Extensiones simples

Facultad de Ciencias UNAM

Introducción

En la sección anterior hicimos la siguiente conjetura:

> *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 esta sección precisamos esta idea empezando por la siguiente definición.

El campo generado por A sobre F

Definición

Supongamos que K/F es una extensión de campos y A un subconjunto de F.
El campo generado por A sobre F es el siguiente subcampo de K

$$F(A) \coloneqq \bigcap \{S \mid S \text{ es subcampo de } K \text{ y } F \cup A \subset S\}.$$

Si A es numerable, por ejemplo $A = \{a_1, a_2, \dots\}$, escribimos

$$F(a_1, a_2, \dots) = F\left(\{a_1, a_2, \dots\}\right).$$

Si es finito, por ejemplo $A = \{a_1, \dots, a_n\}$, escribimos

$$F(a_1, \dots, a_n) = F\left(\{a_1, \dots, a_n\}\right).$$

Observación

Cabe recalcar que $F(A)$ esta bien definido porque (i) la familia $\{S \mid S \text{ es subcampo de } K \text{ y } F \cup A \subset S\}$ es no vacía[1] y (ii) la intersección de subcampos es un subcampo.

Es importante recordar que $F(A)$ solo tiene sentido cuando F y A estan contenidos en un campo K. Esto es obvio, pero lo mencionamos porque pueden haber confusiones.

Por ejemplo, si F y E son dos campos, no tiene sentido hablar de "el campo generado por F y E" *a menos* de que haya un campo K que contiene a F y E como subcampos.

[1] Por ejemplo, K pertenece a ella.

Extensiones simples

Definición

Supongamos que K/F es una extensión de campos. Si existe $\alpha \in K$ tal que $F(\alpha) = K$, decimos que K **es una extensión simple de** F y que α es un **elemento primitivo** de la extensión.

Por ejemplo,

- $\mathbb{C}$ es una extensión simple de $\mathbb{R}$: Es fácil verificar que $\mathbb{R}(i) = \mathbb{C}$.
- $\mathbb{R}$ no es una extensión simple de $\mathbb{Q}$: Es fácil verificar que para toda $\alpha \in^2 \mathbb{R} \setminus \mathbb{Q}$,

$$\mathbb{Q}(\alpha) = \{p + q\alpha \in \mathbb{R} \mid p, q \in \mathbb{Q}\}$$

Veamos que la función

$$(p, q) \in \mathbb{Q} \times \mathbb{Q} \mapsto p + q\alpha \in \mathbb{Q}(\alpha)$$

es una biyección.

[2] El caso en que $\alpha \in \mathbb{C}$, $\mathbb{Q}(\alpha) = \mathbb{Q}$ y por lo tanto no hace falta considerarlo.

La suprayectividad es obvia, veamos la inyectividad. Supongamos que $p + q\alpha = r + s\alpha$ con $p, q, r, s \in \mathbb{Q}$. Entonces $p - r = (s - q)\alpha$.

$$\underbrace{(s-q)}_{\in\mathbb{Q}}\underbrace{\alpha}_{\in\mathbb{R}\setminus\mathbb{Q}} = p - r \in \mathbb{Q}$$

Como el producto de un racional (no nulo) con un irracional (no nulo) no puede ser racional, entonces la igualdad anterior implica que $(s - q)\alpha = 0$. Usando esto es fácil concluir que $p = r$ y $q = s$.

$F[x]/(p(x)) \cong F(\alpha)$ si α es una raíz de $p(x)$

Teorema 1

Supongamos que K/F es una extensión de campos y que $p(x) \in F[x]$ es irreducible en $F[x]$ con $\deg p(x) = n$. Si $\alpha \in K$ es una raíz de $p(x)$ en K, entonces

$$F[x]/(p(x)) \cong F(\alpha).$$

Demostración. Sea φ el homomorfismo que a cada polinomio sobre F le asigna su valor en α. Específicamente, sea

$$\begin{aligned} \varphi : F[x] &\to K \\ a(x) &\mapsto a(\alpha) \end{aligned}$$

Como $p(\alpha) = 0$, entonces $p(x) \in \ker \varphi$ y en particular $(p(x)) \subset \ker \varphi$.

Por el (primer inciso del) primer teorema de isomorfismos, esto implica que la función

$$\begin{aligned} \overline{\varphi} : F[x]/(p(x)) &\to K \\ \overline{a(x)} &\mapsto a(\alpha) \end{aligned}$$

esta bien definida y es un homomorfismo. Como $\overline{\varphi}$ es un homomorfismo no nulo entre campos que respeta unidades[3], entonces $\overline{\varphi}$ es inyectiva.

Ahora bien, como el dominio de un homomorfismo inyectivo es isomorfo a la imagen de este homomorfismo, basta probar que

$$\operatorname{im} \overline{\varphi} = F(\alpha).$$

[3] El valor del polinomio 1 evaluado en α es 1.

Para esto, primero notemos que

$$\begin{aligned}
\operatorname{im}\overline{\varphi} &= \left\{\overline{\varphi}(\overline{a(x)}) \mid \overline{a(x)} \in F[x]/(p(x))\right\} \\
&= \left\{\overline{\varphi}(\overline{a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1}}) \mid a_0, a_1, a_2, \ldots, a_{n-1} \in F\right\} \\
&= \left\{a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} \mid a_0, a_1, a_2, \ldots, a_{n-1} \in F\right\} \qquad (1)
\end{aligned}$$

donde la segunda igualdad se cumple porque por la proposición 2.4.2,

$$F[x]/(p(x)) = \left\{\overline{a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1}} \mid a_0, a_1, a_2, \ldots, a_{n-1} \in F\right\}.$$

Ahora si, veamos que $\operatorname{im}\overline{\varphi} = F(\alpha)$.

$\supset$) Como evaluar α en un polinomio constante $a \in F \subset F[x]$ nos regresa a, entonces $\overline{\varphi}(a) = a$ para toda $a \in F$. De donde, $F \subset \operatorname{im}\overline{\varphi}$.
Por otro lado, como evaluar el polinomio x en α nos regresa α, entonces $\overline{\varphi}(\overline{x}) = \alpha$ y por lo tanto $\alpha \in \operatorname{im}\overline{\varphi}$.
En resumen, $F \cup \{\alpha\} \subset \operatorname{im}\overline{\varphi}$ y por lo tanto $F(\alpha) \subset \operatorname{im}\overline{\varphi}$.

$\subset$) Por definición de $F(\alpha)$, basta probar que $\operatorname{im}\overline{\varphi}$ esta contenido en todos los subcampos de K que contienen a F y a α. Sin embargo, esto es consecuencia inmediata de la igualdad

$$\operatorname{im}\overline{\varphi} = \left\{ a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} \mid a_0, a_1, a_2, \ldots, a_{n-1} \in F \right\}.$$

$\square$

$\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ es una F-base de $F(\alpha)$

Corolario 2

Supongamos que K/F es una extensión de campos y que $p(x) \in F[x]$ es irreducible en $F[x]$ con $\deg p(x) = n$. Si $\alpha \in K$ es una raíz de $p(x)$ en K, entonces

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

y el conjunto $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ es una F-base de $F(\alpha)$.

Demostración. El isomorfismo $F[x]/(p(x)) \cong F(\alpha)$ y la proposición 2.3.2 implican la primera de las siguientes igualdades.

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

La segunda igualdad es consecuencia del corolario 2.4.3.

Ahora, veamos que $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ es una F-base de $F(\alpha)$. Como

$$\left|\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}\right| = n$$

y todo subconjunto generador con la misma cardinalidad que la dimensión del espacio es una base (c.f. proposición 2.2.7), entonces basta probar que $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ es un F-conjunto generador de $F(\alpha)$. Sin embargo, esto es consecuencia de las siguientes igualdades (vistas en la demostración del teorema anterior).

$$\begin{aligned} F(\alpha) &= \operatorname{im} \overline{\varphi} \\ &= \left\{ a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} \mid a_0, a_1, a_2, \ldots, a_{n-1} \in F \right\} \\ &= \operatorname{span}_F \left(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\right) \end{aligned}$$

□

Observación

La igualdad

$$F(\alpha) = \left\{ a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} \mid a_0, a_1, a_2, \ldots, a_{n-1} \in F \right\}$$

nos dice algo muy interesante acerca de los elementos que son raíces de algún polinomio: para encontrar el *campo* mas chico que contiene a F y α, basta agregarle α a F y "cerrar" el conjunto resultante respecto a suma y multiplicación. La parte interesante es que *no hace falta cerrar bajo división.*

También notemos que demostrar

$$F(\alpha) = \left\{ a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} \mid a_0, a_1, a_2, \ldots, a_{n-1} \in F \right\}$$

directamente no es tan sencillo como considerar

$$p(x) = p_n x^n + \cdots + p_1 x + p_0 \in F[x] \text{ con } p(\alpha) = 0$$

y encontrar[4] α^k con $k \leq -1$ en términos de $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ a partir de la igualdad

$$p_n\alpha^n + \cdots + p_1\alpha + p_0 = 0.$$

La razón es que dada una combinación lineal arbitraria

$$b_0 + b_1\alpha + b_2\alpha^2 + \cdots b_k\alpha^k$$

no es claro quien es su inverso en términos de $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$.

[4] De la misma manera en la que encontramos θ^k con $k \leq -1$ en términos de $1, \theta, \theta^2, \ldots, \theta^{n-1}$.

Observación

Una consecuencia inmediata del teorema anterior es la siguiente:

Supongamos que K/F es una extensión de campos y que $p(x) \in F[x]$ es irreducible en $F[x]$. Si α y β son raíces de $p(x)$ en K, entonces

$$F(\alpha) \cong F(\beta).$$

Una forma de interpretar esto es que las raíces de un polinomio irreducible son *algebraicamente* indistinguibles, pues los campos que generan sobre F son isomorfos. En otras palabras, desde el punto de vista de un elemento de F, cualesquiera dos raíces de un polinomio irreducible en F se comportan (algebraicamente) de la misma manera.

En lo que sigue, damos una generalización de esta observacion usando isomorfismos entre campos. Pero antes, recordamos un poquito de notación y definimos un isomorfismo que nos auxiliara en la generalización.

El isomorfismo auxiliar

Lema 3

Supongamos que $\phi : F \to F'$ es un isomorfismo entre campos y que $\Phi : F[x] \to F'[x]$ es tal que

$$\Phi\left(a_n x^n + \cdots + a_1 x + a_0\right) = \phi(a_n)x^n + \cdots + \phi(a_1)x + \phi(a_0).$$

Si $p(x) \in F[x]$ es irreducible en $F[x]$, entonces $\Phi(p(x))$ también es irreducible en $F'[x]$ y la función

$$\begin{aligned} F[x]/(p(x)) &\to F'[x]/\left(\Phi(p(x))\right) \\ a(x) + (p(x)) &\mapsto \Phi(a(x)) + \left(\Phi(p(x))\right) \end{aligned}$$

es un isomorfismo de campos[5].

[5] Recuerda que $F[x]/(p(x))$ y $F'[x]/(\Phi(p(x))$ son campos porque $p(x)$ y $\Phi(p(x))$ son irreducibles.

Demostración. Supongamos que $p(x) \in F[x]$ es irreducible en $F[x]$. Como los isomorfismos preservan irreducibilidad (c.f. proposición 1.16.5), entonces $\Phi(p(x))$ es irreducible en $F'[x]$.

Para ver que la función

$$\begin{aligned} F[x]/(p(x)) &\to F'[x]/\left(\Phi(p(x))\right) \\ a(x) + (p(x)) &\mapsto \Phi(a(x)) + \left(\Phi(p(x))\right) \end{aligned}$$

es un isomorfismo de campos, sácale cociente al isomorfismo $\Phi : F[x] \to F'[x]$ (c.f. proposición 1.7.5) para obtener el isomorfismo de anillos

$$\begin{aligned} F[x]/(p(x)) &\to F'[x]/\Phi\left((p(x))\right) \\ a(x) + (p(x)) &\mapsto \Phi(a(x)) + \Phi\left((p(x))\right). \end{aligned}$$

Claramente, este isomorfismo preserva la unidad y por lo tanto, también es un isomorfismos de campos. Finalmente, es fácil verificar que

$$\Phi\left((p(x))\right) = \left(\Phi(p(x))\right)$$

Juntando esto con el isomorfismo anterior, obtenemos lo deseado. $\square$

$$F(\alpha) \cong F'(\alpha') \text{ si } F \overset{\phi}{\cong} F',\ p(\alpha) = 0, \text{ y } \Phi\left(p(x)\right)(\alpha') = 0$$

Teorema 4

Supongamos que F, F' son campos, que $\phi : F \to F'$ es un isomorfismo, que $p(x) \in F[x]$ es irreducible en $F[x]$, y que $p'(x) = \Phi(p(x))$ donde Φ es como en el lema anterior.

Sean K/F y K'/F' extensiones de campo en donde $p(x)$ y $p'(x)$ tienen raíces (respectivamente)[6].

Si α es una raíz de $p(x)$ en K y α' es una raíz de $p'(x)$ en K', entonces existe un isomorfismo

$$\sigma : F(\alpha) \to F'(\alpha')$$

tal que $\sigma(\alpha) = \alpha'$ y $\sigma \restriction_F = \phi$.

[6] Recuerda que en el lema anterior vimos que $\Phi(p(x))$ también es irreducible y por eso sabemos que existe K'/F'.

Demostración. Considera los siguientes isomorfismos[7].

$$F(\alpha) \to F[x]/(p(x))$$
$$f(\alpha) \mapsto f(x) + (p(x))$$

$$F[x]/(p(x)) \to F'[x]/\left(p'(x)\right)$$
$$f(x) + (p(x)) \mapsto \Phi(f(x)) + \left(p'(x)\right)$$

$$F'[x]/\left(p'(x)\right) \to F'(\alpha')$$
$$b(x) + \left(p'(x)\right) \mapsto b(\alpha')$$

La composición de estos es un isomorfismo de $F(\alpha)$ a $F'(\alpha')$ que satisface

$$\alpha \mapsto x + (p(x)) \mapsto \Phi(x) + \left(p'(x)\right) = x + \left(p'(x)\right) \mapsto \alpha' \quad \text{y}$$
$$a \mapsto a + (p(x)) \mapsto \Phi(a) + \left(\Phi(p(x))\right) = \phi(a) + \left(\Phi(p(x))\right) \mapsto \phi(a).$$

para toda $a \in F$. Por lo tanto, $\sigma =$ la composición de estos isomorfismos cumple lo deseado. □

[7] El primero y el tercero son los isomorfismos que definimos en el teorema 1 para demostrar que $F[x]/(p(x)) \cong F(\alpha)$. El segundo es el isomorfismo auxiliar.

Comentario

Otra forma de ver el resultado anterior es que tenemos el siguiente diagrama conmutativo donde las flechas horizontales son isomorfismos y las flechas verticales son inclusiones.

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

¿Que podemos decir de los polinomios que no son irreducibles?

Corolario 5

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

Demostración. El caso en que $p(x)$ es irreducible esta dado por el teorema de existencia de raíces.

Por eso, supongamos que $p(x)$ no es irreducible. En particular, $p(x)$ no es invertible (c.f. proposición 1.16.2).

Por otro lado, recordemos que como F es un campo, $F[x]$ es un DFU (c.f. proposición 1.24.2). Como $p(x)$ no es invertible, podemos escribir

$$p(x) = p_1(x)p_2(x)\cdots p_n(x)$$

con $p_1(x), p_2(x), \ldots, p_n(x)$ irreducibles en $F[x]$. Aplicando el teorema de existencia de raíces a cualquiera de los $p_i(x)$ y usando que toda raíz de $p_i(x)$ también es raíz de $p(x)$, obtenemos lo deseado. $\square$