Introducción a teoría de campos

Facultad de Ciencias UNAM

Introducción

En esta sección veremos las definiciones básicas y algunos resultados de teoría de campos.

Homomorfismos de campos

Definición

Supongamos que F y F' son campos. Decimos que una función $\phi : F \to F'$ es un **homomorfismo de campos** si

- ϕ es un homomorfismo de anillos y
- $\phi(1_F) = 1_{F'}$.

Naturalmente, también decimos que $\phi : F \to F'$ es un **isomorfismo de campos** si es un homomorfismo de campos biyectivo.

En lo que sigue, si F y F' son campos y decimos que $\phi : F \to F'$ es un homomorfismo, queremos decir que $\phi : F \to F'$ es un homomorfismo de campos.

En la siguiente proposición recordamos un resultado que ya habíamos visto en la sección 1.6.

Todo homomorfismo de campos es inyectivo

Proposición 1

Supongamos que F y F' son campos. Si $\phi : F \to F'$ es un homomorfismo de campos, entonces ϕ es inyectivo.

Veamos que $\ker \varphi = 0$.

$$\begin{aligned} x \in \ker \varphi &\iff \varphi(x) = 0 \\ &\implies x \text{ no es invertible} \\ &\iff x = 0 && \text{(pues } F \text{ es campo)} \end{aligned}$$

$\square$

Extensiones de campos

Definición

Si K es un campo y F es un subcampo de K, entonces decimos (i) que K **es una extensión de** F, o (ii) que K/F **es una extensión de campos**, o (iii) escribimos el siguiente diagrama

$$\begin{array}{c} K \\ | \\ F \end{array}$$

En este caso, también decimos que F es el **campo base** de la extensión K/F.

Cabe recalcar que la notación "K/F" no es un cociente.

Observación

Notemos que dada una extensión de campos K/F, podemos considerar a K como espacio vectorial sobre F con la multiplicación por escalares $\cdot : F \times K \to K$ dada por

$$\alpha \cdot v = \alpha \times_K v \text{ para toda } \alpha \in F \text{ y } v \in K.$$

En otras palabras, la multiplicación por escalares es la restricción de $\times_K$ a $F \times K$. Específicamente,

$$\cdot := \times_K \restriction_{F \times K} .$$

De esta manera, $(K, +_K, F, \cdot)$ es un espacio vectorial.

Naturalmente, en lo que sigue trabajaremos con conjuntos generadores y de conjuntos de vectores linealmente independientes - conceptos que están definidos en términos de combinaciones lineales. Cuando hagamos esto, hay que tener cuidado de que los coeficientes de nuestras combinaciones lineales sean elementos de F. Específicamente, las combinaciones lineales que nosotros estamos considerando (pues estamos trabajando en el espacio vectorial K sobre F) son de la forma

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$$

con $\alpha_1, \alpha_2, \ldots, \alpha_n \in F$ y $v_1, v_2, \ldots, v_n \in K$.

Con esto en mente, introducimos la siguiente definición.

El grado de una extensión de campos

Definición

Supongamos que K/F es una extensión de campos. Definimos el **grado de la extensión** K/F como la dimensión de K como espacio vectorial sobre F. En otras palabras, si denotamos el grado de la extensión K/F por $[K : F]$, entonces

$$[K : F] \coloneqq \dim_F K.$$

Si $[K : F] < \infty$, decimos que la extensión K/F es finita; y si $[K : F] = \infty$, decimos que la extensión K/F es infinita.

$[K : F] = [K' : F]$ si $K \cong K'$

Proposición 2

Supongamos que K/F y K'/F son extensiones de campos. Si $K \cong K'$, entonces $[K : F] = [K' : F]$.

Demostración. Supongamos que $\varphi : F \to F'$ es un isomorfismo. Es fácil verificar que si $\{v_1, \ldots, v_n\}$ es una base de K sobre F, entonces $\{\varphi(v_1), \ldots, \varphi(v_n)\}$ es una base de K' sobre F. □

Alternativamente, si el lector esta familiarizado con funciones lineales, isomorfismos de espacios vectoriales, y la equivalencia

$$V \text{ y } W \text{ son isomorfos como espacios vectoriales} \iff \dim V = \dim W,$$

entonces el lector puede demostrar que φ también es un isomorfismo entre espacios vectoriales. Cabe recalcar que esto es consecuencia de la definición de multiplicación por escalares que estamos considerando en K y K'.

$[L : F] = [L : K][K : F]$

Teorema 3

Supongamos que F, K, L son campos tales que $F \subset K \subset L$. Si L/K y K/F son extensiones finitas, entonces

$$[L : F] = [L : K][K : F]$$

Si L/F es una extensión infinita o K/F es una extensión infinita, entonces L/K también es una extensión infinita.

Demostración. Supongamos que $[L : K] = m < \infty$ y $[K : F] = n < \infty$. Mas aun, supongamos que

$$\begin{aligned} &\{w_1, \ldots, w_m\} \text{ es una } K\text{-base de } L \quad \text{ y} \\ &\{v_1, \ldots, v_n\} \text{ es una } F\text{-base de } K. \end{aligned}$$

Veamos que el conjunto de los productos por pares de estas bases forma una F-base de L. Específicamente, veamos que

$$\mathcal{B} \coloneqq \left\{ v_i w_j \mid i \in \{1, \ldots, n\} \text{ y } j \in \{1, \ldots, m\} \right\}$$

es una F-base de L. Esto es suficiente porque de esta manera,

$$[L : F] = |\mathcal{B}| = mn = [L : K][K : F].$$

Primero veamos que $\mathcal{B}$ es un F-conjunto generador de L. Para esto, supongamos que $a \in L$. Como $\{w_1, \ldots, w_m\}$ es una K-base de L, entonces podemos escribir

$$a = \beta_1 w_1 + \cdots + \beta_m w_m \tag{1}$$

para algunas $\beta_1, \ldots, \beta_m \in K$. Mas aun, como $\{v_1, \ldots, v_n\}$ es una F-base de K, entonces para cada $j \in \{1, \ldots, m\}$ podemos escribir

$$\beta_j = \alpha_{1,j} v_1 + \cdots + \alpha_{n,j} v_n$$

para algunas $\alpha_{1,j}, \ldots, \alpha_{n,j} \in F$. Sustituyendo cada una de estas expresiones en (1) obtenemos

$$\begin{aligned} a &= \big(\alpha_{1,1} v_1 + \cdots + \alpha_{n,1} v_n\big)\, w_1 + \cdots + \big(\alpha_{1,m} v_1 + \cdots + \alpha_{n,m} v_n\big)\, w_m \\ &= \alpha_{1,1} v_1 w_1 + \cdots + \alpha_{n,1} v_n w_1 + \cdots + \alpha_{1,m} v_1 w_m + \cdots + \alpha_{n,m} v_n w_m \\ &\in \operatorname{span}_F(\mathcal{B}). \end{aligned}$$

Por lo tanto, $\operatorname{span}_F(\mathcal{B}) = L$ y $\mathcal{B}$ es un F-conjunto generador de L.

Ahora, veamos que $\mathcal{B}$ es un conjunto de vectores F-linealmente independientes: Para esto, necesitamos ver que si una F-combinación lineal de todos los elementos de $\mathcal{B}$ es igual a 0, entonces todos los coeficientes de esta combinación lineal son 0. Por eso, supongamos que

$$0 = \sum_{\substack{i=1,\ldots,n \\ j=1,\ldots,m}} \lambda_{i,j} v_i w_j. \tag{2}$$

para algunos $\lambda_{i,j} \in F$ con $i \in \{1, \ldots, n\}$ y $j \in \{1, \ldots, m\}$ y veamos que $\lambda_{i,j} = 0$ para toda i, j.

Reordenando el lado derecho de (2) podemos escribir

$$\begin{aligned} 0 = \sum_{j=1,\ldots,m} \left(\sum_{i=1,\ldots,n} \lambda_{i,j} v_i w_j \right) &= \sum_{j=1,\ldots,m} \left(\sum_{i=1,\ldots,n} \lambda_{i,j} v_i \right) w_j \\ &= \left(\sum_{i=1,\ldots,n} \lambda i, 1 v_i \right) w_1 + \cdots + \left(\sum_{i=1,\ldots,n} \lambda i, 1 v_i \right) w_m. \end{aligned} \tag{3}$$

Como para cada $j \in \{1, \ldots, m\}$ tenemos

$$\sum_{i=1,\ldots,n} \lambda i, j v_i = \lambda_{1,j} v_1 + \cdots + \lambda_{n,j} v_n \in K,$$

entonces la ultima expresión en (3) en realidad es una K-combinación lineal de $w_1, \ldots, w_m$. Como $w_1, \ldots, w_m$ son K-linealmente independientes, (3) implica que

$$\sum_{i=1,\ldots,n} \lambda i, j v_i = \lambda_{1,j} v_1 + \cdots + \lambda_{n,j} v_n = 0$$

para cada $j \in \{1, \ldots, n\}$. Mas aun, como (i) $\lambda_{i,j} \in F$ para cada i, j y (ii) $v_1, \ldots, v_n$ son F-linealmente independientes, la ecuación anterior implica que $\lambda_{i,j} = 0$ para toda $i \in \{1, \ldots, n\}$. Como esto es cierto para cada $j \in \{1, \ldots, m\}$, obtenemos lo deseado.

$\square$

$[L : K] = \infty$ o $[K : F] = \infty \implies [L : F] = \infty$

Proposición 4

Supongamos que F, K, L son campos tales que $F \subset K \subset L$. Si $[L : K] = \infty$ o $[K : F] = \infty$, entonces $[L : F] = \infty$.

De esta manera, podemos ambiguamente[1] decir que la igualdad

$$[L : F] = [L : K][K : F]$$

también se cumple en el caso infinito. Mas precisamente, si un lado de la ecuación es infinito, entonces el otro también.

[1] Los términos $n \cdot \infty$ o $\infty \cdot \infty$ se precisan en teoría de conjuntos.

Demostración. Antes de empezar, recordemos que en el corolario 2.2.8 demostramos que un espacio vectorial es infinito dimensional si y solo si contiene un conjunto infinito de vectores linealmente independientes. Con esto en mente, procedamos.

Supongamos que $[K : F] = \infty$. Por el corolario 2.2.8, existe un conjunto infinito de elementos de K que son F-linealmente independientes. En particular, (como $K \subset L$) existe un conjunto infinito de elementos de L que son F-linealmente independientes. Por el corolario 2.2.8 esto es equivalente a que $[L : F] = \infty$.

Supongamos que $[L : K] = \infty$. Por el corolario 2.2.8, existe un conjunto infinito de elementos de L que son K-linealmente independientes. En particular, (como $F \subset K$) también son F-linealmente independientes. Por el corolario 2.2.8 esto es equivalente a que $[L : F] = \infty$.

$\square$