Álgebra III

Foto: José Juan Castro

Los Del DGIIM, losdeldgiim.github.io

Doble Grado en Ingeniería Informática y Matemáticas
Universidad de Granada

Álgebra III

Los Del DGIIM, `losdeldgiim.github.io`

José Juan Urrutia Milán

Granada, 2025

Índice general

1. Extensiones de cuerpos y raíces de polinomios

¿Qué es un cuerpo (o field, campo)? Es un tipo de anillo conmutativo.¿Qué es un anillo?

Definición 1.1 (Anillo)**.** Un anillo es un conjunto no vacío A que tiene definidas dos operaciones binarias, $+ : A \times A \to A$, que tendrá un elemento destacado, denotado por 0; y $\cdot : A \times A \to A$, que tiene un elemento destacado, denotado por 1. Abreviando:

$$(A, +, 0, \cdot, 1)$$

A con $+$ es un grupo aditivo conmutativo con elemento neutro 0. A con $\cdot$ A es un monoide, es decir, una operación binaria asociativa, que no tiene por qué ser conmutativa.

Para completar el anillo hacen falta las leyes distributivas:

$$a \cdot (b + c) = a \cdot b + a \cdot c \qquad \forall a, b, c \in A$$

Y como no exigimos conmutatividad:

$$(a + b) \cdot c = a \cdot c + b \cdot c \qquad \forall a, b, c \in A$$

Definición 1.2 (Cuerpo)**.** Un cuerpo es un anillo A al que se le pide además $A \setminus \{0\}$ es un grupo, es decir, $\forall a \in A \setminus \{0\}$ $\exists a^{-1} \in A$ de forma que $a \cdot a^{-1} = 1$, de donde $0 \neq 1$.

Definición 1.3 (Cuerpo)**.** Es un anillo conmutativo A de forma que $A \setminus \{0\}$ es un grupo.

Ejemplo. Algunos ejemplos de los cuerpos más famosos son:

- $\mathbb{Q}$.
- $\mathbb{R}$.
- $\mathbb{C}$.
- $\mathbb{Z}_p$ con p primo.

Definición 1.4 (Subanillo)**.** Sea A un anillo y $B \subseteq A$, B es un subanillo de A si:

- $1 \in B$.

- $(B, +)$ es un subgrupo de $(A, +)$.
- $a, b \in B \Longrightarrow ab \in B$.

Ejemplo. Por ejemplo, $\mathbb{Z}$ no tiene subanillos propios.

- $\mathbb{Z}$ es subanillo de $\mathbb{Q}$.
- $\mathbb{Q}$ es subanillo de $\mathbb{R}$.
- $\mathbb{R}$ es subanillo de $\mathbb{C}$.
- $\mathbb{Z}_p$ no puede ser subanillo de $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, ya que tiene característica p.

Definición 1.5 (Homomorfismo de anillos)**.** Sean A, B anillos, un homomorfismo de anillos es una aplicación$f : A \to B$ que verifica:

- $f(1) = 1$.
- $f(a + b) = f(a) + f(b)$ (homomorfismo de grupos).
- $f(ab) = f(a)f(b)$ (homomorfismo de monoides).

Definición 1.6 (Característica de un anillo)**.** Sea A un anillo, existe un único homomorfismo de anillos

$$\chi : \mathbb{Z} \to A$$

Ya que:

$$\chi(n) = \sum_{k=1}^{n} \chi(1) = \sum_{k=1}^{n} 1_A \qquad \forall n \in \mathbb{N} \setminus \{0\}$$

Además, $\ker \chi$ es un ideal en $\mathbb{Z}$, y todos los ideales de $\mathbb{Z}$ eran principales, es decir, de la forma $n\mathbb{Z}$ para cierto $n \in \mathbb{N}$. La característica de A es $\ker \chi$.

Definición 1.7 (Subcuerpo)**.** Si K es un cuerpo, un subcuerpo de K es un subanillo F de K tal que F es un cuerpo (es decir, que F es cerrado para los inversos de cada elemento no nulo de K).

1.0.1. Cuerpos primos

Sea K un cuerpo y Γ un conjunto no vacío (ya que el propio cuerpo siempre es un subcuerpo del mismo) de subcuerpos de K. Es fácil ver que:

$$\bigcap_{F \in \Gamma} F \text{ es un subcuerpo de } K$$

Sea ahora $S \subseteq K$ un subconjunto de un cuerpo K (nada impide que $S \neq \emptyset$), tomamos como Γ el conjunto de los subcuerpos de K que contienen a S. Para dicho Γ, consideramos:

$$\bigcap_{F \in \Gamma} F$$

Obtenemos el subcuerpo más pequeño de K que contiene a S.

Observemos que si $S = \emptyset$, obtenemos el menor subcuerpo de K. Llamaremos a dicho cuerpo "subcuerpo primo de K".
El primer Teorema de Isomorfismo nos dice ($\leqslant$ para subanillo):

$$\frac{\mathbb{Z}}{p\mathbb{Z}} = \frac{\mathbb{Z}}{\ker \chi} \cong Im\chi \leqslant K$$

Y $\mathbb{Z}/p\mathbb{Z}$ es un dominio de integridad cuando p es 0 o primo. (En un dominio en el que todos los ideales son principales, los ideales que dan como cociente un dominio de integridad son el 0 o uno que automáticamente es un cuerpo).

Proposición 1.1. *Sea K un cuerpo de característica p, entonces si $p > 0$, el subcuerpo primo de K es isomorfo a $\mathbb{Z}_p$, y si $p = 0$, el subcuerpo primo de K es isomorfo a $\mathbb{Q}$.*

Demostración. Sea Π el subcuerpo primo de K:

- Si $p > 0$, $Im\chi$ es un subcuerpo de K, ya que:

$$\frac{\mathbb{Z}}{p\mathbb{Z}} = \frac{\mathbb{Z}}{\ker \chi} \cong Im\chi \leqslant K$$

Por tanto, como Π es el menor subcuerpo de K, tenemos que $\Pi \subseteq Im\chi \cong \mathbb{Z}_p$, y como $\mathbb{Z}_p$ no contiene subcuerpo más que él mismo, tenemos que $\Pi = Im\chi \cong \mathbb{Z}_p$.

- Si $p = 0$, entonces $\mathbb{Z} \cong Im\chi \leqslant K$, como cualquier subanillo contiene a $Im\chi$, tenemos que $Im\chi \subseteq \Pi$.
Si Q es el cuerpo de fracciones de $Im\chi$, como $Im\chi \cong \mathbb{Z}$, tendremos que $Q \cong \mathbb{Q}$.
Por la propiedad universal del cuerpo de fracciones, podemos meter una copia isomorfa del cuerpo de fracciones dentro de Π: $Q \subseteq \Pi$, y como Π es el subcuerpo más chico de K y Q es un cuerpo, $\Pi = Q$.

□

Definición 1.8 (Extensión de cuerpos)**.** Sea F subcuerpo de un cuerpo K, diremos que K es una extensión de cuerpos de F, notado por $F \leqslant K$ (esta notación se reservará para esto próximamente).

Observación. Si $F \leqslant K$ es una extensión, entonces K es un espacio vectorial sobre F.

- $(K, +)$ es un grupo aditivo.
- Si $\lambda \in F$ y $\alpha \in K$, $\lambda\alpha$ es el producto que ya conocemos de K.

Definición 1.9. Si $F \leqslant K$ es una extensión, la dimensión de K sobre F como espacio vectorial recibe el nombre de "grado de la extensión $F \leqslant K$", denotado por $[K : F]$.

Ejemplo. Como ejemplo a destacar:

- $\mathbb{R} \leqslant \mathbb{C}$ tiene grado de extensión 2.
- $[\mathbb{R} : \mathbb{Q}]$.

Si $[\mathbb{R} : \mathbb{Q}]$ fuese finito e igual a n, entonces $\mathbb{R} \cong \mathbb{Q}^n$; por lo que $[\mathbb{R} : \mathbb{Q}] = \infty$, ya que $\mathbb{R}$ no es numerable.

Notación. Si la extensión de un cuerpo no es finita, diremos que es infinita.

Ejercicio 1. Demostrar que el cardinal de un cuerpo finito es de la forma p^n, con p primo y $n \geqslant 1$. (algebra lineal)

Como es finito, el primo es de la forma $\mathbb{Z}_p$, luego es un espacio vectorial de dimensión finita n sobre $\mathbb{Z}_p$, isomorfo como espacio vectorial a $\mathbb{Z}_p \times \ldots \times \mathbb{Z}_p$ n veces, luego de cardinal p^n.

Haremos una clasificacion de cuerpos finitos, cada n$^{\underline{o}}$ primo y numero natural no nulo, existe un cuerpo de p^n elementos y todos ellos serán isomorfos entre sí.

Notación. Sea $F \leqslant K$ extensión, $S \subseteq K$, el menor subcuerpo de K que contiene a $F \cup S$ lo denoto por $F(S)$, que recibe el nombre de "extensión de F generada por S".

Si $S = \{s_1, \ldots, s_t\}$, simplifico la notación como $F(s_1, \ldots, s_t)$.

Ejemplo. $\mathbb{Q}(\sqrt{2})$ es el menor subcuerpo de $\mathbb{R}$ que contiene a $\sqrt{2}$, que puede calcularse:

$$\mathbb{Q}(\sqrt{2}) = \left\{ a + b\sqrt{2} : a, b \in \mathbb{Q} \right\}$$

Demostración. Veámoslo:

$\supseteq$) Si tomo $a + b\sqrt{2}$, tomo 3 elementos de dicho cuerpo y se quedan dentro del cuerpo.

$\subseteq$) Si demuestro que dicho subconjunto es un cuerpo, tengo inmediatamente la igualdad, por ser el menor subcuerpo que contiene a $\sqrt{2}$. Que es subanillo se ve facil, para ver que es subcuerpo, se imita lo que pasa con los numeros complejos: dado $a + b\sqrt{2}$, lo multiplicamos por su conjugado, que es distinto de cero y luego lo ponemos en el denominador, usando que $\sqrt{2}$ no es racional, luego denominador no nulo.

□

Observemos que tenemos $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.