palabras, $F[x]/(p(x))$ es el conjunto de polinomios de grado $< \deg p(x)$ sobre la variable θ donde θ es una raíz de $p(x)$ en K .

Demostración.

- $\{1, \theta, \theta^2, \dots, \theta^{n-1}\}$ genera a K :

Primero notemos que

$$\begin{aligned}\text{span} \left(1, \theta, \theta^2, \dots, \theta^{n-1} \right) &= \left\{ a_0 + a_1 \theta + a_2 \theta^2 + \dots + a_{n-1} \theta^{n-1} \mid a_0, a_1, a_2, \dots, a_{n-1} \in F \right\} \\ &= \left\{ \overline{b(x)} \mid \deg b(x) < \deg p(x) \right\}\end{aligned}$$

y por lo tanto, basta demostrar que

$$F[x]/(p(x)) = \left\{ \overline{b(x)} \mid \deg b(x) < \deg p(x) \right\}.$$

Equivalentemente, basta demostrar que para toda $a(x) \in F[x]$, existe un único $b(x) \in F[x]$ tal que $\overline{a(x)} = \overline{b(x)}$ y $\deg b(x) < \deg p(x)$.

Para esto, supongamos que $a(x) \in {}^1F[x] \setminus \{0\}$. Como $\deg p(x) \geq 1$, en particular $p(x) \neq 0$ y por lo tanto, por el algoritmo de la división en $F[x]$, existen $q(x), r(x) \in F[x]$ únicos tales que

$$a(x) = q(x)p(x) + r(x) \text{ con } r(x) = 0 \text{ o } \deg r(x) < \deg p(x) \quad (1)$$

En caso de que $r(x) = 0$, entonces $p(x)|a(x)$ y por lo tanto, $\overline{a(x)} = \overline{p(x)} = \overline{0}$. Como $\deg 0 = -1 < 1 \leq \deg p(x)$, la igualdad anterior implica lo deseado. En caso de que $\deg r(x) < \deg p(x)$, entonces restamos $r(x)$ en ambos lados de (1) para obtener

$$a(x) - r(x) = q(x)p(x).$$

En particular, $p(x)|a(x) - r(x)$ o equivalentemente $\overline{a(x)} = \overline{r(x)}$. Por lo tanto, $b(x) := r(x)$ cumple lo deseado.

¹El caso $a(x) = 0$ es trivial porque si $b(x) = 0$, entonces $\deg b(x) = \deg 0 = -1 < 1 \leq \deg p(x)$. \diamond

- $1, \theta, \theta^2, \dots, \theta^{n-1}$ son linealmente independientes:

Supongamos lo contrario. Es decir, supongamos que existen $b_0, b_1, \dots, b_{n-1} \in F$ no todas 0 tales que

$$b_0 + b_1\theta + b_2\theta^2 + \dots + b_{n-1}\theta^{n-1} = 0_K.$$

Por definición de K y θ , esto es equivalente a que

$$(b_0 + b_1x + b_2x^2 + \dots + \dots + b_{n-1}x^{n-1}) + (p(x)) = (p(x))$$

Mas aun, esto es equivalente a que

$$p(x) \text{ divide a } b_0 + b_1x + b_2x^2 + \dots + \dots + b_{n-1}x^{n-1} \text{ en } F[x].$$

Sin embargo, como $\deg p(x) = n$, esto es imposible. Una contradicción.

□

$$[F(x)/(p(x)) : F] = \deg p(x)$$

Corolario 3

Supongamos que F es un campo. Si $p(x) \in F[x]$ es irreducible en $F[x]$, entonces

$$[F(x)/(p(x)) : F] = \deg p(x).$$

Demostración. Es consecuencia inmediata de que $\{1, \theta, \theta^2, \dots, \theta^{n-1}\}$ es base de $F[x]/(p(x))$ considerado como espacio vectorial sobre F . □

Comentario

Los resultados anteriores tal vez dejaron la errónea idea de que lo único que importa en el campo $F[x]/(p(x))$ es el grado de $p(x)$. Al fin y al cabo, si $p(x), q(x) \in F[x]$ son irreducibles con $\deg p(x) = n = \deg q(x)$ y denotamos $\theta = x + (p(x))$, $\xi = x + (q(x))$, entonces la función

$$\begin{aligned} a_0 + a_1\theta + a_2\theta^2 + \cdots + a_{n-1}\theta^{n-1} &\in F[x]/(p(x)) \mapsto \\ a_0 + a_1\xi + a_2\xi^2 + \cdots + a_{n-1}\xi^{n-1} &\in F[x]/(q(x)) \end{aligned}$$

es una biyección. *Pero* no (necesariamente) es un isomorfismo. En otras palabras, los elementos de $F[x]/(p(x))$ no (necesariamente) se operan de la misma manera que los elementos de $F[x]/(q(x))$.

En lo que sigue, estudiamos las operaciones de $F[x]/(p(x))$. Para esto, es útil antes entender al elemento $\theta^k \in F[x]/(p(x))$ con $k \geq n$.

θ^k con $k \geq n$

Supongamos que $p(x) = p_n x^n + p_{n-1} x^{n-1} + \cdots + p_1 x + p_0$. Como $p(\theta) = 0$, entonces

$$p_n \theta^n + p_{n-1} \theta^{n-1} + \cdots + p_1 \theta + p_0 = 0.$$

Despejando θ^n obtenemos

$$\theta^n = \frac{1}{p_n} \left(-p_{n-1} \theta^{n-1} - p_{n-2} \theta^{n-2} - \cdots - p_1 \theta - p_0 \right). \quad (2)$$

Es decir, acabamos de encontrar la expresión explícita de θ^n en la base $\{1, \theta, \theta^2, \dots, \theta^{n-1}\}$.

Mas aun, si multiplicamos por θ en ambos lados de (2) y luego sustituimos (2) en esta nueva ecuación, obtenemos la expresión explícita de θ^{n+1} en la base $\{1, \theta, \theta^2, \dots, \theta^{n-1}\}$.

En efecto,

$$\begin{aligned}\theta^{n+1} &= \theta\theta^n \\&= \theta \frac{1}{p_n} (-p_{n-1}\theta^{n-1} - p_{n-2}\theta^{n-2} - \dots - p_1\theta - p_0) \\&= \frac{1}{p_n} (-p_{n-1}\theta^n - p_{n-2}\theta^{n-1} - \dots - p_1\theta^2 - p_0\theta) \\&= \frac{1}{p_n} \left(-p_{n-1} \underbrace{\left(\frac{1}{p_n} (-p_{n-1}\theta^{n-1} - p_{n-2}\theta^{n-2} - \dots - p_1\theta - p_0) \right)}_{\theta^n} - p_{n-2}\theta^{n-1} - \dots - p_1\theta^2 - p_0\theta \right) \\&= \frac{1}{p_n} \left(\left(\frac{p_{n-1}^2}{p_n} \theta^{n-1} + \frac{p_{n-1}p_{n-2}}{p_n} \theta^{n-2} + \dots + \frac{p_{n-1}p_1}{p_n} \theta + \frac{p_{n-1}p_0}{p_n} \right) - p_{n-2}\theta^{n-1} - \dots - p_1\theta^2 - p_0\theta \right) \\&= \frac{1}{p_n} \left(\left(\frac{p_{n-1}^2}{p_n} - p_{n-2} \right) \theta^{n-1} + \left(\frac{p_{n-1}p_{n-2}}{p_n} - p_{n-3} \right) \theta^{n-2} + \dots + \left(\frac{p_{n-1}p_1}{p_n} - p_0 \right) \theta + \frac{p_{n-1}p_0}{p_n} \right)\end{aligned}$$

De manera análoga, podemos encontrar expresiones para θ^k con $k \geq n$ en términos de la base $\{1, \theta, \theta^2, \dots, \theta^{n-1}\}$.

A través de estas expresiones se vuelve claro que el grado de $p(x)$ no es lo único que importa en el campo $F[x]/(p(x))$.

θ^k con $k \leq -1$

Supongamos que $p(x) = p_n x^n + p_{n-1} x^{n-1} + \cdots + p_1 x + p_0$. De nuevo, como $p(\theta) = 0$, entonces

$$p_n \theta^n + p_{n-1} \theta^{n-1} + \cdots + p_1 \theta + p_0 = 0.$$

Restando p_0 obtenemos

$$-p_0 = p_n \theta^n + p_{n-1} \theta^{n-1} + \cdots + p_1 \theta = \theta \left(p_n \theta^{n-1} + p_{n-1} \theta^{n-2} + \cdots + p_1 \right).$$

De donde

$$\theta^{-1} = -\frac{1}{p_0} \left(p_n \theta^{n-1} + p_{n-1} \theta^{n-2} + \cdots + p_1 \right).$$

Usando (i) esta igualdad, (ii) que $\theta^{-m} = (\theta^{-1})^m$ para toda $m \in \mathbb{Z}_{\geq 1}$, y (iii) que tenemos expresiones para θ^l con $l \geq n$ en términos de la base $\{1, \theta, \theta^2, \dots, \theta^{n-1}\}$, entonces podemos encontrar expresiones para θ^k con $k \leq -1$ en términos de la base $\{1, \theta, \theta^2, \dots, \theta^{n-1}\}$.

Las operaciones en $F[x]/(p(x))$

La proposición 2 nos da una buena descripción del *conjunto* del anillo $F[x]/(p(x))$, pero no nos dice nada acerca de sus *operaciones*.

La suma se hace como si estuviéramos en $F[\theta]$:

$$\begin{aligned} & \left(a_0 + a_1\theta + a_2\theta^2 + \cdots + a_{n-1}\theta^{n-1} \right) + \left(b_0 + b_1\theta + b_2\theta^2 + \cdots + b_{n-1}\theta^{n-1} \right) = \\ & \left(\left(a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} \right) + (p(x)) \right) + \\ & \quad \left(\left(b_0 + b_1x + b_2x^2 + \cdots + b_{n-1}x^{n-1} \right) + (p(x)) \right) = \\ & \qquad \qquad \qquad (\text{por def. de } +_{F[x]/(p(x))}) \\ & \left((a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots + (a_{n-1} + b_{n-1})x^{n-1} \right) + (p(x)) = \\ & (a_0 + b_0) + (a_1 + b_1)\theta + (a_2 + b_2)\theta^2 + \cdots + (a_{n-1} + b_{n-1})\theta^{n-1}. \end{aligned}$$

En contraste, una descripción de la multiplicación (en términos de la base $\{1, \theta, \theta^2, \dots, \theta^{n-1}\}$) es un poquito mas complicada. La razón para esta diferencia es que la suma de dos polinomios de grado $< n$ es un polinomio de grado $< n$, *pero* el producto de dos polinomios de grado $< n$ no es necesariamente un polinomio de grado $< n$.

Afortunadamente, las expresiones para θ^k con $k \geq n$ en términos de la base $\{1, \theta, \theta^2, \dots, \theta^{n-1}\}$ resuelven este problema. En efecto, [para calcular un producto en \$F\[x\]/\(p\(x\)\)\$](#) , multiplicamos como si estuviéramos en $F[\theta]$ y luego sustituimos todos los θ^k con $k \geq n$ por sus respectivas expresiones en términos de la base $\{1, \theta, \theta^2, \dots, \theta^{n-1}\}$.

Casos específicos de $F[x]/(p(x))$

- Supongamos que $F = \mathbb{R}$ y que $p(x) = x^2 + 1$ (irreducible en $\mathbb{R}[x]$ pues tiene grado 2 y no tiene raíces en \mathbb{R})². Si denotamos $K = \mathbb{R}[x]/(x^2 + 1)$ y $\theta = \bar{x} = x + (x^2 + 1) \in K$, entonces

$$K = \{a + b\theta \mid a, b \in \mathbb{R}\} \quad \text{y} \quad \theta^2 + 1 = p(\theta) = 0.$$

Mas aun, las operaciones en K están dadas por

$$(a + b\theta) + (c + d\theta) = (a + c) + (b + d)\theta \quad \text{y}$$

$$(a + b\theta) \cdot (c + d\theta) = ac + ad\theta + bc\theta + bd\underbrace{\theta^2}_{-1} = (ac - bd) + (ad + bc)\theta$$

Usando esto, es fácil verificar que la función de K en \mathbb{C} dada por

$$a + b\theta \mapsto a + bi$$

es un isomorfismo. En particular, $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$ y por lo tanto, por la proposición 2.3.2 y el corolario 3

$$[\mathbb{C} : \mathbb{R}] = [\mathbb{R}[x]/(x^2 + 1) : \mathbb{R}] = \deg(x^2 + 1) = 2.$$

²c.f. corolario 1.27.3

- Supongamos que $F = \mathbb{Q}$ y que $p(x) = x^2 + 1$ (irreducible en $\mathbb{Q}[x]$ por la misma razón que antes). Por un argumento completamente análogo al del ejemplo anterior, obtenemos que $\mathbb{Q}[x]/(x^2 + 1) \cong \mathbb{Q}(i)$.
- Supongamos que $F = \mathbb{Q}$ y que $p(x) = x^2 - 2$ (irreducible en $\mathbb{Q}[x]$ por la misma razón que antes). Si denotamos $K = \mathbb{Q}[x]/(x^2 - 2)$ y $\theta = \bar{x} = x + (x^2 - 2)$, entonces

$$K = \{a + b\theta \mid a, b \in \mathbb{Q}\} \quad \text{y} \quad \theta^2 - 2 = p(\theta) = 0.$$

Mas aun, las operaciones en K están dadas por

$$(a + b\theta) + (c + d\theta) = (a + c) + (b + d)\theta \quad \text{y}$$

$$(a + b\theta) \cdot (c + d\theta) = ac + ad\theta + bc\theta + bd \underbrace{\theta^2}_2 = (ac + 2bd) + (ad + bc)\theta$$

Usando esto, es fácil verificar que la función de K en $\mathbb{Q}(\sqrt{2})$ dada por

$$a + b\theta \mapsto a + b\sqrt{2}$$

es un isomorfismo. En particular, $\mathbb{Q}[x]/(x^2 - 2) \cong \mathbb{Q}(\sqrt{2})$.

Observación

Como

- \mathbb{C} es el subcampo de \mathbb{C} mas chico que contiene a \mathbb{R} y a i .
- $\mathbb{Q}(i)$ es el subcampo de \mathbb{R} mas chico que contiene a \mathbb{Q} y a i .
- $\mathbb{Q}(\sqrt{2})$ es el subcampo de \mathbb{R} mas chico que contiene a \mathbb{Q} y a $\sqrt{2}$.

Entonces los ejemplos anteriores sugieren un patrón general: si K/F es una extensión de campos, $p(x) \in F[x]$, y α es una raíz de $p(x)$ en K , entonces $F[x]/(p(x))$ es isomorfo al subcampo de K mas chico que contiene a F y a α .

En la siguiente sección precisamos esta idea.