



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<sup>1</sup>. Lo primero que sabemos es que un cuerpo es un tipo de anillo conmutativo. Un anillo<sup>2</sup> 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 yuxtaposición<sup>3</sup>, 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  $A$ .

---

<sup>1</sup>*field* en inglés

<sup>2</sup>*ring* en inglés

<sup>3</sup>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**  $f : A \rightarrow B$  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 anillos<sup>4</sup>  $\chi : \mathbb{Z} \rightarrow A$ . 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  $\Gamma$  un conjunto no vacío<sup>5</sup> 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  $\Gamma$  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,

<sup>4</sup>se prueba fácilmente por inducción

<sup>5</sup>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  $\Pi$  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 lineales<sup>6</sup> 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<sup>7</sup> 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<sup>8</sup> 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<sup>9</sup> todas sus raíces en  $\mathbb{C}$ , digamos  $\alpha_1, \dots, \alpha_t$  y c.d.d de  $f$  es  $\mathbb{Q}(\alpha_1, \dots, \alpha_t)$

**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  $F \leq K$  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

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

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<sup>10</sup>  $\mathbb{Q}(\sqrt[3]{2}, w)$

**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  $n \geq 1$ . 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

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

<sup>6</sup>de grado 1

<sup>7</sup>no tiene raíces en  $\mathbb{R}$  y no se puede descomponer en producto de polinomios de grado menor

<sup>8</sup>cuerpo de descomposición

<sup>9</sup>alpicando el Teorema Fundamental del Álgebra

<sup>10</sup>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  $F \leq K$  una extensión,  $\alpha \in K$ , diremos que  $\alpha$  es **algebraico sobre  $F$**  si  $f(\alpha) = 0$  para algún  $f \in F[x]$ ,  $f \neq 0$ . Sino,  $\alpha$  se llama **trascendente sobre  $F$** .

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

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

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

*Demostración.* Tomo  $e_\alpha : F[X] \rightarrow K$  la aplicación definida por  $e_\alpha(y) = g(\alpha)$ . Entonces tenemos que  $e_\alpha$  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 isomorfismo para anillos tenemos que

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

Como  $\text{Im } e_\alpha$  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  $h = f$ .

Veamos el isomorfismo. Sabemos que  $\text{Im } e_\alpha$  es un subcuerpo de  $K$ , que  $F \leq \text{Im } e_\alpha$  y  $\alpha \in \text{Im } e_\alpha$ . Tenemos entonces que  $F(\alpha) \leq \text{Im } e_\alpha$ . Un elemento de  $\text{Im } e_\alpha$  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  $F(\alpha) = \text{Im } e_\alpha \cong \frac{F[X]}{\langle f \rangle}$ .

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

<sup>11</sup>el coeficiente director es 1

<sup>12</sup>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  $\alpha$  sobre  $F$ . Lo notaremos como  $f = \text{Irr}(\alpha, F)$ .

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

**Ejemplo.**

- )  $\text{Irr}(i, \mathbb{Q}) = x^2 + 1 \in \mathbb{Q}[x]$ , por lo que  $\{1, i\}$  es una  $\mathbb{Q}$ -base de  $\mathbb{Q}(i)$
- )  $\text{Irr}(\sqrt{2}, \mathbb{Q}) = x^2 - 2 \in \mathbb{Q}[x]$
- )  $\text{Irr}(e^{\frac{i2\pi}{3}}, \mathbb{Q})$ . 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  $\text{Irr}(e^{\frac{i2\pi}{3}}, \mathbb{Q}) = (x^2 + x + 1)$ . 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  $F \leq K \leq L$  extensiones. Entonces se tiene que

$$F \leq L \text{ es finita} \iff \begin{array}{c} F \leq K \\ \text{y} \\ K \leq L \end{array} \text{ son finitos}$$

Además,  $[L : F] = [L : K][K : F]$ .

*Demostración.*

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

□

El nombre de este lema proviene de que cuando se tienen extensiones de cuerpos  $F_1 \leq F_2 \leq \dots \leq F_s$ , 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  $F \leq K$  una extensión de cuerpos,  $\alpha \in K$ . Entonces se tiene

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

*Demostración.*

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

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

□

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

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

*Demostración.*

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

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

□

*Observación.* Hemos visto que si  $\alpha_1, \dots, \alpha_n \in K$  y  $\alpha_1$  es algebraico sobre  $F$ ,  $\alpha_2$  es algebraico sobre  $F(\alpha_1)$ ,  $\dots$ ,  $\alpha_n$  es algebraico sobre  $F(\alpha_1, \dots, \alpha_n)$ , entonces  $[F(\alpha_1, \dots, \alpha_n) : F] \leq \infty$ .

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

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

entonces  $\Lambda$  es un subcuerpo de  $K$  y  $F \leq \Lambda$  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  $F \leq F(\alpha, \beta)$  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.**  $\Lambda$  se llama **clausura algebraica** de  $F$  en  $K$ .

**Ejemplo.** Si tomamos  $F = \mathbb{Q}$  y  $K = \mathbb{C}$  obtenemos 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  $\mathbb{Q}(\sqrt[n]{2}) \leq \overline{\mathbb{Q}}$  y  $\text{Irr}(\sqrt[n]{2}, \mathbb{Q}) = x^n - 2$  ya que por el criterio de Eisenstein<sup>13</sup> se tiene que  $x^n - 2$  es irreducible.

**Ejemplo.**  $W \in \mathbb{C}$

<sup>13</sup>si no te acuerdas pues lo recuerdas