Notas Curso Álgebra Moderna III
Una Introducción a la Teoría de Galois Finita

Cristo Daniel Alvarado

9 de julio de 2024

Índice general

Capítulo 1

Extensiones de Campos

1.1. Fundamentos

Observación 1.1.1
El símbolo $\forall^{\infty}$ significa para casi todo salvo una cantidad finita de elementos.

Definición 1.1.1
Sean E y F campos. Decimos que E/F es una **extensión de campos** si se cumple que $F \subseteq E$. Se denomina como **grado de la extensión** E/F a la dimensión de E como espacio vectorial sobre F, denotado por $[E : F]$, esto es

$$[E : F] = \dim_F(E)$$

Definición 1.1.2
Decimos que una extensión de campos E/F es una **extensión finita**, si $[E : F] < \infty$. En caso contrario, decimos que es una **extensión infinita**, y lo escribimos como $[E : F] = \infty$.

Teorema 1.1.1
Sea $K \subseteq F \subseteq E$ una torre de campos (también llamada cadena de campos). Entonces,

$$[E : K] = [E : F] \cdot [F : K]$$

Demostración:
Sea $\{\alpha_i\}_{i\in I}$ y $\{\beta_j\}_{j\in J}$ bases de F sobre K y E sobre F, respectivamente.

$$\begin{array}{l} E \\ \ \mid \leftarrow \{\beta_j\}_{j\in J} \\ F \\ \ \mid \leftarrow \{\alpha_i\}_{i\in I} \\ K \end{array}$$

Afirmamos que $\{\alpha_i\beta_j\}_{(i,j)\in I\times J}$ es base de E sobre K. En efecto, claramente $\alpha_i\beta_j \in E$ para todo $(i,j) \in I \times J$. Notemos que necesariamente

$$\left|\left\{\alpha_i \middle| i \in I\right\}\right| = |I| \quad \text{y} \quad \left|\left\{\beta_j \middle| j \in J\right\}\right| = |J|$$

por ser ambas bases. Sea $u \in E$, entonces u se expresa de forma única como combinación lineal de elementos de la base $\{\beta_j\}_{j\in J}$ con coeficientes en F, digamos

$$u = \sum_{j\in J} f_j \beta_j$$

donde $f_j \in F$ para todo $j \in J$ y $f_j = 0 \; \forall\!\!\!\!\frown j \in J$. Por otro lado, cada $f_j \in F$ se expresa de forma única como una combinación lineal de elementos de la base $\{\alpha_i\}_{i\in I}$ sobre K:

$$f_j = \sum_{i\in I} k_{i,j} \alpha_i$$

donde $k_{i,j} \in K$ para todo $i \in I$ siendo $k_{i,j} = 0 \; \forall\!\!\!\!\frown i \in I$, para cada $j \in J$. Luego,

$$\begin{aligned} u &= \sum_{j\in J} f_j \beta_j \\ &= \sum_{j\in J} \left(\sum_{i\in I} k_{i,j} \alpha_i \right) \beta_j \\ &= \sum_{(i,j)\in I\times J} k_{i,j} \alpha_i \beta_j \end{aligned}$$

donde $k_{i,j} \in K$ y $k_{i,j} = 0 \; \forall\!\!\!\!\frown (i,j) \in I \times J$. Luego

$$E = \mathcal{L}\left(\left\{ \alpha_i \beta_j \middle| (i,j) \in I \times J \right\} \right)$$

Probemos que $\{\alpha_i\beta_j\}_{(i,j)\in I\times J}$ es l.i. sobre K. En efecto, sean $a_{i,j} \in F$ tales que

$$\sum_{(i,j)\in I\times J} a_{i,j} \alpha_i \beta_j = 0$$

entonces,

$$\begin{aligned} &\sum_{(i,j)\in I\times J} a_{i,j} \alpha_i \beta_j = 0 \\ \Rightarrow &\sum_{j\in J} \left(\sum_{i\in I} a_{i,j} \alpha_i \right) \beta_j = 0 \end{aligned}$$

como $\{\beta_j\}_{j\in J}$ es base de E sobre F, entonces

$$\sum_{i\in I} a_{i,j} \alpha_i = 0 \quad \forall j \in J$$

y, como $\{\alpha_i\}_{i\in I}$ es base de F sobre K, se tiene que

$$a_{i,j} = 0 \quad \forall (i,j) \in I \times J$$

Así, $\{\alpha_i\beta_j\}_{(i,j)\in I\times J}$ es l.i. sobre K, y

$$\left| \left\{ \alpha_i \beta_j \middle| (i,j) \in I \times J \right\} \right| = |I \times J| = |I|\,|J|$$

por ende, $[E : K] = [E : F][F : K]$. ∎

Ejemplo 1.1.1
Sean $p, q \in \mathbb{N}$ números primos diferentes. Podemos suponer que $p < q$. Definimos

$$E = \mathbb{Q}(\sqrt{p})$$

Proposición 1.1.1
Sean $p_1, ..., p_n \in \mathbb{N}$ primos distintos tales que $p_i < p_{i+1}$ para todo $i \in [\![1, n-1]\!]$. Definimos por recursión $E_0 = \mathbb{Q}$ y

$$E_i = E_{i-1}(\sqrt{p_i}), \quad \forall i \in [\![1, n]\!]$$

Entonces, $E_0 \subseteq E_1 \subseteq ... \subseteq E_n$ es una torre de campos tal que la extensión E_i/E_{i-1} tiene una base $\left\{1, \sqrt{p_i}\right\}$ para todo $i \in [\![1, n]\!]$. En particular,

$$[E_n : E_0] = 2^n$$

Demostración:

■

1.2. Construcciones

Observación 1.2.1
Sea E un campo y $S \subseteq E$ un subconjunto de E no vacío. Denotamos por $\mathcal{F}$ al conjunto de subcampos (respectivamente, $\mathcal{A}$ al de subanillos) que contienen a S no triviales (es decir, que al menos contienen al 0 y 1). Se sabe que

$$\bigcap \mathcal{F} \quad \text{y} \quad \bigcap \mathcal{A}$$

son un campo y un anillo, respectivamente, contenidos en E. Ambos los denotamos por (S) y $[S]$, respectivamente.

Definición 1.2.1
En la observación (S) es el mínimo subcampo de E que contiene a S, llamado **subcampo generado por** S y, $[S]$ es el mínimo subanillo de E que contiene a S, llamado **subanillo generado por** S.

Al conjunto S se le llama **conjunto de generadores de** (S) **ó** $[S]$.

En el caso que $S = \emptyset$, denominamos como **campo primo de** E a $(S) = (\emptyset)$ denotado por P_E.

Observación 1.2.2
En general, $S \neq \emptyset$. Si $S \subseteq E$ y K es subcampo de E, entonces denotamos por $K(S)$ (resp. $K[S]$) a $(K \bigcup S)$ (resp. $[K \cup S]$). Si K y L son subcampos de E, entonces $(L \cup K)$ (resp. $[L \cup K]$) es denotado por $KL = K(L) = LK = L(K)$ (resp. $K[L] = L[K]$). KL es llamado **el compuesto de** K **y** L.

En el caso que S sea subconjunto finito de E con $S = \{u_1, ..., u_n\}$ escribimos:

$$K(u_1, ..., u_n) = K(\{u_1, ..., u_n\})$$

Definición 1.2.2
Sea E/K una extensión de campos. Decimos que E/K es **finitamente generada** si existen $u_1, ..., u_n \in E$ tales que $E = K(u_1, ..., u_n)$.