



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 cuerpo¹. Lo primero que sabemos es que un cuerpo es un tipo de anillo conmutativo. Un anillo² 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:

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

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, \mathbb{C} .
-) \mathbb{Z}_p con p primo.

Notación. Denotaremos el producto de 2 elementos por yuxtaposición³, 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

³Las 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** $f : A \rightarrow B$ 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 anillos⁴ $\chi : \mathbb{Z} \rightarrow A$. 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 $n = \text{car}(A)$.

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 vacío⁵ 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 $\chi : \mathbb{Z} \rightarrow K$ 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

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

Donde la última inclusión es de subanillo. Como $\text{Im} \chi$ 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,

⁴se prueba fácilmente por inducción

⁵El 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 $\text{Im}\chi$ es un subcuerpo de $K \Rightarrow \Pi \subseteq \text{Im}\chi$, pero $\text{Im}\chi \cong \mathbb{Z}_p$ y como \mathbb{Z}_p no tiene subcuerpos propios, entonces $\Pi = \text{Im}\chi \cong \mathbb{Z}_p$
-) Si $p = 0$, entonces $\mathbb{Z} \cong \text{Im}\chi \leq K$ (subanillo) y entonces $\text{Im}\chi \subseteq \Pi$, ya que $\text{Im}\chi$ es el subanillo más pequeño. Si Q es el cuerpo de funciones de $\text{Im}\chi$, 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 $F \leq K$ es una **extensión de cuerpos**.

Observación. Sea $F \leq K$ 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 $\mathbb{R} \leq K$ una extensión, entonces la dimensión de K sobre F (como espacio vectorial) se llama **grado** de la extensión $F \leq K$ 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 $F \leq K$ es finita. Si $[K : F] = \infty$ diremos que $F \leq K$ 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 $n \geq 1$.

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 inclusión \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 $K \leq E$ una extensión de cuerpos tal que f se descompone completamente en $E[X]$ como producto de polinomios lineales⁶ 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 irreducible⁷ 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.d⁸ 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 $f \in \mathbb{Q}[x]$, entonces tomo todas sus raíces en \mathbb{C} , digamos $\alpha_1, \dots, \alpha_t$ y c.d.d de f es $\mathbb{Q}(\alpha_1, \dots, \alpha_t)$

⁶de grado 1

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

⁸cuerpo de descomposición