Universidad de Granada

Doble Grado en Ingeniería Informática y Matemáticas

Álgebra III

Autor:
Jesús Muñoz Velasco

Curso 2025-2026

Índice general

Introducción

Comenzaremos la introducción al contenido de esta asignatura recordando brevemente el concepto de cuerpo[1]. Lo primero que sabemos es que un cuerpo es un tipo de anillo conmutativo. Un anillo[2] es un conjunto no vacío, A que tiene definidas dos aplicaciones binarias y dos elementos especiales, $(A, +, 0, \cdot, 1)$. Con $(+, 0)$ tenemos que A es un grupo aditivo y con $(\cdot, 1)$ tenemos que A es un monoide, es decir, que cuenta con una aplicación asociativa con elemento neutro 1. Además estas 2 operaciones tienen que guardar una cierta compatibilidad (axiomas), que llamamos leyes distributivas y que son los siguientes:

- •) $a \cdot (b + c) = a \cdot b + a \cdot c$
- •) $(b + c) \cdot a = b \cdot a + c \cdot a, \quad \forall a, b \in A$

Con esto habremos completado la definición de anillo. La conmutatividad hace referencia a la siguiente propiedad:

$$a \cdot b = b \cdot a \ \ \forall a, b \in A$$

Veamos ahora qué tiene que suceder para que a este anillo conmutativo lo llamemos cuerpo. Para ello, es equivalente decir que $A \setminus \{0\}$ es un grupo y que $\forall a \in A \setminus \{0\}$ existe un $a^{-1} \in A \setminus \{0\}$ tal que $a \cdot a^{-1} = 1$ (lo cual implica claramente $0 \neq 1$).

Ejemplo.

- •) Los racionales, $\mathbb{Q}$.
- •) Los reales, $\mathbb{R}$.
- •) Los complejos, $\mathcal{C}$.
- •) $\mathbb{Z}_p$ con p primo.

Notación. Denotaremos el producto de 2 elementos por yuxtaposición[3], es decir, $a \cdot b = ab$

Recordaremos ahora los conceptos de subanillo y subcuerpo. Para ello consideramos A un anillo y un subconjunto $B \subseteq A$ tal que $1 \in B$. Si además tenemos que $(B, +)$ es un subgrupo de $(A, +)$ y que para todo $a, b \in B$ se tiene que $ab \in B$, entonces diremos que B es un subanillo de A.

---

[1] *field* en inglés

[2] *ring* en inglés

[3] Las matemáticas son el arte de ser ambiguo siendo preciso en cada instante (Torrecillas, 18-9-2025)

Ejemplo.

- •) $\mathbb{Z}$ es subanillo de $\mathbb{Q}$.
- •) $\mathbb{Q}$ es subanillo de $\mathbb{R}$.
- •) $\mathbb{R}$ es subanillo de $\mathbb{C}$

Definición 0.1 (Homomorfismo de anillos)**.** Dados A y B dos anillos, un **homomorfismo** $f : A \to B$ es una aplicación que verifica para todo $a, b \in A$ las siguientes propiedades:

- •) $f(1) = 1$
- •) $f(a + b) = f(a) + f(b)$
- •) $f(ab) = f(a)f(b)$

Definición 0.2 (Característica de un anillo)**.** Dado A un anillo, existe un único homomorfismo de anillos[4] $\chi : \mathbb{Z} \to A$. Entonces $\ker \chi$ es un ideal de $\mathbb{Z}$ y por tanto será principal, es decir, que $\ker \chi = n\mathbb{Z}$ para cierto $n \in \mathbb{N}$. Dicho n es el número al que llamaremos **característica** de A y la notaremos como $n = car(A)$.

Definición 0.3 (Subanillo)**.** Si K es un cuerpo, entonces un subcuerpo de K es un **subanillo** F de K tal que F es un cuerpo.

Observación. Sea K un cuerpo y Γ un conjunto no vacío[5] de subcuerpos de K. Entonces $\bigcap_{F \in \Gamma} F$ es un subcuerpo de K.

Definición 0.4 (Subcuerpo primo)**.** Sea K un cuerpo y tomamos $S \subset K$ un subconjunto y consideramos

$$\Gamma = \{ \text{ subcuerpos de } K \text{ que contienen a } S\}$$

En Γ podemos tomar la intersección, $\bigcap_{F \in \Gamma} F$ que es el subgrupo más pequeño que contiene a S. Para $S = \emptyset$ obtengo el menor subcuerpo de K y a este subcuerpo lo llamaremos **subcuerpo primo** de K.

Observación. Si tenemos $\chi : \mathbb{Z} \to K$ el homomorfismo de anillos, de forma que p es la característica de K, es decir, $p\mathbb{Z} = \ker \chi$. Entonces por el primer teorema de isomorfía tenemos que

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

Donde la última inclusión es de subanillo. Como $Im\chi$ es un dominio de integridad tendremos que $p = 0$ o, si $p > 0$, entonces p es primo.

Proposición 0.1. Sea K un cuerpo de característica p, entonces,

[4] se prueba fácilmente por inducción

[5] El propio K está en este conjunto

- •) si $p > 0$, el subcuerpo primo de K es isomorfo a $\mathbb{Z}_p$
- •) si $p = 0$, el subcuerpo primo de K es isomorfo a $\mathbb{Q}$

Demostración. Denotamos por Π al subcuerpo primo de K.

- •) Si $p > 0$, entonces $Im\chi$ es un subcuerpo de $K \Rightarrow \Pi \subseteq Im\chi$, pero $Im\chi \cong \mathbb{Z}_p$ y como $\mathbb{Z}_p$ no tiene subcuerpos propios, entonces $\Pi = Im\chi \cong \mathbb{Z}_p$
- •) Si $p = 0$, entonces $\mathbb{Z} \cong Im\chi \leqslant K$ (subanillo) y entonces $Im\chi \subseteq \Pi$, ya que $Im\chi$ es el subanillo más pequeño. Si Q es el cuerpo de funciones de $Im\chi$, entonces $Q \cong \mathbb{Q}$. Aplicando la propiedad universal del cuerpo de fracciones tenemos que $\mathbb{Q} \subseteq \Pi$ por lo que $\mathbb{Q} = \Pi$ por unicidad del cuerpo de fracciones excepto isomorfismos.

□

Definición 0.5 (Extensión de cuerpos)**.** Sea F un subcuerpo de K, diremos que $F \leqslant K$ es una **extensión de cuerpos**.

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

- •) la suma de K es la suma como espacio vectorial
- •) la acción de los escalares, $\lambda \in F$, $\alpha \in K$, $\lambda\alpha$ es el producto en K

Definición 0.6. Sea $\mathbb{R} \leqslant K$ una extensión, entonces la dimensión de K sobre F (como espacio vectorial) se llama **grado** de la extensión $F \leqslant K$ y se denota por $[K : F]$, es decir

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

Ejemplo.

- •) $[\mathbb{C} : \mathbb{R}] = 2$
- •) $[\mathbb{R} : \mathbb{Q}] = \infty$, ya que $\mathbb{R}$ no es numerable

Notación. Si $[K : F] < \infty$ diremos que $F \leqslant K$ es finita. Si $[K : F] = \infty$ diremos que $F \leqslant K$ no es finita o es infinita.

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

Notación. Sea la extensión $F \subseteq K$ y $S \subseteq K$ un subconjunto de K. Podemos considerar el menor subcuerpo de K que contiene a $F \cup S$ y lo denotaremos por $F(S)$ y lo llamaremos **extensión de F generada por S** (dentro de K). Si S es finito, es decir, $S = \{s_1, \dots, s_t\}$ simplifico la notación como $F(\{s_1, \dots, s_t\}) = F(s_1, \dots, s_t)$

Ejemplo. $\mathbb{Q}(\sqrt{(2)})$ donde $\sqrt{2} \in \mathbb{R}$, es decir, es el menor subcuerpo de los reales que contiene a $\sqrt{2}$. Por tanto $\mathbb{Q}(\sqrt{(2)}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$. Esto se ve fácilmente viendo la doble inclusión. La inclución $\supseteq$ es obvia y demostrando que $\{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ es un subcuerpo tenemos automáticamente la igualdad. Esta extensión tendrá grado 2.

Definición 0.7. Sea K un cuerpo, consideramos el cuerpo de polinomios con coeficientes en K, y lo denotamos por $K[x]$.

Dado un $f \in K[x]$ y $K \leqslant E$ una extensión de cuerpos tal que f se descompone completamente en $E[X]$ como producto de polinomios lineales[6] y $E = K(\alpha_1, \dots, \alpha_t)$ con $\alpha_1, \dots, \alpha_t \in E$ las raíces de f, entonces diremos que E es un **cuerpo de descomposición** (de escisión) de f (sobre K).

Ejemplo. Consideramos el polinomio $x^2 + 1 \in \mathbb{R}[x]$ que es irreducible[7] sobre $\mathbb{R}$. Un cuerpo de descomposición suyo es $\mathbb{C}$.

Podemos considerar además $x^2 + 1 \in \mathbb{Q}[x]$ y entonces el c.d.d[8] es $\mathbb{Q}(i)$ (y además $[\mathbb{C} : \mathbb{Q}(i)] = \infty$ y se deja esto como ejercicio).

$$x^2 + 1 = (x - i)(x + i)$$

Observación. Si $f \in Q[x]$, entonces tomo[9] todas sus raíces en $\mathbb{C}$, digamos $\alpha_1, \dots, \alpha_t$ y c.d.d de f es $Q(\alpha_1, \dots, \alpha_t)$

Ejemplo. Dado $f \in \mathbb{Q}[x]$, $f = x^2 - 2$, entonces el c.d.d de f es $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\{\sqrt{2}\})$

Ejercicio 2. Si tengo $F \leqslant K$ una extensión de cuerpos y dos subconjuntos $S, T \subset K$, demostrar que $F(S \cup T) = F(S)(T)$

Ejemplo. Consideramos el polinomio $f = x^3 - 2 \in \mathbb{Q}[X]$. El conjunto de raíces de f será

$$\text{Raíces de } f = \{\sqrt[3]{2}, w\sqrt[3]{2}, w^2\sqrt[3]{2}\}$$
$$w = e^{\frac{2\pi i}{3}} = \cos\left(\frac{2\pi}{3}\right) + i \operatorname{sen}\left(\frac{2\pi}{3}\right) = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$$
$$(\sqrt[3]{2}w)^3 = 2 \Rightarrow \sqrt[3]{2}w \in \text{Raíces de } f$$

En este caso decimos que el c.d.d de f es $\mathbb{Q}(\sqrt[3]{2}, w\sqrt[3]{2}, w^2\sqrt[3]{2})$, o lo que es lo mismo[10] $\mathbb{Q}(\sqrt[3]{2}, w)$

Ejercicio 3. (Solo hay que plantearse la pregunta, en eso consiste el ejercicio) ¿Quién es el c.d.d de $x^2 + x + 1 \in \mathbb{Z}_2[x]$?¿Existe?

Ejemplo. $f = x^n - 1$ con $n \geqslant 1$. Sabemos que tiene n raíces ya que $f = nx^{n-1}$ por lo que no puede haber raíces con multiplicidad mayor que 1 y por tanto hay n raíces distintas en $\mathbb{C}$. Además, sus raíces son

$$\left\{\left(e^{\frac{i2\pi}{n}}\right)^k : k = 0, \dots, n-1\right\}$$

[6]de grado 1

[7]no tiene raíces en $\mathbb{R}$ y no se puede descomponer en producto de polinomios de grado menor

[8]cuerpo de descomposición

[9]alpicando el Teorema Fundamental del Álgebra

[10]se puede comprobar fácilmente viendo que el conjunto de generadores de un espacio está en el otro y viceversa

que son las raíces n-ésimas de la unidad real. Esto es un subgrupo cíclico de orden n de $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$, con $e^{\frac{i2\pi}{n}}$ como generador. Cada uno de sus generadores se llama raíz n-ésima compleja primitiva de la unidad.

El c.d.d de $x^n - 1 \in \mathbb{Q}[x]$ es $\mathbb{Q}(\eta)$, $\eta \in \mathbb{C}$ que es $\sqrt[n]{1}$ primitiva.

Definición 0.8. Dado $F \leqslant K$ una extensión, $\alpha in K$, diremos que α es **algebraico sobre** F si $f(\alpha) = 0$ para algún $f \in F[x]$, $f \neq 0$. Sino, α se llama **trascendente sobre** F.