

CAPÍTULO III

Sea A dominio

(P.66)

• **A DE** si $\exists \varphi: A \setminus \{0\} \rightarrow \mathbb{N}$ (grado) t_q

1) $\forall a, b \in A \setminus \{0\} \quad \varphi(a) \leq \varphi(ab)$

2) $\forall a, b \in A \setminus \{0\} \quad \exists q, r \in A : a = bq + r$ $\begin{cases} r=0 \\ 0 < r < \varphi(b) \end{cases}$

(φ dada a A de dom. euclídeo)

• Si: $\exists \varphi \quad t_q \uparrow \Rightarrow$ t_q es única ($K \neq$ los bsnr)

Sea ℓ grado ($\ell(A)$) $\Rightarrow \mathcal{U}(A) = \{u \in A : \forall (u) = \ell(u)\}$

Además, si: $m = \min(\text{im } \varphi) \Rightarrow \mathcal{U}(A) = \{u \in A : \forall (u) = m\}$

• Si: K cuerpo $\Rightarrow K$ es **DE**

De hecho, $\varphi: K \setminus \{0\} \rightarrow \mathbb{N}$ es cte.

• Sea ℓ función que dota de estructura de

DE a A (no cuerpo) $\Rightarrow \ell$ no cte

• $\exists \ell: \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{N}$ dada a \mathbb{Z} de

estructura de **DE** (P.72)

\exists infinitos primos $p \equiv 5 \pmod{12}$ (P.22)

$\mathbb{H}: \mathbb{Z}[i] \setminus \{0\} \rightarrow \mathbb{N}$

$x \mapsto x\bar{x}$, enteros \Leftrightarrow
 $x \in \mathbb{Z}[i]$ es irreducible

i) $|x|$ es entero primo

ii) $\exists p$ primo: $p \equiv 3 \pmod{4}$
 $y \quad x = \pm p \quad x = \pm ip$ (P.26)

(P.26)

A DIP

i) Si: $d = \text{mcd}(a_1, \dots, a_n) \Rightarrow dd = (a_1, \dots, a_n)A$

(diferencia: $3a_1 - a_2 = a_1, \dots, a_n - a_1 = d$)

a_1, \dots, a_n

ii) a_1, \dots, a_n son primos entre sí: $(a_1, \dots, a_n) = 1$

A

iii) Si: $m = \text{lcm}(a_1, \dots, a_n) \Rightarrow mA = \bigcap_{i=1}^n A_i$

Algoritmo Euclídeo: $\varphi: A \setminus \{0\} \rightarrow \mathbb{N}$ grado (A DE)

Sean $a, b \in A, b \neq 0$. $a = bq + r$, $b = sr + t$

... $\text{mcd}(a, b) = \text{mcd}(b, r) = \dots = \text{mcd}(t, 0) = r$
(P.90)

A DFU si $\forall a \in A \setminus \{\text{totorial}\}$:

1) $\exists p_1, \dots, p_r \in A$ irreducibles: $a = p_1 \cdots p_r$ (no totorial divisible)

2) Si: $q_1, \dots, q_s \in A$ irreducibles en A tq

$a = q_1 \cdots q_s \Rightarrow s \leq r$ y, recordando factores primos suponemos que p_1, \dots, p_r son irreducibles

A DFU si y solo si: (P.70)

1) Todo elemento irreducible es primo

2) Todo elemento no nulo ni unidad es producto de elementos irreducibles

$\mathbb{Z}[i]$ dominio noetheriano (P.71)

$\forall a \in A \setminus \{\text{totorial}\}, a$ es producto finito de elementos irreducibles de A .

los factores grado ℓ que satisfacen $\ell(xy) = \ell(x)\ell(y)$

Son NORMAS.

Dominio: $\mathbb{Z}[\sqrt{-5}] \rightarrow \mathbb{N}$ (\Rightarrow $\mathbb{Z}[\sqrt{-5}]$ es DIP)

\bullet $\mathbb{Z}[\sqrt{-11}]$ norma, A no cuerpo (P.71)

Luego $\mathcal{U}(A) = \{u \in A : \forall (u) = 1\}$ (P.71)

$\mathbb{Z}[i]$ es un DE con

$\varphi: \mathbb{Z}[i] \setminus \{0\} \rightarrow \mathbb{N}$ (P.71)

$x = x_1i \rightarrow x = x_1^2 + x_2^2$

$\mathcal{U}(\mathbb{Z}[i]) = \{z \in \mathbb{Z} : z^2 = 1\}$

$w = e^{\frac{2\pi i}{3}}$, $w^2 = 1 = (w-1)(1+w+w^2)$

Luego $A = \{a+bw : a, b \in \mathbb{Z}\}$ es

Subanillo unitario de \mathbb{C} , y con norma

$\mathbb{H}: A \setminus \{0\} \rightarrow \mathbb{N} : x = x\bar{x} = a^2 + b^2 - ab$

es un DE: $\mathcal{U}(A) = \{1, w, \pm(1+w)\}$

(P.72)

Sea A DFU \Rightarrow

$\forall a, b \in A \quad \exists$ un $\text{mcd}(a, b)$ en A

\bullet Si: d es un $\text{mcd}(a, b)$ en A y m es mcd cumple que $\text{mcd} = ab \Rightarrow m$ es un $\text{mcm}(a, b)$.

\bullet Sean $a_1, \dots, a_n \in A \Rightarrow \exists$
 $\text{med}(a_1, \dots, a_n), \text{mcm}(a_1, \dots, a_n)$
y $\forall b \in A \quad \text{mcd}(ba_1, \dots, ba_n) = b \cdot \text{mcd}(a_1, \dots, a_n)$ (P.90, P.91)

A DFU, $a \in A \setminus \{\text{totorial}\} \Rightarrow \exists u \in \mathbb{U}(A)$ y

$p_1, \dots, p_r \in A$ no anidados y $a = p_1 \cdots p_r$

$a = up_1^{\alpha_1} \cdots p_r^{\alpha_r}$ (P.68)

A DFU, $x, y, z \in A$: $\text{mcd}(x, y) = 1$

y $\exists u \in \mathbb{U}(A) : xy = u^2 \Rightarrow \exists a, b \in A$

$x = ua^2$ y $y = ub^2$ (P.69)

A DIP \Leftrightarrow **DIF** \Rightarrow **DFU** (P.71)

$\mathbb{Z}[i], \mathbb{Z}[\sqrt{-3}]$ son DE con

$\varphi(x) = |x|^2 = |a^2 - b^2|$ (P.73)

$\sqrt[n]{-1}$, $n \geq 3$ es

subanillo del cuerpo \mathbb{C}

pero **NO** es DFU

Primeras de $\mathbb{H}: t^2 - 1 = 5, (6 \pm 5\sqrt{-5})$

$A = \{1, \pm 5, \pm 2\sqrt{-5}\}$ es DIP pero

No DE: $\mathcal{U}(A) = \{1, \pm 1, \pm (1 \pm \sqrt{-5})\}$ (P.90)

p primo impar $\in \mathbb{Z}^+$ entonces son equivalentes:

(P.84)

\bullet p seducible en $\mathbb{Z}[i]$

\bullet p es suma de dos cuadrados (\Leftrightarrow cte. impar)

\bullet $p \equiv 1 \pmod{4}$

\bullet $\exists x \in \mathbb{Z} \quad t_q = -1 \equiv x^2 \pmod{p}$ (P.95)

Critério Hasse: A dom, sup. $\exists N: A \rightarrow \mathbb{N}$

ta $N'(0) = 1$ y $\forall a, b \in A$ tq $b \neq 0$,

$a \neq bd$ y $N(b) \leq N(a) \Rightarrow c, d \in A$:

$0 \leq N(ac-bd) \leq N(b)$

$\Rightarrow A$ es DIP (P.90)

Sea $p \in \mathbb{Z}$ primo impar \Rightarrow

$\exists x, y, m \in \mathbb{Z} \quad t_q = -1 \equiv x^2 + y^2 \pmod{p}$

(P.95)

Th. Lagrange ($t = x^2 + y^2 + z^2 + w^2$)

(P.91)