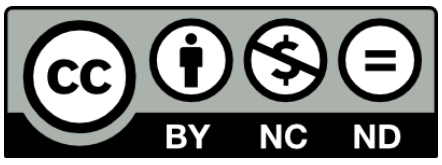
Álgebra III

Los Del DGIIM, losdeldgiim.github.io

Doble Grado en Ingeniería Informática y Matemáticas
Universidad de Granada



Esta obra está bajo una Licencia Creative Commons Atribución-NoComercial-SinDerivadas 4.0 Internacional (CC BY-NC-ND 4.0).

Eres libre de compartir y redistribuir el contenido de esta obra en cualquier medio o formato, siempre y cuando des el crédito adecuado a los autores originales y no persigas fines comerciales.

Álgebra III

Los Del DGIIM, `losdeldgiim.github.io`

José Juan Urrutia Milán

Granada, 2025

Índice general

Antes de proceder con la asignatura de Álgebra III, cuyo principal objetivo es dar solución a las ecuaciones polinómicas mediante el uso y estudio de los cuerpos finitos, recomendamos repasar en anteriores apuntes los siguientes conceptos:

- En los apuntes de Álgebra I los conceptos de: anillo, subanillo, homomorfismo de anillos e ideal.
- En los apuntes de Álgebra II los conceptos de: grupo, subgrupo, homomorfismo de grupos y monoide.

Una vez repasados dichos conceptos, estamos en condiciones de comenzar la asignatura.

1. Extensiones de cuerpos y raíces de polinomios

Comenzamos definiendo el objeto de estudio protagonista a lo largo de esta asignatura: los cuerpos, llamados también campos, del inglés *fields*.

Notación. Aunque las dos operaciones de los anillos (y también de los cuerpos) no tengan por qué ser una suma y una multiplicación, optaremos por dichas notaciones, junto con las notaciones de "cero" para el elemento neutro de la operación "suma" y de "uno" para el elemento neutro de la operación "producto"; por ser familiares a los anillos a los que estamos acostumbrados. De esta forma, para nosotros un anillo será una tupla $(A, +, 0, \cdot, 1)$, a la que podremos referirnos simplemente por A cuando las dos operaciones y elementos neutros estén claros por el contexto.

Definición 1.1 (Cuerpo)**.** Un cuerpo es un anillo A en el que $A \setminus \{0\}$ es un grupo.

Observemos que estamos suponiendo implícitamente que el anillo $\{0\}$ jamás puede ser un cuerpo.

Ejemplo. Algunos ejemplos de los cuerpos más famosos son:

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

Con el objetivo de definir de forma totalmente rigurosa lo que es la característica de un anillo (concepto que puede que se haya mencionado ya en cursos anteriores), nos es necesaria la siguiente proposición:

Proposición 1.1. *Sea A un anillo, existe un único homomorfismo de anillos*

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

Además, $Im\chi$ es el menor subanillo que contiene A.

Demostración. Sean $\chi, \varphi : \mathbb{Z} \to A$ dos homomorfismos de anillos, demostremos por inducción que $\chi(k) = \varphi(k)$ para todo $k \in \mathbb{Z}$:

Para $k = 1$. Como χ y φ son homomorfismos de anillos, estos cumplen

$$\chi(1) = 1 = \varphi(1)$$

Para $k = 0$. De manera análoga, $\chi(0) = 0 = \varphi(0)$.

Supuesto para todo $s \leqslant k$, vemos que:

$$\chi(k+1) = \chi(k) + \chi(1) = \varphi(k) + \varphi(1) = \varphi(k+1)$$
$$\chi(-(k+1)) = -\chi(k+1) = -\varphi(k+1) = \varphi(-(k+1))$$

Acabamos de probar que $\chi = \varphi$, por lo que en caso de existir solo existe un único homomorfismo $\chi : \mathbb{Z} \to A$. Sin embargo, este se puede calcular exigiendo $\chi(1) = 1$.

Ahora, para ver que $Im\chi$ es el menor subanillo que contiene A, sea $S \subseteq A$ otro subanillo de A, como subanillo de A que es ha de contener al 1, al 0 y ser cerrado para sumas y opuestos, luego ha de contener también a $n \cdot 1$ y $-(n \cdot 1)$, para todo $n \in \mathbb{N}$. Sin embargo, tenemos que:

$$Im\chi = \{\chi(n) : n \in \mathbb{Z}\} = \{0\} \cup \left\{\sum_{k=1}^{n} \chi(1) : n \in \mathbb{N}\right\} \cup \left\{\sum_{k=1}^{n} \chi(-1) : n \in \mathbb{N}\right\}$$

Por lo que $Im\chi \subseteq S$. □

Definición 1.2 (Característica de un anillo)**.** Sea A un anillo, sabemos por la Proposición anterior que existe un único homomorfismo de anillos

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

En dicho caso, sabemos de Álgebra I que $\ker \chi$ es un ideal en $\mathbb{Z}$, y como todos los ideales de $\mathbb{Z}$ son principales, sabemos que $\exists n \in \mathbb{N}$ de forma que $\ker \chi = n\mathbb{Z}$. Dicho número n recibe el nombre de "característica de A" (aunque varios números cumplan esta definición, suele tomarse el más pequeño de ellos que sea positivo, en caso de no ser el ideal trivial).

Proposición 1.2. *La característica de un anillo ha de ser un número primo o cero.*

Demostración. Supongamos que A es un anillo de característica $n \neq 0$, por lo que:

$$\sum_{k=1}^{n} 1 = n \cdot 1 = 0$$

Por reducción al absurdo, supongamos que n no es primo, con lo que puedo encontrar un primo p y $m \neq 0$ de forma que:

$$0 = n \cdot 1 = p \cdot m$$

Como $0 \neq m \in A$, existe m^{-1}, que puede multiplicarse a ambos lados de la igualdad, obteniendo que $p = 0$, contradicción, por lo que n ha de ser primo. □

Definición 1.3 (Subcuerpos y extensiones de cuerpos)**.** Si K es un cuerpo, un subcuerpo de K es un subanillo F de K tal que F es un cuerpo. En dicho caso, diremos que K es una extensión del cuerpo F, y se podrá notar por:

$$F \leqslant K$$

1.1. Subcuerpos primos

Es fácil ver que las intersecciones arbitrarias de cuerpos siguen siendo cuerpos, propiedad que justifica el concepto que vamos a introducir.

Definición 1.4 (Subcuerpo generado por un conjunto)**.** Sea K un cuerpo y $S \subseteq K$, si consideramos:

$$\Gamma = \{F \subseteq K : F \leqslant K \text{ y } S \subseteq F\}$$

es decir, el conjunto de todos los subcuerpos de K que contienen a S, definimos el subcuerpo de K generado por S como el subcuerpo:

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

Que se caracteriza por ser el menor subcuerpo de K que contiene a S.

Definición 1.5 (Subcuerpo primo de un cuerpo)**.** Si dado un cuerpo K pensamos en el subcuerpo generado por el conjunto vacío obtenemos el "subcuerpo primo de K", que viene dado por:

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

donde $\Gamma = \{F \subseteq K : F \leqslant K\}$ este es el menor subcuerpo de K.

Proposición 1.3. *Sea K un cuerpo de característica p, entonces el subcuerpo primo de K es isomorfo a:*

- $\mathbb{Z}_p$ *si* $p > 0$.
- $\mathbb{Q}$ *si* $p = 0$.

Demostración. Si consideramos el único homomorfismo $\chi : \mathbb{Z} \to K$, tenemos que $Im\chi$ es el menor subanillo de K, por lo que estará contenido (hágase) en el subcuerpo primo de K, que denotaremos por Π; es decir, $Im\chi \subseteq \Pi$. Aplicando el Primer Teorema de Isomofría sobre χ obtenemos que:

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

Si $p > 0$ tendremos (vimos anteriormente que p debe ser primo):

$$\mathbb{Z}_p = \frac{\mathbb{Z}}{p\mathbb{Z}} \cong Im\chi$$

Por lo que $Im\chi$ es un subcuerpo de K, y como Π es el menor subcuerpo de K, tenemos que $\Pi \subseteq Im\chi$, lo que nos da la igualdad $\Pi = Im\chi \cong \mathbb{Z}_p$.

Si $p = 0$ tendremos entonces $\mathbb{Z} \cong Im\chi$, por lo que los cuerpos de fracciones de $\mathbb{Z}$ y de $Im\chi$ (a quien denotaremos por Q) han de ser isomorfos:

$$\mathbb{Q} \cong Q$$

Como teníamos que $Im\chi \subseteq \Pi$, podemos calcular Q dentro[1] de Π, obteniendo que $Q \subseteq \Pi$, pero como Π es el menor subcuerpo de K, tendremos $\Pi \subseteq Q$, lo que nos da la igualdad $\Pi = Q \cong \mathbb{Q}$.

[1] Si $A \subseteq B$ como subanillo, entonces el cuerpo de fracciones de A está dentro del cuerpo de fracciones de B, pero si B es un cuerpo, coincide con su cuerpo de fracciones.

□

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

Definición 1.6. 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 $[\mathbb{C} : \mathbb{R}] = 2$.
- Si $[\mathbb{R} : \mathbb{Q}] = n$, entonces tendríamos que $\mathbb{R} \cong \mathbb{Q}^n$ como subespacio, por lo que $\mathbb{R}$ no sería numerable. En consecuencia, podemos notar que $[\mathbb{R} : \mathbb{Q}] = \infty$, para notar que no tiene un grado de extensión finito. En estos casos, diremos que el grado de la extensión del cuerpo es infinito.

Ejercicio 1.1.1. Demostrar que el cardinal de un cuerpo finito es de la forma p^n, con p primo y $n \geqslant 1$.

Sea K un cuerpo finito, este no podrá tener característica cero, por lo que existe un primo p de forma que su cuerpo primo sea isomorfo a $\mathbb{Z}_p$. De esta forma, K será un espacio vectorial sobre un cuerpo isomorfo a $\mathbb{Z}_p$, con cierto grado de extensión $n \in \mathbb{N} \setminus \{0\}$, por lo que como espacio vectorial será isomorfo a:

$$\underbrace{\mathbb{Z}_p \times \ldots \times \mathbb{Z}_p}_{n \text{ veces}}$$

Luego K ha de tener cardinal p^n.

Haremos próximamente una clasificacion de cuerpos finitos, en la que cada primo y natural no nulo nos definan un único cuerpo de cardinal p^n.

Definición 1.7. Sea $F \leqslant K$ extensión, $S \subseteq K$, definimos la "extensión de F generada por S" como el menor subcuerpo de K que contiene a $F \cup S$, denotado por $F(S)$.
Si $S = \{s_1, \ldots, s_t\}$, simplificaremos la notación y escribiremos $F(s_1, \ldots, s_t)$.

Ejemplo. $\mathbb{Q}(\sqrt{2})$ es el menor subcuerpo de $\mathbb{R}$ que contiene a $\sqrt{2}$, y viene dado por:

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

Demostración. Veámoslo:

$\supseteq$) Sean $a, b \in \mathbb{Q}$, tenemos que $a, b, \sqrt{2} \in \mathbb{Q}(\sqrt{2})$, por lo que $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$.

$\subseteq$) Si demostramos que $\{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ es un cuerpo, entonces tenemos esta inclusión, ya que $\mathbb{Q}(\sqrt{2})$ es el menor subcuerpo de $\mathbb{R}$ que contiene a $\sqrt{2}$. Es evidente que dicho conjunto es un anillo. Para ver que es un cuerpo, dado

$\alpha = a + b\sqrt{2}$, buscamos calcular un elemento inverso al mismo que sea de la misma forma. Sea:

$$\beta = \frac{a}{a^2 - 2b^2} - \frac{b\sqrt{2}}{a^2 - 2b^2} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} \in \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$$

Observamos que:

$$\alpha\beta = \left(a + b\sqrt{2}\right) \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{\left(a + b\sqrt{2}\right)\left(a - b\sqrt{2}\right)}{\left(a + b\sqrt{2}\right)\left(a - b\sqrt{2}\right)} = 1$$

Por lo que dicho conjunto es un cuerpo, al tener todo elemento un inverso.

□

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

Definición 1.8 (Cuerpo de descomposición)**.** Sea K un cuerpo, $f \in K[x]$ y $K \leqslant E$ extensión de cuerpos tal que f se descompone completamente en $E[x]$ como producto de polinomios lineales (es decir, de grado 1) 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 (o de escisión) de f sobre K.

Ejemplo. Veamos varios ejemplos de cuerpos de descomposición de polinomios:

- Si consideramos $x^2 + 1 \in \mathbb{R}[x]$, como $\mathbb{R} \leqslant \mathbb{C}$ y se cumple que $\mathbb{C} = \mathbb{R}(i, -i)$, tenemos que $\mathbb{C}$ es un cuerpo de descomposición de $x^2 + 1$.
- Por ejemplo, si $x^2 + 1 \in \mathbb{Q}[x]$, el cuerpo de descomposición en este caso es $\mathbb{Q}(i)$, ya que $\mathbb{Q} \leqslant \mathbb{Q}(i)$ y $\mathbb{Q}(i) = \mathbb{Q}(i, -i)$.

Observación. Si $f \in \mathbb{Q}[x]$ y tomo[2] todas sus raíces en $\mathbb{C}$, digamos $\alpha_1, \ldots, \alpha_t$, entonces el cuerpo de descomposición de f es $\mathbb{Q}(\alpha_1, \ldots, \alpha_t)$

Ejemplo. Si tomamos $x^2 - 2 \in \mathbb{Q}[x]$, entonces su cuerpo de descomposición es $\mathbb{Q}(\sqrt{2})$.

Ejercicio 1.1.2. Si tenemos $F \leqslant K$ extensión de cuerpos y $S, T \subseteq K$, demostrar que:

$$F(S \cup T) = F(S)(T)$$

Demostración. Veámoslo por doble inclusión:

$\subseteq$) $F(S \cup T)$ es por definición el menor subcuerpo de K que contiene a $F \cup S \cup T$. Como $F(S)(T)$ es el menor subcuerpo de K que contiene a $F(S) \cup T$ y $F(S)$ es el menor subcuerpo de K que contiene a $F \cup S$, tenemos que $F(S)(T)$ contiene a $F \cup S \cup T$ y es un cuerpo, por lo que tenemos $F(S \cup T) \subseteq F(S)(T)$.

$\supseteq$) Está claro que el menor subcuerpo de K que contiene a $F \cup S \cup T$ ha de contener al menor subcuerpo de K que contiene a $F \cup S$, por lo que:

$$F(S \cup T) \supseteq F(S)$$

de donde:

$$F(S \cup T) = F(S \cup T)(T) \supseteq F(S)(T)$$

[2]Fundamentado por el Teorema Fundalmental del Álgebra.

□

Ejemplo. Si tomamos $f = x^3 - 2 \in \mathbb{Q}[x]$, este polinomios tiene 3 raíces distintas, ya que su polinomio derivado tiene como raíces el cero, incompatibles con las de f. Las raíces de f son $\sqrt[3]{2}$ y el resto son dos raíces complejas, que se calculan usando las raíces terciarias de la unidad:

$$\omega = e^{\frac{2\pi i}{3}} = \cos\left(\frac{2\pi}{3}\right) + i\,\mathrm{sen}\left(\frac{2\pi}{3}\right) = \frac{-1}{2} + i\frac{\sqrt{3}}{2}$$

Por lo que $\omega^3 = 1$, de donde $\left(\sqrt[3]{2}\omega\right)^3 = 2$. Así que el cuerpo de descomposición de f es $\mathbb{Q}\left(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\right)$, que es igual a $\mathbb{Q}\left(\sqrt[3]{2}, \omega\right)$.

Demostración. Como:

$$\mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2})(\omega\sqrt[3]{2}, \omega^2\sqrt[3]{2})$$

$$\mathbb{Q}(\sqrt[3]{2}, \omega) = \mathbb{Q}(\sqrt[3]{2})(\omega)$$

Basta ver:

$$\omega = \frac{\omega\sqrt[3]{2}}{\sqrt[3]{2}} \in \mathbb{Q}\left(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\right)$$

□

Ejercicio 1.1.3. Pregunta: ¿Quién es el cuerpo de descomposición de $x^2 + x + 1 \in \mathbb{Z}_2[x]$? ¿Existe? Todavía no podemos dar respuesta, por lo que necesitamos una noción más sofisticada de cuerpos de descomposición.

Ejemplo. Tomamos $f = x^n - 1$ con $n \geqslant 1$ y nos preguntamos sobre el cuerpo de descomposición de dicho polinomio, que tiene n raíces, y:

$$f' = nx^{n-1}$$

Por lo que no comparte raíces con f', luego tiene n raíces distintas, todas ellas de multiplicidad 1, que son:

$$\left\{\left(e^{\frac{2\pi i}{n}}\right)^k : k \in \{0, \ldots, n-1\}\right\}$$

Que es un subgrupo cíclico de orden n de $\mathbb{C} \setminus \{0\}$, generado por $e^{\frac{2\pi i}{n}}$. Cada uno de sus generadores se llama raíz $n-$ésima compleja primitiva de la unidad.

El cuerpo de descomposición de $x^n - 1 \in \mathbb{Q}[x]$ es $\mathbb{Q}(\eta)$, donde η es una raíz $n-$ésima compleja primitiva de la unidad.

Definición 1.9. Sea $F \leqslant K$ extensión y $\alpha \in K$, diremos que α es algebraico sobre F si $f(\alpha) = 0$ para algún $f \in F[x] \setminus \{0\}$. En caso contrario, diremos que α es trascendente sobre F.