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 $\bigcap\limits_{F \in \Gamma} F$ 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, $\bigcap\limits_{F \in \Gamma} F$ 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, $S = \{s_1, \ldots, s_t\}$ simplifico la notación como $F(\{s_1, \ldots, s_t\}) = F(s_1, \ldots, s_t)$

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 $E = K(\alpha_1, \ldots, \alpha_t)$ con $\alpha_1, \ldots, \alpha_t \in E$ 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 $\alpha_1, \ldots, \alpha_t$ y c.d.d de f es $Q(\alpha_1, \ldots, \alpha_t)$

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

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

[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, αinK, 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.

Proposición 0.2. Sea $F \leqslant K$ una extensión de cuerpos, $\alpha \in K$ algebraico sobre F. Entonces existe un único polinomio mónico[11] irreducible[12] $f \in F[X]$ tal que $f(\alpha) = 0$. Además, se tiene un isomorfismo de cuerpos

$$F(\alpha) \cong \frac{F[X]}{\langle f \rangle}$$

y además, $\{1, \alpha, \ldots, \alpha^{\deg f - 1}\}$ es una F-base de $F(\alpha)$. Adí, $[F(\alpha) : F] = \deg f$

Demostración. Tomo $e_\alpha : F[X] \to K$ la aplicación definida por $e_\alpha(y) = g(\alpha)$. Entonces tenemos que e_α es un homomorfismo de anillos. Tomo $\ker e_\alpha$, que es un ideal de $F[X]$ y

$$\exists f \in F[X] \text{ tal que } \ker e_\alpha = \langle f \rangle \text{ mónico}$$

Por el teorema de isomofismo para anillos tenemos que

$$Im\ e_\alpha \cong \frac{F[X]}{\ker e_\alpha} = \frac{F[X]}{\langle f \rangle}$$

Como $Im\ e_\alpha$ es subanillo de K, resulta ser un dominio de integridad por lo que $\frac{F[X]}{\langle f \rangle}$ es un DI. Por tanto f es irreducible y $\frac{F[X]}{\langle f \rangle}$ es un cuerpo.

Veamos ahora la unicidad. Si tomo $h \in F[X]$ irreducible y mónico tal que $h(\alpha) = 0$, entonces $h \in \langle f \rangle$, luego $\langle h \rangle \subseteq \langle f \rangle$ y al ser maximal se tiene que $\langle h \rangle = \langle f \rangle$ y al ser mónicos se tiene $h = f$.

NVeamos el isomorfismo. Sabemos que $Im\ e_\alpha$ es un subcuerpo de K, que $F \leqslant Im\ e_\alpha$ y $\alpha \in Im\ e_\alpha$. Tenemos entonces que $F(\alpha) \leqslant Im\ e_\alpha$. Un elemento de $Im\ e_\alpha$ es de la forma $g(\alpha)$ para $g \in F[X]$. Tendremos que $g(x) = \sum_{i=0}^{n} g_i X^i$, con $g_i \in F$ por lo que $g(\alpha) = \sum_{i=0}^{n} g_i \alpha^i$ luego tenemos el espacio completo y la otra inclusión. Concluimos que $F(\alpha) = Im\ e_\alpha \cong \frac{F[X]}{\langle f \rangle}$.

Finalmente, $\{1, \alpha, \ldots, \alpha^{\deg f - 1}\}$ es F-lineal de $F(\alpha)$ porque $\{1 + \langle f \rangle, X + \langle f \rangle, \ldots, X^{\deg f - 1} + \langle f \rangle\}$ es F-base de $\frac{F[X]}{\langle f \rangle}$ en vista de la división euclidiana. □

[11]el coeficiente director es 1

[12]que no se puede factorizar como producto de polinomios propios

Definición 0.9. El f de la proposición anterior se llama **polinomio irreducible** (o **mínimo**) de α sobre F. Lo notaremos como $f = Irr(\alpha, F)$.

Observación. $Irr(\alpha, F)$ es el mónico de grado mínimo en $F[X]$ del cual α es raíz. Todo otro polinomio $g \in F[X]$ tal que $g(\alpha) = 0$ satisface que $g = h \cdot Irr(\alpha, F)$

Ejemplo.

- •) $Irr(i, \mathbb{Q}) = x^2 + 1 \in \mathbb{Q}[x]$, por lo que $\{1, i\}$ es una $\mathbb{Q} - base$ de $\mathbb{Q}(i)$
- •) $Irr(\sqrt{2}, \mathbb{Q}) = x^2 - 2 \in \mathbb{Q}[x]$
- •) $Irr(e^{\frac{i2\pi}{3}}, \mathbb{Q})$. Sabemos que $e^{\frac{i2\pi}{3}}$ es raíz de $x^3 - 1 \in \mathbb{Q}$, sin embargo no es irreducible ya que $x^3 - 1 = (x-1)(x^2+x+1)$ y como (x^2+x+1) es irreducible (si se calculan las raíces es fácil ver que no están en $\mathbb{Q}$) y $e^{\frac{i2\pi}{3}}$ sigue siendo raíz suya por lo que $Irr(e^{\frac{i2\pi}{3}}, \mathbb{Q}) = (x^2+x+1)$. Una $\mathbb{Q}-$base de $\mathbb{Q}(e^{\frac{i2\pi}{3}})$ es $\{1, e^{\frac{i2\pi}{3}}\}$ y $[\mathbb{Q}(e^{\frac{i2\pi}{3}}), \mathbb{Q}] = 2$.

Lema 0.3 (de la torre)**.** Sean $F \leqslant K \leqslant L$ extensiones. Entonces se tiene que

$$F \leqslant L \text{ es finita} \iff \begin{matrix} F \leqslant K \\ \text{y} \\ K \leqslant L \end{matrix} \quad \text{son finitos}$$

Además, $[L : F] = [L : K][K : F]$.

Demostración.

- ⇒) Supongamos $F \leqslant J$ finito. Encones como K es un F-subespacio vectorial de K entonces $F \leqslant K$ es finita. Si tomo $\{\alpha_1, \ldots, \alpha_t\}$ generados del F-espacio vectorial L, entonces $\{\alpha_1, \ldots, \alpha_t\}$ también es un sistema de generadores del K-subespacio vectorial de L por lo que $K \leqslant L$ es finito.
- ⇐) Sean $\{u_1, \ldots, u_n\}$ base de L sobre K y $\{v_1, \ldots, v_m\}$ base de Ksobre F . Afirmo que $\{u_i v_j : 1 \leqslant i \leqslant n, \;\; 1 \leqslant j \leqslant m\}$ es una F-base de L (rutinario).

□

El nombre de este lema proviene de que cuando se tienen extensiones de cuerpos $F_1 \leqslant F_2 \leqslant \ldots \leqslant F_s$, se suele decir que tenemos una torre de cuerpos. Haciendo una inducción sobre este lema es fácil ver que se puede usar para un número finito de cuerpos (la torre).

Proposición 0.4. Sea $F \leqslant K$ una extensión de cuerpos, $\alpha \in K$. Entonces se tiene

$$\alpha \text{ alegraico sobre } F \iff \exists F \leqslant K \leqslant K \text{ tal que } F \leqslant L \text{ finita y } \alpha \in L$$

Demostración.

- ⇒) Supongamos euqe α es algorítmico en F. Tomo $L = F(\alpha)$ y por la proposición vista anteriormente esto se verifica.

$\Leftarrow$) Sea $\alpha \in L$ con $F \leqslant L$ finito. El lema de la torre afirma que $F \leqslant F(\alpha)$ es finita. En geometría I y álgebra I se estudió que $\{1, \alpha, \alpha^2, \ldots, \alpha^n, \ldots\}$ es F-linealmente dependiente por lo que $\exists m \geqslant 1$ tal que α^m es F-linealmente dependiente de $\{1, \alpha, \ldots, \alpha^{m-1}\}$ por lo que $\alpha^m = \sum_{i=0}^{m-1} a_i \alpha^i$ con $a_i \in F$ por lo que α es algorítmico en F.

□

Definición 0.10. Sea $F \leqslant K$ una extensión de cuerpos, se dice **algebraica** si todo $\alpha \in K$ es algebraico sobre F.

Teorema 0.5. Una extensión $F \leqslant G$ es finita si y solo si es algebraica y finitamente generada.

Demostración.

$\Rightarrow$) Tomo $\{u_1, \ldots, u_t\}$ una F-base de K, por lo que $K = F(u_1, \ldots, u_t)$ (la otra implicación no es cierta en general). Además, si $\alpha \in K$, entonces $F \leqslant F(\alpha)$ y la proposición anterior nos da esta implicación.

$\Leftarrow$) Sea $K = F(\alpha_1, \ldots, \alpha_n)$ y α_i es algebraico sobre F para todo $i \in \{1, \ldots, n\}$. Por el lema de la torre tenemos que $F \leqslant F(\alpha_1) \leqslant \ldots \leqslant F(\alpha_1, \ldots, \alpha_n)$ cada uno es una extensión finita de la anterior, por lo que $F(\alpha_1, \ldots, \alpha_n) \geqslant F$ es finita.

□

Observación. Hemos visto que si $\alpha_1, \ldots, \alpha_n \in K$ y α_1 es algebraico sobre F, α_2 es algebraico sobre $F(\alpha_1)$,..., α_n es algebraico sobre $F(\alpha_1, ..., \alpha_n)$, entonces $[F(\alpha_1, \ldots, \alpha_n) : F] \leqslant \infty$.

Corolario 0.5.1. Sea $F \leqslant K$ una extensión de cuerpos y definimos

$$\Lambda = \text{conjunto de elementos de } K \text{ algebraicos sobre } F$$

entonces Λ es un subcuerpo de K y $F \leqslant \Lambda$ es algebraica

Demostración. Veamos primero que es un anillo. Es claro que $1 \in \Lambda$ y nos queda ver que

$$\alpha, \beta \in \Lambda \Rightarrow \begin{cases} \alpha - \beta \in \Lambda \\ \alpha\beta \in \Lambda \end{cases}$$

Sabemos que $F \leqslant F(\alpha, \beta)$ es algebraica y $\alpha\beta, \alpha - \beta \in F(\alpha, \beta)$. Si $\alpha \neq 0$, entonces $\alpha^{-1} \in F(\alpha)$, luego $\alpha^{-1} \in \Lambda$. □

Notación. Λ se llama **clausura algebraica** de F en K.

Ejemplo. Si pojngo $F = \mathbb{Q}$ y $K = \mathbb{C}$ obtento la llamada clausura algebraica (en $\mathbb{C}$).

Notación. $\overline{\mathbb{Q}}$ sus elementos son los números algebraicos

Ejemplo. $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$ por que $\mathbb{Q}(\sqrt[n]{2}) \leqslant \overline{\mathbb{Q}}$ y $Irr(\sqrt[n]{2}, \mathbb{Q}) = x^n - 2$ ya que por el criterio de Eisenstein[13] se tiene que $x^n - 2$ es irreducible.

[13] si no te acuerdas pues lo recuerdas