Extensiones algebraicas

Facultad de Ciencias UNAM

Introducción

En la sección anterior demostramos el siguiente resultado.

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

Por eso, en esta sección estudiamos con mas detalle a los elementos de una extensión K/F que son raíces de algún polinomio no cero (y no necesariamente irreducible) con coeficientes en F.

Elementos algebraicos, elementos trascendentales, y extensiones algebraicas

Definición

- Decimos que un elemento $\alpha \in K$ es **algebraico sobre** F si es raíz de algún polinomio no cero sobre F. En otras palabras, $\alpha \in K$ es algebraico si existe $p(x) \in F[x]$ tal que $p(\alpha) = 0$.
- Decimos que un elemento $\alpha \in K$ es **trascendental sobre** F si *no* es algebraico sobre F.
- Decimos que la extensión K/F es **algebraica** si todo elemento de K es algebraico sobre F.

Cabe recalcar que si un elemento de F, digamos $\alpha \in F$ es algebraico sobre F, entonces también es algebraico sobre cualquier extensión L de F.

El polinomio mínimo de α sobre F

Proposición 1

Supongamos que $\alpha \in K$ es algebraico sobre F. Entonces existe un único polinomio mónico e irreducible $m_{\alpha,F}(x) \in F[x]$ que tiene a α como raíz. Mas aun, $m_{\alpha,F}(x)$ satisface

$$\alpha \text{ es raíz de } p(x) \in F[x] \iff m_{\alpha,F}(x) \text{ divide a } p(x) \text{ en } F[x]$$

para toda $p(x) \in F[x]$.

Al polinomio $m_{\alpha,F}(x)$ le llamamos **el polinomio mínimo de α sobre F** y definimos el **grado de** α, denotado $\deg_F \alpha$, como el grado de $m_{\alpha,F}(x)$. Es decir, $\deg_F \alpha := \deg m_{\alpha,F}(x)$.

Por brevedad, cuando no haya ambigüedad respecto al campo F, omitimos la F en las expresiones $m_{\alpha,F}(x)$ y $\deg_F \alpha$.

Demostración.

Existencia.

Supongamos que $\alpha \in K$ es algebraico sobre F. Por definición, existe un polinomio sobre F que tiene a α como raíz y por lo tanto, el conjunto

$$\{\deg a(x) \mid a(x) \in F[x] \text{ y } a(\alpha) = 0\} \subset \mathbb{Z}_{\geq 1}$$

es no vació. Por el axioma del buen orden, existe un polinomio $q(x) \in F[x]$ tal que $q(\alpha) = 0$ y $\deg q(x) \leq \deg a(x)$ para toda $a(x) \in F[x]$ con $a(\alpha) = 0$. Definimos

$$m_{\alpha,F}(x) := \frac{1}{q_n} q(x)$$

donde q_n es el coeficiente delantero de $q(x)$.

De esta manera, $m_{\alpha,F}(x)$ es mónico y tiene a α como raíz. Veamos que también es irreducible. Para esto, supongamos lo contrario. Es decir, supongamos que existen $f(x), g(x) \in F[x]$ no invertibles tales que $m_{\alpha,F}(x) = f(x)g(x)$.

Como $f(x), g(x) \in F[x]$ no son invertibles y F es campo, entonces $f(x)$ y $g(x)$ no son polinomios constantes. En particular, $1 \leq \deg f(x), \deg g(x)$. Mas aun, la igualdad $m_{\alpha,F}(x) = f(x)g(x)$ implica que $\deg f(x), \deg q(x) < \deg m_{\alpha,F}(x)$ y que

$$0 = m_{\alpha,F}(\alpha) = f(\alpha)g(\alpha).$$

Como F es campo, esto implica que $f(\alpha) = 0$ o $g(\alpha) = 0$. En cualquier caso, como $\deg f(x), \deg q(x) < \deg m_{\alpha,F}(x)$, estamos contradiciendo el hecho de que (por definición)

$$\deg m_{\alpha,F}(x) = \deg q(x) \leq \deg a(x) \text{ para toda } \alpha(x) \in F[x] \text{ con } a(\alpha) = 0.$$

Por lo tanto, $m_{\alpha,F}(x)$ es irreducible y obtenemos lo deseado.

Fin de la demostración de existencia.

Antes de ver la unicidad, veamos la equivalencia

$$\alpha \text{ es raíz de } p(x) \in F[x] \iff m_{\alpha,F}(x) \text{ divide a } p(x) \text{ en } F[x].$$

para toda $p(x) \in F[x]$.

$\Longrightarrow$) Supongamos que $p(x) \in F[x]$ tiene a α como raíz. Por el algoritmo de la división en $F[x]$, existen $q(x), r(x) \in F[x]$ tales que

$$p(x) = q(x)m_{\alpha,F}(x) + r(x) \text{ con } r(x) = 0 \text{ o } \deg r(x) < \deg m_{\alpha,F}(x).$$

Evaluando en α obtenemos

$$0 = p(\alpha) = q(x)\cancelto{0}{m_{\alpha,F}(\alpha)} + r(\alpha) = r(\alpha).$$

Como (i) $\deg m_{\alpha,F}(x) = \deg q(x) \leq \deg a(x)$ para toda $\alpha(x) \in F[x]$ con $a(\alpha) = 0$ y (ii) $r(x) = 0$ o $\deg r(x) < \deg m_{\alpha,F}(x)$, entonces $r(x) = 0$. En particular, $p(x) = q(x)m_{\alpha,F}(x)$ y por lo tanto $m_{\alpha,F}(x)$ divide a $p(x)$ en $F[x]$.

$\Longleftarrow$) Si $m_{\alpha,F}(x)$ divide a $p(x)$ en $F[x]$, entonces existe $b(x) \in F[x]$ tal que $p(x) = b(x)m_{\alpha,F}(x)$. De donde $p(\alpha) = b(\alpha)m_{\alpha,F}(x) = b(\alpha)0 = 0$.

Ahora si, veamos la unicidad.

Unicidad.

Supongamos que $m(x) \in F[x]$ es mónico, irreducible, y tiene a α como raíz. Por la implicación "$\Longrightarrow$" de la equivalencia anterior, $m_{\alpha,F}(x)$ divide a $m(x)$ en $F[x]$. Es decir, existe $b(x) \in F[x]$ tal que $m(x) = b(x)m_{\alpha,F}(x)$. Como $m(x)$ es irreducible, esta igualdad implica que $b(x)$ es invertible o $m_{\alpha,F}(x)$ es invertible. Pero como $m_{\alpha,F}(x)$ no es invertible, entonces $b(x)$ es invertible. En particular, $b(x)$ es un polinomio constante. Finalmente, como $m_{\alpha,F}(x)$ y $m(x)$ son mónicos, la igualdad $m(x) = b(x)m_{\alpha,F}(x)$ implica que $b(x) = 1$. En particular, $m(x) = m_{\alpha,F}(x)$.

Fin de la demostración de unicidad.

□

$[F(\alpha) : F] = \deg_F \alpha$ si α es algebraico sobre F

Corolario 2

Supongamos que $\alpha \in K$ es algebraico sobre F. Entonces

$$F(\alpha) \cong F[x]/(m_{\alpha,F}(x)) \quad \text{y} \quad [F(\alpha) : F] = \deg_F \alpha.$$

Demostración. El isomorfismo $F(\alpha) \cong F[x]/(m_\alpha(x))$ es consecuencia inmediata de que α es raíz de $m_{\alpha,F}(x)$ y del teorema 2.5.1. La igualdad $[F(\alpha) : F] = \deg_F \alpha$ es consecuencia inmediata de que $m_{\alpha,F}(x)$ es irreducible y de que

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

para todo $p(x) \in F[x]$ irreducible en $F[x]$ con $p(\alpha) = 0$ (c.f. corolario 2.4.3). $\square$

Aplicaciones del corolario anterior

- Supongamos que $n \in \mathbb{Z}_{\geq 1}$. Por el criterio de Eisenstein, el polinomio $m_{2,\mathbb{Q}}(x) = x^n - 2$ es irreducible en $\mathbb{Q}[x]$. Por lo tanto,

$$[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n.$$

- En contraste, como $m_{\sqrt[n]{2},\mathbb{R}}(x) = x - \sqrt[n]{2}$, entonces por el corolario anterior,

$$[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{R}] = 1.$$

También notemos que acabamos de ver que el grado de un elemento depende del campo base de la extensión.

- $\sqrt{2} \notin \mathbb{Q}(\alpha)$ donde α es una raíz de cualquier polinomio $p(x) \in \mathbb{Q}[x]$ irreducible en $\mathbb{Q}[x]$ de grado n impar:

  De lo contrario, tendríamos $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\alpha)$ y por lo tanto,

$$\begin{aligned} n = \deg p(x) = [\mathbb{Q}(\alpha) : \mathbb{Q}] &= [\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2})]\,[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] \\ &= [\mathbb{Q}(\alpha) : \mathbb{Q}]\,2 \end{aligned}$$

  lo cual es imposible pues $[\mathbb{Q}(\alpha) : \mathbb{Q}] \in \mathbb{Z}_{\geq 1}$ y n es impar.

  Para apreciar un poquito mas la utilidad de la igualdad $[L : F] = [L : K][K : F]$ invitamos al lector a intentar probar que si (por ejemplo) $p(x) = x^3 + 3x + 1$ y α es la raíz real de este polinomio, entonces $\sqrt{2}$ no puede ser escrito como combinación lineal de $1, \alpha, \alpha^2$ (la base de $\mathbb{Q}(\alpha)$).

- $x^3 - \sqrt{2}$ es irreducible en $\mathbb{Q}(\sqrt{2})$:

  La igualdad

$$6 = [\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}(\sqrt{2})]\,[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}(\sqrt{2})]\,2$$

  implica que $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}(\sqrt{2})] = 3$ y por lo tanto,

$$\deg\left(m_{\sqrt[6]{2},\mathbb{Q}(\sqrt{2})}(x)\right) = 3.$$

  De donde,

$$m_{\sqrt[6]{2}}(x) = x^3 - \sqrt{2}.$$

  En particular, $x^3 - \sqrt{2}$ es irreducible en $\mathbb{Q}(\sqrt{2})$.

  De nuevo, para apreciar la utilidad de la igualdad $[L : F] = [L : K][K : F]$ invitamos al lector a intentar demostrar directamente que $x^3 - \sqrt{2}$ es irreducible en $\mathbb{Q}(\sqrt{2})$.

Si $F \subset K \subset L \subset M$ y $\alpha \in M$ es algebraico sobre F, entonces $m_{\alpha,L}(x)$ divide a $m_{\alpha,K}(x)$ en $L[x]$

Corolario 3

Supongamos que F, K, L, M son campos tales que $F \subset K \subset L \subset M$. Si α es algebraico sobre K y también es algebraico sobre L, entonces $m_{\alpha,L}(x)$ divide a $m_{\alpha,K}(x)$ en $L[x]$.

En particular, $\deg m_{\alpha,L}(x) \leq \deg m_{\alpha,K}$ si $K \subset L$.

Demostración. Por la proposición anterior, ya sabemos que

$$\alpha \text{ es raíz de } p(x) \in L[x] \iff m_{\alpha,L}(x) \text{ divide a } p(x) \text{ en } L[x]$$

para toda $p(x) \in L[x]$. Poniendo $p(x) = m_{\alpha,F}(x)$ obtenemos lo deseado. $\square$

$[F(\alpha) : F] \leq \deg p(x)$ para todo $p(x) \in F[x]$ con $p(\alpha) = 0$

Corolario 4

Si $\alpha \in K$ es algebraico, entonces

$$[F(\alpha) : F] \leq \deg p(x) \text{ para todo } p(x) \in F[x] \text{ con } p(\alpha) = 0.$$

Demostración. Supongamos que $\alpha \in K$ es algebraico. Entonces $m_\alpha(x)$ existe y sabemos que satisface

1. $m_\alpha(x)$ divide a $p(x)$ para todo $p(x) \in F[x]$ con $p(\alpha) = 0$ y
2. $[F(\alpha) : F] = \deg m_\alpha(x)$.

Una consecuencia de (1) es que $\deg m_\alpha(x) \leq \deg p(x)$ para todo $p(x) \in F[x]$ con $p(\alpha) = 0$. Juntando esto con (2) obtenemos lo deseado. $\square$

Extensión finita $\implies$ extensión algebraica

Proposición 5

Supongamos que $[K : F] = n < \infty$. Entonces para toda $\alpha \in K$ existe $p(x) \in F[x]$ tal que $\deg p(x) \leq n$ y $p(\alpha) = 0$.

En particular, $\alpha \in K$ es algebraico. Como esto es para cualquier $\alpha \in K$, entonces la extensión K/F es algebraica.

Demostración. Supongamos que $[K : F] = n$ y que $\alpha \in K$. Como cualquier conjunto de vectores con cardinalidad mayor que la base es linealmente dependiente (c.f. corolario 2.2.2), entonces los $n + 1$ vectores $1, \alpha, \alpha^2, \ldots, \alpha^n$ son linealmente dependientes. Es decir, existen $b_0, b_1, b_2, \ldots, b_n \in F$ no todos cero tales que

$$b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_n\alpha^n = 0.$$

Por lo tanto, $p(x) := b_0 + b_1x + b_2x^2 + \cdots + b_nx^n$ cumple lo deseado. $\square$

Corolario 6

Para toda $\alpha \in K$,

$$\alpha \in K \text{ es algebraico sobre } F \iff \text{la extensión } F(\alpha)/F \text{ es finita.}$$

Demostración.

$\Longrightarrow$) Es consecuencia inmediata del corolario 4.

$\Longleftarrow$) Es consecuencia inmediata de la proposición 5.

□

Terminamos esta sección generalizando la famosa formula chicharronera.

La chicharronera en campos con característica $\neq 2$

Proposición 7

Supongamos que K/F es una extensión de campos y que $\mathrm{ch}(F) \neq 2$. Sea

$$p(x) = x^2 + bx + c \in F[x]$$

Si α es una raíz de $p(x)$ en K, entonces la ecuación

$$x^2 - (b^2 - 4c) = 0$$

tiene soluciones $x = \pm(b + 2\alpha)$. Mas aun, si denotamos $\sqrt{b^2 - 4c} = b + 2\alpha$, entonces las las raíces de $p(x)$ son

$$\frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

La demostración es muy sencilla y por eso se la dejamos al lector. Cabe recalar que la hipótesis $\mathrm{ch}(F) \neq 2$ es necesaria para que el cociente $\frac{-b \pm \sqrt{b^2-4c}}{2}$ tenga sentido.

Extensiones cuadráticas

Proposición 8

Si K/F es una extensión de campos y $\mathrm{ch}(F) \neq 2$, entonces $[K : F] = 2$ si y solo si $K = F(\sqrt{D})$ donde $\sqrt{D}$ es una solución a la ecuación

$$x^2 - D = 0$$

y D es tal que $a^2 \neq D$ para toda $a \in F$.

Por esta equivalencia, a los extensiones de campo con grado 2, les llamamos **extensiones cuadráticas**.

Demostración.

$\Longleftarrow$) Primero notemos que como $a^2 \neq D$ para toda F, entonces el polinomio $x^2 - D$ no tiene raíces en F y por lo tanto (como es de grado 2), $x^2 - D$ es irreducible en $F[x]$. Entonces $m_{\sqrt{D},F}(x) = x^2 - D$ y por lo tanto

$$[K : F] = [F(\sqrt{D}) : F] = \deg m_{\sqrt{D},F}(x) = 2.$$

$\Longrightarrow$) Supongamos que $[K : F] = 2$. Sea $\alpha \in K \setminus F$. Por la proposición 5, existe $p(x) \in F[x]$ tal que $\deg p(x) \leq 2$ y $p(\alpha) = 0$.

Ahora bien, como α es raíz de $f(x)$, entonces $\deg m_{\alpha,F}(x) \leq \deg p(x)$. Veamos que $\deg m_{\alpha,F}(x) = 2$. Como $\deg m_{\alpha,F}(x) \leq \deg p(x) \leq 2$, entonces basta probar que $\deg m_{\alpha,F}(x) \neq 1$. De lo contrario, existirían $a_0, a_1 \in F$ tales que

$$m_{\alpha,F}(x) = a_1 x + a_0 \quad \text{y} \quad 0 = p(\alpha) = a_1\alpha + a_0$$

Despejando α obtendríamos $\alpha = -\frac{a_0}{a_1} \in F$. Contradiciendo $\alpha \in K \setminus F$.

Por lo tanto, $\deg m_{\alpha,F}(x) = 2$. Como (por definición) $m_{\alpha,F}(x)$ es mónico, entonces existen $b, c \in F$ tales que

$$m_{\alpha,F}(x) = x^2 + bx + c.$$

Por la proposición anterior, las raíces de $m_{\alpha,F}(x)$ son

$$\frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

Es fácil verificar que $D = b^2 - 4c$ cumple lo deseado. $\square$

Las soluciones de una ecuación cuadrática viven (en el peor de los casos) en una extensión cuadrática

Corolario 9

Supongamos que K/F es una extensión de campos, que $\mathrm{ch}(F) \neq 2$, y que $b, c \in F$. Si $x \in K$ es tal que

$$x^2 + bx + c = 0,$$

entonces existe $\alpha \in F$ tal que $x \in F(\sqrt{\alpha})$.

Demostración. Por la proposición 7,

$$x = \frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

Por lo tanto, $x \in F\left(\sqrt{b^2 - 4c}\right) \subset K$. □