Extensiones finitamente generadas

Facultad de Ciencias UNAM

Introducción

Conociendo la importancia de $F(\alpha) \subset K$ donde $\alpha \in K$ es algebraico sobre F, es natural interesarse en las extensiones de la forma $F(\alpha_1, \ldots, \alpha_k) \subset K$ donde $\alpha_1, \ldots, \alpha_k \in K$ son algebraicos sobre F. En esta sección estudiamos extensiones de esta forma.

Proposición 1

Si $\alpha, \beta \in K$ son algebraicos sobre F, entonces

$$F(\alpha, \beta) = \big(F(\alpha)\big)(\beta)$$

En palabras, el campo generado por α y β sobre F coincide con el campo generado por β sobre $F(\alpha)$.

Demostración.

$\subset$) Claramente, $\big(F(\alpha)\big)(\beta)$ es un campo que contiene a F, α, y β. Por lo tanto, (por definición de $\big(F(\alpha)\big)(\beta)$) $F(\alpha, \beta) \subset \big(F(\alpha)\big)(\beta)$.

$\supset$) Claramente, $F(\alpha, \beta)$ es un campo que contiene a $F(\alpha)$ y β. Por lo tanto, (por definición de $F(\alpha, \beta)$) $\big(F(\alpha)\big)(\beta) \subset F(\alpha, \beta)$.

$\square$

Corolario 2

Si $\alpha, \beta \in K$ son algebraicos, entonces

$$[F(\alpha,\beta):F] = \deg_F \alpha \cdot \deg_{F(\alpha)} \beta.$$

En particular, $[F(\alpha,\beta):F] \leq \deg_F \alpha \cdot \deg_F \beta$.

Demostración. Para ver la igualdad, considera

$$\begin{aligned}
[F(\alpha,\beta):F] &= [\big(F(\alpha)\big)(\beta):F] \\
&= [\big(F(\alpha)\big)(\beta):F(\alpha)]\,[F(\alpha):F] \\
&= \deg_{F(\alpha)} \beta \cdot \deg_F \alpha.
\end{aligned}$$

Donde la ultima igualdad se cumple por el corolario 2.6.2.

Para ver la desigualdad simplemente recuerda que $\deg_L \gamma \leq \deg_K \gamma$ cuando $K \subset L$ (c.f. corolario 2.6.3) y usa la igualdad anterior. □

El grado de $F(\alpha_1, \alpha_2, \ldots, \alpha_k)$ sobre F

Corolario 3

Si que $\alpha_1, \alpha_2, \ldots, \alpha_k \in K$ son algebraicos, entonces

$$[F(\alpha_1, \alpha_2, \ldots, \alpha_k) : F] =$$
$$(\deg_F \alpha_1) \cdot \left(\deg_{F(\alpha_1)} \alpha_2\right) \cdot \left(\deg_{F(\alpha_1,\alpha_2)}\right) \cdots \left(\deg_{F(\alpha_1,\ldots,\alpha_{k-1})} \alpha_k\right)$$

En particular,

$$[F(\alpha_1, \alpha_2, \ldots, \alpha_k) : F] \leq \deg_F \alpha_1 \cdot \deg_F \alpha_2 \cdots \deg_F \alpha_k.$$

Demostración. Usando el corolario anterior, la demostración de la igualdad es una inducción sencilla sobre k y por eso se la dejamos al lector. La desigualdad es consecuencia inmediata de la igualdad. □

Un caso donde $[F(\alpha,\beta):F] < \deg_F \alpha \cdot \deg_F \beta$

Si $F=\mathbb{Q}$, $\alpha=\sqrt[6]{2}$ y $\beta=\sqrt{2}$, entonces $\beta^3=\alpha$ y por lo tanto, $\sqrt{2}\in\mathbb{Q}(\sqrt[6]{2})$. De donde, $\deg_{\mathbb{Q}(\sqrt[6]{2})}\sqrt{2}=1$ y

$$\begin{aligned}[\mathbb{Q}(\sqrt[6]{2},\sqrt{2}):\mathbb{Q}] &= \deg_{\mathbb{Q}}\sqrt[6]{2}\cdot\deg_{\mathbb{Q}(\sqrt[6]{2})}\sqrt{2}\\ &< \deg_{\mathbb{Q}}\sqrt[6]{2}\cdot 2\\ &= \deg_{\mathbb{Q}}\sqrt[6]{2}\cdot\deg_{\mathbb{Q}}\sqrt{2}\end{aligned}$$

Una aplicación de la igualdad $[F(\alpha, \beta) : F] = \deg_F \alpha \cdot \deg_{F(\alpha)} \beta$

Veamos que $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$.

Primero notemos que como $x^2 - 3$ es irreducible, mónico y tiene a $\sqrt{3}$ como raíz, entonces

$$m_{\sqrt{3},\mathbb{Q}}(x) = x^2 - 3$$

De donde,

$$\deg m_{\sqrt{3},\mathbb{Q}(\sqrt{2})}(x) \leq \deg m_{\sqrt{3},\mathbb{Q}}(x) = 2. \tag{1}$$

Usando esto, veamos que $\deg m_{\sqrt{3},\mathbb{Q}(\sqrt{2})}(x)$ es precisamente 2. De lo contrario, por (1) tendríamos $\deg m_{\sqrt{3},\mathbb{Q}(\sqrt{2})}(x) = 1$ o equivalentemente, existirían $a, b \in\in \mathbb{Q}$ tales que

$$\sqrt{3} = a + b\sqrt{2}.$$

Alzando al cuadrado esta ecuación obtenemos

$$3 = a^2 + 2ab\sqrt{2} + b^2 2 \in \mathbb{Q}(\sqrt{2})$$

De donde[1]

$$3 = a^2 + b^2 2 \quad \text{y} \quad 0 = 2ab\sqrt{2}.$$

Por la segunda ecuación, tenemos dos casos:

Caso 1. $a = 0$: Entonces despejando b de la primera ecuación tendríamos $\sqrt{\frac{3}{2}} = b \in \mathbb{Q}$, lo cual no es cierto.

Caso 2. $b = 0$: Entonces despejando a de la primera ecuación tendríamos $\sqrt{3} = a \in \mathbb{Q}$, lo cual tampoco es cierto.

Una contradicción. Por lo tanto, $\deg m_{\sqrt{3},\mathbb{Q}(\sqrt{2})}(x) = 2$ y

$$\begin{aligned}[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] &= [\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2}]\,[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] \\ &= \underbrace{[\Big(\mathbb{Q}(\sqrt{2})\Big)\,(\sqrt{3}) : \mathbb{Q}(\sqrt{2})]}_{\deg m_{\sqrt{3},\mathbb{Q}(\sqrt{2})}(x)}\,[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4.\end{aligned}$$

[1] Recuerda que en la proposición 1.14.2 demostramos que si $D \in \mathbb{Q}$ es tal que $\sqrt{D} \notin \mathbb{Q}$, entonces $a + b\sqrt{D} = c + d\sqrt{D}$ implica $a = c$ y $b = d$.

$[F(\alpha,\beta):F] = \deg_F \alpha \cdot \deg_F \beta$ si ¿?

Corolario 4

Supongamos que $\alpha, \beta \in K$ son algebraicos sobre F. Si $m_{\beta,F}(x)$ es irreducible en $F(\alpha)[x]$, entonces

$$[F(\alpha,\beta):F] = \deg_F \alpha \cdot \deg_F \beta.$$

Demostración. Por hipótesis, $m_{\beta,F}(x)$ es irreducible en $F(\alpha)[x]$ y por definición, $m_{\beta,F}(x)$ tiene a β como raíz. Esto implica[2] que $m_{\beta,F(\alpha)}(x) = m_{\beta,F}(x)$. De donde,

$$[\big(F(\alpha)\big)(\beta) : F(\alpha)] = \deg m_{\beta,F(\alpha)}(x) = \deg m_{\beta,F}(x) = \deg_F \alpha$$

Entonces (por el corolario 3),

$$[F(\alpha,\beta):F] = \deg_F \alpha \cdot \deg_{F(\alpha)} \beta = \deg_F \alpha \cdot \deg_F \beta.$$

□

[2] Recuerda que (por definición) el polinomio mínimo de β sobre $F(\alpha)$ es el *único* polinomio mónico irreducible en $F(\alpha)[x]$ que tiene a β como raíz

Una F-base de $F(\alpha, \beta)$

Proposición 5

Si $\alpha, \beta \in K$ son algebraicos sobre F, $n = \deg_F \alpha$, y $m = \deg_{F(\alpha)}(\beta)$, entonces

$$\mathcal{B} = \left\{ \alpha^i \beta^j \mid i \in \{0, 1 \ldots, n-1\} \text{ y } j \in \{0, 1, \ldots, m-1\} \right\}$$

es una F-base de $F(\alpha, \beta)$.

Demostración. Por el corolario 2.5.2, ya sabemos que

- $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ es una F-base de $F(\alpha)$ y que
- $\{1, \beta, \beta^2, \ldots, \beta^{m-1}\}$ es una $F(\alpha)$-base de $\big(F(\alpha)\big)(\beta) = F(\alpha, \beta)$.

Ahora bien, como

$$[F(\alpha,\beta):F] = \deg_F \alpha \cdot \deg_{F(\alpha)} \beta = n \cdot m,$$

$$|\mathcal{B}| = \left|\left\{\alpha^i\beta^j \mid i \in \{0,1\ldots,n-1\} \text{ y } j \in \{0,1,\ldots,m-1\}\right\}\right| = n \cdot m,$$

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 $\mathcal{B}$ es un F-conjunto generador de $F(\alpha,\beta)$.

Para esto, supongamos que $v \in F(\alpha,\beta)$. Como $\{1,\beta,\beta^2,\ldots,\beta^{m-1}\}$ es una $F(\alpha)$-base de $F(\alpha,\beta)$, entonces podemos escribir

$$v = \lambda_0 + \lambda_1\beta + \lambda_2\beta^2 + \cdots + \lambda_{m-1}\beta^{m-1}$$

para algunas $\lambda_0,\lambda_1,\lambda_2,\ldots,\lambda_{m-1} \in F(\alpha)$.

Mas aun, como $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ es una F-base de $F(\alpha)$, entonces para cada $j \in \{0, 1 \ldots, m-1\}$ podemos escribir

$$\lambda_j = \mu_{0,j} + \mu_{1,j}\alpha + \mu_{2,j}\alpha^2 + \cdots + \mu_{n-1,j}\alpha^{n-1}$$

Si sustituimos cada una de estas expresiones en la igualdad

$$v = \lambda_0 + \lambda_1\beta + \lambda_2\beta^2 + \cdots + \lambda_{m-1}\beta^{m-1}$$

y luego distribuimos, obtenemos lo deseado. □

Una F-base de $F(\alpha_1, \alpha_2, \ldots, \alpha_k)$

Proposición 6

Supongamos que $\alpha_1, \alpha_2, \ldots, \alpha_k \in K$ son algebraicos sobre F y para cada $i \in \{0, 1 \ldots, k-1\}$ denotemos

$$F_{i+1} = F_i(\alpha_{i+1}) \quad \text{y} \quad n_{i+1} = \deg_{F_i} \alpha_{i+1}.$$

donde $F_0 = F$. Entonces

$$\left\{ \alpha_1^{j_1} \alpha_2^{j_2} \cdots \alpha_m^{j_m} \mid j_l \in \{0, 1 \ldots, n_i - 1\} \text{ para cada } l \in \{1, 2, \ldots, k\} \right\}$$

es una F-base de $F(\alpha_1, \alpha_2, \ldots, \alpha_k)$.

Demostración. De nuevo, usando el corolario anterior, la demostración es una inducción sencilla (pero tediosa) sobre k y por eso se la dejamos al lector. □

Un conjunto generador de $F(\alpha_1, \alpha_2, \ldots, \alpha_k)$

Corolario 7

Supongamos que $\alpha_1, \alpha_2, \ldots, \alpha_k \in K$ son algebraicos sobre F. Si para cada $i \in \{1, \ldots, k\}$ denotamos $N_i = \deg_F \alpha_i$, entonces

$$\left\{ \alpha_1^{j_1} \alpha_2^{j_2} \cdots \alpha_m^{j_m} \mid j_l \in \{0, 1 \ldots, N_i - 1\} \text{ para cada } l \in \{1, 2, \ldots, k\} \right\} \tag{2}$$

es un F-conjunto generador de $F(\alpha_1, \alpha_2, \ldots, \alpha_k)$.

Demostración. Usando la notación de la proposición anterior tenemos que $F \subset F_i$ para toda $i \in \{1, \ldots, k\}$ y por lo tanto

$$n_i = \deg_{F_{i-1}} \alpha_i \leq \deg_F \alpha_i = N_i$$

para toda $i \in \{1, \ldots, k\}$. Usando esto (y la proposición anterior) vemos que el conjunto en (2) contiene una base y en particular, F-genera. $\square$

Extensiones finitamente generadas

Definición

Decimos que una extensión K/F es **finitamente generada** si existen $\alpha_1, \ldots, \alpha_n \in K$ tales que $K = F(\alpha_1, \ldots, \alpha_n)$.

Una extensión es finita si y solo si es finitamente generada por elementos algebraicos.

Teorema 8

$[K : F] < \infty$ si y solo si $K = F(\alpha_1, \ldots, \alpha_n)$ para algunos $\alpha_1, \ldots, \alpha_n \in K$ algebraicos sobre F.

Demostración.

$\Longrightarrow$) Supongamos que $[K : F] = n < \infty$ y que $\{\alpha_1, \ldots, \alpha_n\}$ es una F-base de K. Obviamente $K = F(\alpha_1, \ldots, \alpha_n)$ y por lo tanto, solo resta probar que cada α_i es algebraico. En el corolario 2.6.6, vimos que esto es equivalente a que $[F(\alpha_i) : F] < \infty$. Pero esto es consecuencia de que

$$[F(\alpha) : F] \leq [K : F(\alpha)][F(\alpha) : F] = [K : F] < \infty.$$

$\Longleftarrow$) Si $K = F(\alpha_1, \ldots, \alpha_n)$ con $\alpha_1, \ldots, \alpha_n \in K$ algebraicos, entonces

$$[K : F] = [F(\alpha_1, \ldots, \alpha_k) : F] \leq \deg_F \alpha_1 \cdots \deg_F \alpha_k < \infty$$

Donde la primera desigualdad es por el corolario 3.

□

La suma, resta, multiplicación, y división de elementos algebraicos es un elemento algebraico

Corolario 9

Si $\alpha, \beta \in K$ son algebraicos sobre F, entonces $\alpha \pm \beta$, $\alpha\beta$, y α/β también son algebraicos sobre F.

Demostración. Los elementos $\alpha \pm \beta$, $\alpha\beta$, y α/β pertenecen a la extensión $F(\alpha, \beta)/F$ que es finitamente generada por elementos algebraicos. Por el teorema anterior, la extensión $F(\alpha, \beta)/F$ es finita. Finalmente, como toda extensión finita es algebraica (c.f. corolario 2.6.6), obtenemos lo deseado. $\square$

El conjunto de elementos que son algebraicos sobre F es un subcampo de K

Corolario 10

Si $L = \{\alpha \in K \mid \alpha \text{ es algebraico sobre } F\}$, entonces L es un subcampo de K tal que $F \subset L \subset K$.

Demostración. Las inclusiones $F \subset L \subset K$ son evidentes. El hecho de que L es subcampo es consecuencia inmediata del corolario anterior. $\square$

El campo de números algebraicos

Definición

Considera la extensión $\mathbb{C}/\mathbb{Q}$. El **campo de números algebraicos**, es el siguiente subcampo de $\mathbb{C}$

$$\overline{\mathbb{Q}} := \left\{\alpha \in \mathbb{Q} \mid \alpha \text{ es algebraico sobre } \mathbb{C}\right\}.$$

Por ejemplo, $\sqrt[n]{2} \in \overline{\mathbb{Q}}$ para toda $n \in \mathbb{Z}_{\geq 2}$. Veamos que esto implica que, $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$. Si $[\overline{\mathbb{Q}} : \mathbb{Q}] < \infty$, entonces

$$[\overline{\mathbb{Q}} : \mathbb{Q}] = [\overline{\mathbb{Q}} : \mathbb{Q}(\sqrt[n]{2})] \underbrace{[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}]}_{n} \geq n$$

para toda $n \in \mathbb{Z}_{\geq 2}$. Contradiciendo $[\overline{\mathbb{Q}} : \mathbb{Q}] < \infty$.

Observación

Veamos que el conjunto de elementos de $\mathbb{R}$ que son algebraicos en $\mathbb{Q}$ es numerable: Primero considera las siguientes igualdades.

$$\begin{aligned}\overline{\mathbb{Q}} \cap \mathbb{R} &= \{\text{elementos de } \mathbb{R} \text{ que son algebraicos en } \mathbb{Q}\} \\ &= \{\alpha \in \mathbb{R} \mid \exists p(x) \in \mathbb{Q}[x] \text{ tal que } p(\alpha) = 0\} \\ &= \bigcup_{p(x)\in\mathbb{Q}[x]} \{\text{las raíces reales de } p(x)\}.\end{aligned}$$

Como $\mathbb{Q}[x]$ es numerable (es biyectable con el conjunto de sucesiones finitas en $\mathbb{Q}$) y todo $p(x) \in \mathbb{Q}[x]$ tiene a lo mas $\deg p(x)$ raíces en $\mathbb{R}$ (c.f. proposición 1.27.2), entonces el ultimo termino de las igualdades es una unión numerable de conjuntos finitos y en particular, es un conjunto numerable. En particular, $\overline{\mathbb{Q}} \cap \mathbb{R} \subsetneqq \mathbb{R}$ y esto implica que $\overline{\mathbb{Q}} \subsetneqq \mathbb{C}$. Mas aun, como $\mathbb{R}$ es no numerable, entonces $\mathbb{R} \setminus \left(\overline{\mathbb{Q}}) \cap \mathbb{R}\right)$ es no numerable. En palabras, hay una cantidad no numerable de reales trascendentales (en $\mathbb{Q}$).

La propiedad "es algebraico sobre" es transitiva

Proposición 11

Supongamos que L/K y K/F son extensiones de campos. Si L/K y K/F son algebraicas, entonces L/F también es algebraica.

Demostración. Supongamos que $\alpha \in L$. Como L/K es algebraica, existen $a_0, a_1, \ldots, a_n \in K$ tales que

$$0 = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n.$$

Notemos que para ver que α es algebraico sobre K, basta probar que $F(\alpha, a_0, a_1, \ldots, a_n)/F$ es una extensión finita. En efecto, si $F(\alpha, a_0, a_1, \ldots, a_n)/F$ es una extensión finita, entonces (por el teorema 8) también sera algebraica. En particular, (como $\alpha \in F(\alpha, a_0, a_1, \ldots, a_n)$) α sera algebraico sobre F.

Por lo tanto, veamos que $F(\alpha, a_0, a_1, \ldots, a_n)/F$ es una extensión finita.

Primero notemos que como K/F es algebraica, entonces $a_0, a_1, \ldots, a_n \in K$ son algebraicos sobre F y por lo tanto, (por el teorema 8) la extensión $F(a_0, a_1, \ldots, a_n)/F$ es finita. Equivalentemente,

$$[F(a_0, a_1, \ldots, a_n) : F] < \infty. \tag{3}$$

Por otro lado, notemos que

$$[F(\alpha, a_0, a_1, \ldots, a_n) : F(a_0, a_1, \ldots, a_n)] = \left[\left(F(a_0, a_1, \ldots, a_n)\right)(\alpha) : F(a_0, a_1, \ldots, a_n)\right] \leq \deg_F \alpha. \tag{4}$$

Juntando (3) y (4), obtenemos

$$[F(\alpha, a_0, a_1, \ldots, a_n) : F] = [F(\alpha, a_0, a_1, \ldots, a_n) : F(a_0, a_1, \ldots, a_n)]\,[F(a_0, a_1, \ldots, a_n) : F] < \infty.$$

□