El producto de subcampos

Facultad de Ciencias UNAM

Introducción

En esta sección definimos y estudiamos el producto de de dos subcampos. Este concepto no aparecerá mucho en el futuro, pero ocasionalmente es útil.

El producto de subcampos

Definición

Supongamos que K_1 y K_2 son subcampos de K. El **producto** de K_1 y K_2, denotado K_1K_2 es el subcampo mas chico de K que contiene a K_1 y K_2. Específicamente,

$$K_1K_2 := \bigcap \{S \mid S \text{ es un subcampo de } K \text{ tal que } K_1 \cup K_2 \subset S\}$$

Análogamente, para $K_1, K_2, \ldots, K_n$ subcampos de K, definimos $K_1K_2 \cdots K_n$. Específicamente,

$$K_1K_2 \cdots K_n := \bigcap \left\{S \mid S \text{ es un subcampo de } K \text{ tal que } \bigcup_{i=1}^{n} K_i \subset S\right\}$$

$F(\alpha_1, \ldots, \alpha_n)F(\beta_1, \ldots, \beta_m) = F(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m)$

Proposición 1

Supongamos que K/F es una extensión de campos. Si $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m \in L$, entonces

$$F(\alpha_1, \ldots, \alpha_n)F(\beta_1, \ldots, \beta_m) = F(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m)$$

Demostración.

$\subset$) Es consecuencia inmediata de las siguientes dos observaciones:

- Por definición, $F(\alpha_1, \ldots, \alpha_n)F(\beta_1, \ldots, \beta_m)$ es el subcampo mas chico de K que contiene a $F(\alpha_1, \ldots, \alpha_n)$ y a $F(\beta_1, \ldots, \beta_m)$.
- $F(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m)$ es un subcampo de K que contiene a $F(\alpha_1, \ldots, \alpha_n)$ y a $F(\beta_1, \ldots, \beta_m)$.

$\supset$) Es consecuencia inmediata de la siguientes dos observaciones:

- $F(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m)$ es el subcampo mas chico de K que contiene a F y a $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m$.
- $F(\alpha_1, \ldots, \alpha_n)F(\beta_1, \ldots, \beta_m)$ es un subcampo de K que contiene a F y a $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m$.

$\square$

Corolario 2

Supongamos que K/F es una extensión de campos. Si $\gamma_1,\dots,\gamma_r \in L$ con $r \in \mathbb{Z}_{\geq 1}$, entonces

$$F(\gamma_1)\cdots F(\gamma_r) = F(\gamma_1,\dots,\gamma_r)$$

Demostración. Procedemos por inducción sobre el numero de elementos. El paso $r = 1$ es trivial y el paso $r = 2$ es un caso particular de la proposición anterior. Por eso, supongamos que $r \geq 3$ y que la igualdad se satisface si el numero de elementos es estrictamente menor a r. Entonces

$$\begin{aligned} F(\gamma_1)\cdots F(\gamma_r) &= F(\gamma_1,\dots,\gamma_{r-1})F(\gamma_r) && \text{(por hipótesis de inducción)} \\ &= F(\gamma_1,\dots,\gamma_{r-1},\gamma_r). && \text{(por la proposición anterior)} \end{aligned}$$

$\square$

Un par de ejemplos

Una consecuencia inmediata de lo visto anteriormente es que

$$\mathbb{Q}(\sqrt{2})\mathbb{Q}(\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}).$$

A veces sucede que podemos simplificar un campo de la forma $F(\alpha, \beta)$ en un campo de la forma $F(\gamma)$. Por ejemplo, veamos que

$$\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) = \mathbb{Q}(\sqrt[6]{2}).$$

$\subset$) Es consecuencia de que $\sqrt{2}, \sqrt[3]{2} \in \mathbb{Q}(\sqrt[6]{2})$ y esto es consecuencia de que $(\sqrt[6]{2})^3 = \sqrt{2}$ y $(\sqrt[6]{2})^2 = \sqrt[3]{2}$.

$\supset$) Es consecuencia de que $\sqrt[6]{2} \in \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ y esto es consecuencia de que $\frac{\sqrt{2}}{\sqrt[3]{2}} = (2)^{1/2}(2)^{-1/3} = 2^{1/6} = \sqrt[6]{2}$.

En particular,

$$\mathbb{Q}(\sqrt{2})\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}(\sqrt[6]{2}).$$

El grado de un producto

Proposición 3

Supongamos que F, K_1, K_2, K son campos tales que $F \subset K_1 \subset K$ y $F \subset K_2 \subset K$. Si $\{\alpha_1, \ldots, \alpha_n\}$ es una F-base de K_1 y $\{\beta_1, \ldots, \beta_m\}$ es una F-base de K_2, entonces

$$K_1K_2 = F(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n)$$

y

$$\{\alpha_i\beta_j \mid i \in \{1, \ldots, n\} \text{ y } j \in \{1, \ldots, m\}\}$$

es un F-conjunto generador de K_1K_2. En particular,

$$[K_1K_2 : F] \leq [K_1 : F][K_2 : F]$$

y la igualdad se satisface si y solo si $\{\alpha_1, \ldots, \alpha_n\}$ es K_2-linealmente independiente o $\{\beta_1, \ldots, \beta_m\}$ es K_1-linealmente independiente.

Demostración. Supongamos que $\{\alpha_1, \ldots, \alpha_n\}$ es una F-base de K_1 y que $\{\beta_1, \ldots, \beta_m\}$ es una F-base de K_2. Usando las puras definiciones, es fácil verificar que

$$K_1K_2 = F(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n).$$

Por el corolario 2.7.7 ya sabemos que esto implica que si $N_i = \deg_F \alpha_i$ y $M_j = \deg_F \beta_j$, entonces el conjunto

$$\left\{\alpha_1^{k_1} \cdots \alpha_n^{k_n} \beta_1^{l_1} \cdots \beta_m^{l_m} \mid k_i \in \{1, \ldots, N_i - 1\} \text{ y } l_j \in \{1, \ldots, M_j - 1\}\right\}$$

es un F-conjunto generador de $F(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n) = K_1K_2$. Ahora bien, como $\{\alpha_1, \ldots, \alpha_n\}$ es una F-base de K_1, entonces

$$\alpha_1^{k_1} \cdots \alpha_n^{k_n} \in K_1 = \operatorname{span}_F(\alpha_1, \ldots, \alpha_n) \text{ con } k_i \in \{1, \ldots, N_i - 1\}. \tag{1}$$

Análogamente, como $\{\beta_1, \ldots, \beta_m\}$ es una F-base de K_2, entonces

$$\beta_1^{l_1} \cdots \beta_m^{l_m} \in K_2 = \operatorname{span}_F(\beta_1, \ldots, \beta_m) \text{ con } l_j \in \{1, \ldots, M_j - 1\}. \tag{2}$$

Es fácil verificar que (1) y (2) implican que

$$\alpha_1^{k_1}\cdots\alpha_n^{k_n}\beta_1^{l_1}\cdots\beta_m^{l_m}\in \operatorname{span}_F\left(\left\{\alpha_i\beta_j \mid i\in\{1,\ldots,n\} \text{ y } j\in\{1,\ldots,m\}\right\}\right).$$

Juntando esto con el hecho de que el conjunto

$$\left\{\alpha_1^{k_1}\cdots\alpha_n^{k_n}\beta_1^{l_1}\cdots\beta_m^{l_m} \mid k_i\in\{1,\ldots,N_i-1\} \text{ y } l_j\in\{1,\ldots,M_j-1\}\right\}$$

es un F-conjunto generador de $F(\alpha_1,\ldots,\alpha_n,\beta_1,\ldots,\beta_n)=K_1K_2$ obtenemos que

$$\left\{\alpha_i\beta_j \mid i\in\{1,\ldots,n\} \text{ y } j\in\{1,\ldots,m\}\right\}$$

es un F-conjunto generador de K_1K_2.

En particular, (como todo conjunto generador tiene cardinalidad mayor o igual que la dimensión, entonces)

$$[K_1K_2:F]\leq nm=[K_1:F][K_2:F].$$

Finalmente, veamos que $[K_1K_2 : F] = [K_1 : F][K_2 : F]$ si y solo si $\{\alpha_1, \ldots, \alpha_n\}$ es K_2-linealmente independiente o $\{\beta_1, \ldots, \beta_m\}$ es K_1-linealmente independiente.

$\Longrightarrow$) Si $[K_1K_2 : F] = [K_1 : F][K_2 : F]$, entonces (como todo conjunto generador con cardinalidad igual a la dimensión es una base)

$$\left\{\alpha_i\beta_j \mid i \in \{1, \ldots, n\} \text{ y } j \in \{1, \ldots, m\}\right\}$$

es una F-base de K_1K_2. Es fácil verificar que esto implica que $\{\alpha_1, \ldots, \alpha_n\}$ es K_2-linealmente independiente *y también* que $\{\beta_1, \ldots, \beta_m\}$ es K_1-linealmente independiente.

$\Longleftarrow$) Si $\{\alpha_1, \ldots, \alpha_n\}$ es K_2-linealmente independiente o $\{\beta_1, \ldots, \beta_m\}$ es K_1-linealmente independiente es fácil verificar que

$$\left\{\alpha_i\beta_j \mid i \in \{1, \ldots, n\} \text{ y } j \in \{1, \ldots, m\}\right\}$$

es una F-base de K_1K_2 y por lo tanto $[K_1K_2 : F] = nm = [K_1 : F][K_2 : F]$.

$\square$

$[K_1K_2 : F] = [K_1 : F][K_2 : F]$ si ¿?

Corolario 4

Supongamos que F, K_1, K_2, K son campos tales que $F \subset K_1 \subset K$ y $F \subset K_2 \subset K$. Si $[K_1 : F]$ y $[K_2 : F]$ son primos relativos, entonces

$$[K_1K_2 : F] = [K_1 : F][K_2 : F].$$

Demostración. Ya sabemos que $[K_1K_2 : F] \leq [K_1 : F][K_2 : F]$, veamos que $[K_1 : F][K_2 : F] \leq [K_1K_2 : F]$. Para esto, primero recordemos que como $F \subset K_1, K_2 \subset K$, entonces

$$[K_1 : F] \text{ divide a } [K_1K_2 : F] \quad \text{y} \quad [K_2 : F] \text{ divide a } [K_1K_2 : F].$$

De donde,

$$\operatorname{mcm}\left\{[K_1 : F], [K_2 : F]\right\} \text{ divide a } [K_1K_2 : F] \tag{3}$$

pero como n y m son primos relativos, entonces

$$\operatorname{mcm}\left\{[K_1 : F], [K_2 : F]\right\} = [K_1 : F][K_2 : F]$$

Juntando esto con (3) obtenemos lo deseado. $\square$