# ANILLOS (2)

**DEF** SEA $A$ ANILLO COMMUTATIVO, SEA $P \subset A$ IDEAL. SE DICE QUE $P$ ES PRIMO SI

- $P \subsetneq A$
- $a.b \in P \Rightarrow a \in P$ ó $b \in P$ $(a, b \in A)$.

**DEF** SE DICE QUE $P$ ES MAXIMAL SI

- $P \subsetneq A$
- NO EXISTEN IDEALES $J \subset A$ TALES QUE $P \subsetneq J \subsetneq A$.

(O SEA, $P \subset J \subsetneq A \Rightarrow P = J$)

**PROP** $P \subset A$ IDEAL MAXIMAL $\Rightarrow P$ ES PRIMO.

**DEM** SEA $P \subset A$ MAXIMAL Y SEA $a \in A, a \notin P$.
ENTONCES $J = P + A.a$ ES IDEAL, $P \subsetneq J$ $(a \in J - P)$
$\Rightarrow J = A \Rightarrow \underline{1 = p + \alpha.a}$, $p \in P, \alpha \in A$.

$P$ ES PRIMO: SUP. $a.b \in P$, $a \notin P$, $b \notin P$

$\Rightarrow 1 = p + \alpha.a$, $1 = q + \beta.b$ CON $p, q \in P$, $\alpha, \beta \in A$

$\Rightarrow 1 = 1.1 = p.q + \beta b p + \alpha a q + \alpha\beta a b \in P$

$\Rightarrow 1 \in P \Rightarrow A = P \Rightarrow\Leftarrow$ ✓

**OBS** LA RECÍPROCA ES FALSA.
P. EJ. $A = \mathbb{Q}[x, y]$, $P = \langle x \rangle$ ES PRIMO (VERIFICAR).
$P$ NO ES MAXIMAL: $\langle x \rangle \subsetneq \langle x, y \rangle \subsetneq A$.

**OBS** ESTA RECÍPROCA ES VERDADERA SI $A$ ES ANILLO PRINCIPAL (VER DEPUÉS).

**DEF** SEA $A$ UN ANILLO CONMUTATIVO

- $A^* = \mathcal{U}(A)$ = GRUPO DE UNIDADES DE $A$
  $= \{a \in A \ / \ \exists b \in A,\ a.b = 1\}$
- $a \in A$ ES DIVISOR DE CERO SI $\exists b \in A,\ b \neq 0,\ a.b = 0$
- SE DICE QUE $A$ ES ANILLO ÍNTEGRO SI EL ÚNICO DIVISOR DE CERO EN $A$ ES $a = 0$.
  (O SEA, VALE $a.b = 0 \Rightarrow a = 0$ o $b = 0$,
  O SEA, EL IDEAL $\{0\}$ ES PRIMO)

  EJERCICIO $\{0\}$ ES MAXIMAL $\Leftrightarrow$ $A$ ES CUERPO. $(A^* = A - \{0\})$
- $a \in A$ ES NILPOTENTE SI $\exists n \in \mathbb{N} \ / \ a^n = 0$
- SE DICE QUE $A$ ES UN ANILLO REDUCIDO SI EL ÚNICO ELEMENTO NILPOTENTE EN $A$ ES $a = 0$

**OBS** $a$ NILPOTENTE $\Rightarrow$ $a$ DIVISOR DE CERO

LA RECÍPROCA ES FALSA: $A = \mathbb{Z}_6$, $a = \overline{2}$.

**PROP** $P \subset A$ IDEAL

$P$ PRIMO $\Leftrightarrow$ $A/P$ ES ANILLO ÍNTEGRO

$P$ MAXIMAL $\Leftrightarrow$ $A/P$ ES CUERPO

**DEM** EJERCICIO

**DEF** SEA $A$ UN DOMINIO (= ANILLO CONMUTATIVO ÍNTEGRO)

UN IDEAL $I \subset A$ SE DICE PRINCIPAL SI $\exists a \in A \ / \ I = \langle a \rangle$.

SE DICE QUE $A$ ES UN DOMINIO DE IDEALES PRINCIPALES

(= $A$ ES DOMINIO PRINCIPAL = $A$ ES DIP) SI TODO IDEAL DE $A$ ES PRINCIPAL.

**EJ** $\mathbb{Z}$ ES DIP, $k[x,y]$ NO ES DIP.

$k[x]$ ES DIP

**DEM** EJERCICIO, O VER DESPUÉS.

DEF SEA $A$ UN DOMINIO, SEAN $a, b \in A$.
DECIMOS QUE $a$ ES ASOCIADO A $b$ SI EXISTE $u \in A^*$ TAL QUE $a = u.b$, EN CUYO CASO ESCRIBIMOS $a \sim b$.

OBS LA RELACIÓN $\sim$ EN $A$ ES RELACIÓN DE EQUIVALENCIA. ES LA RELACIÓN ASOCIADA A LA ACCIÓN DEL GRUPO $(A^*, \cdot)$ EN $A$ DADA POR MULTIPLICACIÓN $A^* \times A \to A$ $(u, b) \mapsto u.b$.

OBS $a \sim b \iff \langle a \rangle = \langle b \rangle$
EN PARTICULAR, $a \sim 1 \iff a \in A^* \iff \langle a \rangle = \langle 1 \rangle = A$.

DEF SEA $A$ UN DOMINIO, SEAN $a, b \in A$.
DECIMOS QUE $a$ DIVIDE A $b$ (ESCRITO $a | b$) SI EXISTE $c \in A$ TAL QUE $b = a.c$

OBS $a | b \iff \langle b \rangle \subset \langle a \rangle$

OBS $a | b, b | c \Rightarrow a | c$
$a | b, b | a \iff a \sim b$

DEF SEA $A$ UN DOMINIO, SEA $a \in A$.

- $a$ ES PRIMO SI $P = \langle a \rangle$ ES IDEAL PRIMO
  ($\iff$ · $a \notin A^*$
  · $a | x.y \Rightarrow a | x$ o $a | y$, PARA $x, y \in A$)
- $a$ ES IRREDUCIBLE SI $b | a \Rightarrow b \in A^*$ o $b \sim a$
  (LOS ÚNICOS DIVISORES DE $a$ SON LOS DIVISORES TRIVIALES: UNIDADES o ELEMENTOS ASOCIADOS)

PROP $a \in A$ PRIMO, $a \neq 0 \Rightarrow a$ ES IRREDUCIBLE.

DEM SEA $b \in A$ / $b | a \Rightarrow a = b.c$, $c \in A \Rightarrow a | b.c$
$\Rightarrow a | b$ o $a | c \Rightarrow b = \beta.a$ o $c = \gamma.a$ $(\beta, \gamma \in A)$
$\Rightarrow a = b.c = c\beta a$ o $a = b.c = b\gamma a$
$\Rightarrow$ $1 = c.\beta$ o $1 = b.\gamma$ $\Rightarrow c \in A^*$ o $b \in A^*$
TACHO $a$
$\Rightarrow b \sim a$ o $b \in A^*$ ✓

OBS LA RECÍPROCA NO VALE EN GENERAL.
(VALE SII A ES DFU, COMO VEMOS ENSEGUIDA)

DEF SEA A UN DOMINIO. DECIMOS QUE A ES UN DOMINIO DE FACTORIZACIÓN ÚNICA (= DFU) SI SE SATISFACEN LAS CONDICIONES

1) TODO ELEMENTO $a \in A$, $a \neq 0$, SE PUEDE REPRESENTAR COMO PRODUCTO DE ELEMENTOS IRREDUCIBLES.
O SEA, $\forall a \in A, a \neq 0, \exists r_1, r_2, \dots, r_n$ IRREDUCIBLES TAL QUE $a = r_1 \cdot r_2 \cdots r_n$

2) LA FACTORIZACIÓN DE 1) ES ÚNICA, SALVO ORDEN Y SALVO ASOCIADOS. O SEA, SI $a = s_1 \cdot s_2 \cdots s_m$ ES OTRA FACTORIZACIÓN CON $s_i$ IRREDUCIBLE $\forall i$ ENTONCES $m = n$ Y $\exists \sigma \in S_n / r_i \sim s_{\sigma(i)}$.

EJ $\mathbb{Z}$ ES DFU (ALGEBRA I, Y VER DESPUES)
$k[t]$ " , $k$ CUERPO (ALGEBRA I, " )
$k$ CUERPO, $k[t_1, \dots, t_n]$, $k[[t_1, \dots, t_n]]$ SON DFU
+ GENERAL: A DFU $\Rightarrow A[t_1, \dots, t_n]$, $A[[t_1, \dots, t_n]]$ DFU
(DEM. DESPUES EN PRACTICA)

EJ $A = k[x_1, x_2, x_3, x_4] / \langle x_1 x_2 - x_3 x_4 \rangle$ NO ES DFU (PRÁCTICA)

EJ $A = \mathbb{Z}[\sqrt{d}]$, $d \in \mathbb{Z}$ DFU PARA ALGUNOS VALORES DE $d$.

$\boxed{\text{EJERCICIO: 1) VALE EN } \mathbb{Z} \text{ (INDUCCIÓN) 1) VALE EN } k[t]}$

OBS LA PROPIEDAD 1) (EXISTENCIA) VALE EN MUCHOS ANILLOS (VALE EN TODOS LOS ANILLOS NOETHERIANOS, DESPUES)
IDEA HEURÍSTICA DE PORQUE VALE: SEA $a \in A$, $a \neq 0$.
QUIERO FACTORIZAR $a$ COMO PRODUCTO DE IRREDUCIBLES.
SI $a$ ES IRREDUCIBLE $a = a$ ES UNA TAL FACTORIZACIÓN.
SI $a$ NO ES IRRED. $\Rightarrow a = a_1 a_2$, $a_i \not\sim a$.
$a_1, a_2$ IRRED. $\Rightarrow$ LISTO.
CASO CONTRARIO, CONTINÚO CON $a_1$ Y $a_2$.
GENERALMENTE ESTE PROCESO TERMINA (ESTO OCURRE SI A ES NOETHERIANO, COMO VEREMOS)
PERO HAY EJEMPLOS DE ANILLOS DONDE 1) NO VALE.

OBS LA PROPIEDAD 2) (UNICIDAD) ES MÁS DELICADA.
TENEMOS:

PROP SEA A UN DOMINIO. SON EQUIVALENTES:

i) A ES DFU (O SEA, 1) + 2))

ii) VALE 1) Y TODO ELEMENTO IRREDUCIBLE DE A ES PRIMO.

DEM

i) $\Rightarrow$ ii): SEA $a \in A$ IRREDUCIBLE. QVQ: $a$ ES PRIMO.
SUP. $a \mid b.c$, O SEA, $b.c = \alpha.a$ ($\alpha \in A$) $\Rightarrow$
$a$ ES UN IRREDUCIBLE QUE FORMA PARTE DE LA FACTORIZACIÓN ÚNICA DE $b$ O DE $c$ (A ES DFU)
$\Rightarrow a \mid b$ o $a \mid c$ ✓

ii) $\Rightarrow$ i) SUP. $r_1.r_2 \dots r_m \overset{\odot}{=} s_1.s_2 \dots s_n$
CON $r_i, s_j$ IRREDUCIBLES.
$r_1$ IRRED. $\Rightarrow r_1$ PRIMO.
$\odot \Rightarrow r_1 \mid s_1 \dots s_n \Rightarrow r_1 \mid s_j$, PARA ALGÚN $j$
$\Rightarrow r_1 \sim s_j$. TACHAR Y SEGUIR ✓

PROP SEA A UN DIP. ENTONCES TODO ELEMENTO IRREDUCIBLE DE A ES PRIMO.

DEM SEA $a \in A$ IRREDUCIBLE. SUP. $a \mid b.c$, $a \nmid b$
QVQ $a \mid c$. EL IDEAL $\langle a, b \rangle$ ES PRINCIPAL $\Rightarrow \langle a, b \rangle = \langle \alpha \rangle$
$\alpha \in A$

AFIRMO: $\langle \alpha \rangle = A = \langle 1 \rangle$ (O SEA, $\alpha \sim 1$)
COMO $a \in \langle a, b \rangle$, VALE $a \in \langle \alpha \rangle \Rightarrow a = \alpha.\alpha'$, $\alpha' \in A$
$\underset{a \text{ IRREDUCIBLE}}{\Rightarrow}$ $\alpha \sim a$ o $\alpha \sim 1$. SI FUESE $\alpha \sim a$
TENDRÍAMOS $\langle \alpha \rangle = \langle a \rangle \Rightarrow \langle a, b \rangle = \langle a \rangle \Rightarrow b \in \langle a \rangle$
$\Rightarrow a \mid b$, CONTRADICCIÓN CON $a \nmid b$. ENTONCES $\alpha \sim 1$
O SEA, $\langle a, b \rangle = \langle 1 \rangle \Rightarrow \exists\, r, s \in A \,/\, 1 = ra + sb$
$\Rightarrow c = (r.c).a + s\,bc \underset{a \mid b.c}{\Rightarrow} a \mid c$ ✓

PROP A DIP $\Rightarrow$ A DFU

DEM BASTA CON VER QUE VALE ii) DE PROP. PAG. 41

A DIP $\Rightarrow$ TODO IRREDUCIBLE ES PRIMO

POR LA PROP ANTERIOR

A DIP $\Rightarrow$ 1) (EXISTENCIA DE FACTORIZACIÓN

QUEDA PENDIENTE PARA CUANDO VEAMOS ANILLOS NOETHERIANOS

---

SEA A UN DOMINIO. SEA $\mathcal{P} \subset A$ UN CONJUNTO DE REPRESENTANTES DE LAS CLASES (EN LA RELACIÓN $\sim$) DE ELEMENTOS IRREDUCIBLES. O SEA, SI $a \in A$ ES IRREDUCIBLE, $\exists! \, p \in \mathcal{P} \,/\, a \sim p$.

EJ: $A = \mathbb{Z}$, $\mathcal{P} = \{p \in \mathbb{Z},\ p \text{ PRIMO},\ p > 0\}$

ENTONCES A ES DFU $\Leftrightarrow$ TODO $a \in A$, $a \neq 0$, SE ESCRIBE DE MODO ÚNICO (SALVO ORDEN) COMO

$$a = u \cdot \prod_{p \in \mathcal{P}} p^{m_p}$$

CON $m_p \in \mathbb{N}$, ~~[illegible]~~ $(m_p)_{p \in \mathcal{P}}$ CON SOPORTE FINITO

$u \in A^*$ $\qquad \{p \in \mathcal{P} \,/\, m_p \neq 0\}$ FINITO

DENOTAMOS $m_p = v_p(a)$

$\Rightarrow$ TENEMOS $v_p : A \to \mathbb{N} \cup \{+\infty\}$, $v_p(0) = +\infty$, $\forall p \in \mathcal{P}$

SE SATISFACE:

1) $v_p(a \cdot b) = v_p(a) + v_p(b)$

2) $v_p(a+b) \geq \min\{v_p(a), v_p(b)\}$

---

$v_p$ SE LLAMA "VALUACIÓN EN EL PRIMO $p \in \mathcal{P}$" de A

(SI A ES UN ANILLO, UNA <u>VALUACIÓN</u> DE A ES UNA FUNCIÓN $v : A \to \mathbb{N} \cup \{+\infty\}$, $v^{-1}(+\infty) = \{0\}$, TAL QUE VALEN 1), 2))

EJ $A = k[[t]]$ ($k$ CUERPO)

$t$ ES IRREDUCIBLE, $A^* = \{a = \sum_{i=0}^{\infty} a_i t^i \,/\, a_0 \neq 0\}$ (VERIFICAR)

$\forall a \in A$, $a = \sum_{i=0}^{\infty} a_i t^i = \sum_{i=r}^{\infty} a_i t^i$ ($a_0 = \cdots = a_{r-1} = 0$, $a_r \neq 0$)

$= u \cdot t^r$, $u = \sum_{i=r}^{\infty} a_i t^{i-r} \in A^*$

$\Rightarrow$ A ES DFU, $\mathcal{P} = \{t\}$

$\nu_t(a) = r$ = "ORDEN DE ANULACIÓN DE $a$ EN 0"

EJ $A = k[[t_1, t_2]]$ ES TAMBIÉN DFU (DEMO. EN PRÁCTICA) REF: LANG, ZARISKI-SAMUEL

PERO $\mathcal{P}$ ES INFINITO (SUP. $k$ INFINITO)

($t_1 + \alpha t_2$, $\alpha \in k$, SON IRREDUCIBLES NO ASOCIADOS)

AUNQUE HAY OTROS IRREDUCIBLES, P. EJ. $t_1^2 - t_2^3$ (VERIFICAR)

---

DEF SEA A UN DOMINIO, SEAN $a, b \in A$.

$c \in A$ ES UN MÁXIMO COMÚN DIVISOR DE $a$ Y $b$ SI (MCD)

1) $c | a$, $c | b$

2) $d|a$, $d|b \Rightarrow d|c$

EQUIVALENTEMENTE:

1)' $\langle c \rangle \supset \langle a, b \rangle = \langle a \rangle + \langle b \rangle$

2)' $\langle d \rangle \supset \langle a, b \rangle \Rightarrow \langle d \rangle \supset \langle c \rangle$

OBS DOS MCD DE $a$ Y $b$ SON ASOCIADOS ($\Leftarrow$ 2)')

OBS SI EL IDEAL $\langle a, b \rangle$ ES PRINCIPAL, $\langle a, b \rangle = \langle c \rangle$ ENTONCES $c$ ES MCD DE $a, b$

EN PARTICULAR, SI A ES DIP ENTONCES $\forall a, b \in A$ $\exists$ MCD $c$ (Y $c = ra + sb$, PARA $r, s \in A$)

OBS SI A ES DFU (AUNQUE A NO SEA DIP) TAMBIÉN EXISTE MCD $\forall a, b \in A$:

TOMAR $c = \prod_{p \in \mathcal{P}} p^{m_p}$, $m_p = \min\{\nu_p(a), \nu_p(b)\}$

EJ: $A = k[[t_1, t_2]] \Rightarrow$ MCD DE $t_1, t_2$ ~~ES~~ ES 1

(OBS: $1 \neq r.t_1 + s.t_2$, $r, s \in A$)

**DEF** SEA $A$ UN DOMINIO, SEAN $a, b \in A$.
$c \in A$ ES UN MÍNIMO COMÚN MÚLTIPLO DE $a$ y $b$ SI (MCM)

1) $a \mid c$, $b \mid c$
2) $a \mid d$, $b \mid d \Rightarrow c \mid d$

EQUIVALENTEMENTE:

1)' $\langle c \rangle \subset \langle a \rangle \cap \langle b \rangle$
2)' $\langle d \rangle \subset \langle a \rangle \cap \langle b \rangle \Rightarrow \langle d \rangle \subset \langle c \rangle$

**OBS** DOS MCM DE $a$ y $b$ SON ASOCIADOS ($\Leftarrow$ 2)')

**OBS** SI EL IDEAL $\langle a \rangle \cap \langle b \rangle$ ES PRINCIPAL, $\langle a \rangle \cap \langle b \rangle = \langle c \rangle$ ENTONCES $c$ ES MCM DE $a$ y $b$.
EN PARTICULAR, SI $A$ ES DIP ENTONCES $\forall a, b \in A$ $\exists$ MCM.

**OBS** SI $A$ ES DFU, EXISTE MCM $\forall a, b \in A$:
TOMAR $c = \prod_{p \in P} p^{n_p}$, $n_p = \max\{v_p(a), v_p(b)\}$

**DEF** SEA $A$ UN DOMINIO. SE DICE QUE $A$ ES UN DOMINIO EUCLIDEANO SI EXISTE $\delta: A-\{0\} \to \mathbb{N}$ TAL QUE:

1) $a \mid b \Rightarrow \delta(a) \leq \delta(b)$

2) DADOS $a, b \in A-\{0\}$, EXISTEN $q, r \in A$ TALES QUE $a = b.q + r$, CON $r=0$ ó $\delta(r) < \delta(b)$.

**EJ** $\mathbb{Z}$ ES EUCLIDEANO, CON $\delta(a) = |a|$, $a \in \mathbb{Z}$

$k[x]$ ($k$ CUERPO) ES EUCLIDEANO, CON $\delta = $ GRADO.

**PROP** $A$ EUCLIDEANO $\Rightarrow$ $A$ DIP

**DEM** SEA $I \subset A$ UN IDEAL.

SEA $a \in I$ TAL QUE $\delta(a) \leq \delta(b)$, $\forall b \in I$

($a \in I$ REALIZA $\min\{\delta(b), b \in I\}$)

AFIRMO: $I = \langle a \rangle$

($\supset$) PORQUE $a \in I$

($\subset$) SEA $b \in I$, ESCRIBO $b = q.a + r$ CON $r=0$ ó $\delta(r) < \delta(a)$

$\Rightarrow r = b - q.a \in I \underset{a \text{ MÍNIMO}}{\Rightarrow} r = 0 \Rightarrow b \in \langle a \rangle$ ✓

**OBS** EUCLIDEANO $\Rightarrow$ DIP $\Rightarrow$ DFU

$\qquad\qquad\qquad\;\; \not\Leftarrow \qquad\quad \not\Leftarrow$

- VER TEORÍA DE NÚMEROS (BOREVICH–SHAFAREVICH, SAMUEL) $A = \mathbb{Z}[\sqrt{d}]$, ...

**OBS** "IDEAL" PROVIENE DE "NÚMERO IDEAL" (T. DE NÚMEROS)

**OBS** "TEORÍA DE IDEALES" PASÓ A "TEORÍA DE MÓDULOS" POR EL CASO $A = k[x_1, \dots, x_n]$ ("SISTEMAS MODULARES" MACAULAY, 1916)