ANILLOS

DEF UN ANILLO ES UN CONJUNTO A PROVISTO DE DOS OPERACIONES BINARIAS $+$ Y $\cdot$ EN A, TALES QUE

1) $(A,+)$ ES GRUPO CONMUTATIVO
(SE DENOTA 0 EL ELEMENTO NEUTRO, Y $-a$ EL INVERSO DE CADA $a \in A$)

2) $(A,\cdot)$ ES MONOIDE
(SE DENOTA 1 EL ELEMENTO NEUTRO)

3) DISTRIBUTIVIDAD DE $\cdot$ RESPECTO A $+$

$$x\cdot(y+z) = (x\cdot y)+(x\cdot z), \quad (y+z)\cdot x = (y\cdot x)+(z\cdot x)$$

$\forall x,y,z \in A$. $\quad$ $(A,+,\cdot)$ ANILLO

SE DICE QUE ES UN ANILLO CONMUTATIVO SI $\cdot$ ES CONMUTATIVA.

DEF SI A Y B SON ANILLOS, UN MORFISMO DE ANILLOS ES UNA FUNCIÓN $f: A \to B$ TAL QUE

a) $f(x+y) = f(x)+f(y), \ \forall x,y \in A$

b) $f(x\cdot y) = f(x)\cdot f(y)$, "

c) $f(1) = 1$

OBS a) $\Rightarrow$ $f(0)=0$ y $f(-x) = -f(x), \ \forall x \in A$.

PROP COMPOSICIÓN DE MORFISMOS DE ANILLOS $A \to B \to C$ ES MORFISMO DE ANILLOS.

c) : HAY QUE PEDIRLO, P. EJ. $f: \mathbb{Z} \to \mathbb{Z}\times\mathbb{Z}$ (PRODUCTO DE ANILLOS)
$f(x) = (x,0)$ SATISFACE a), b) PERO NO c)
YA QUE $f(1) = (1,0) \neq (1,1)$

MÁS GENERAL: $f: (A,*) \to (B,*)$ MORFISMO DE MONOIDES, CON NEUTROS 1_A, 1_B. DEF: $a \in A$ ES IDEMPOTENTE SI $a*a = a$. ENTONCES:

- $a \in A$ IDEMPOTENTE $\Rightarrow$ $f(a) \in B$ IDEMPOTENTE ($\Rightarrow f(1_A) \in B$ IDEMPOTENTE)
- $b \in B$ IDEMP, $(B,*)$ GRUPO $\Rightarrow b = 1_B$ (DEM $b*b = b \Rightarrow b'*(b*b) = b'*b \Rightarrow b = 1_B$)

DEF SEA A UN ANILLO, SEA $X \subset A$ UN SUBCONJUNTO.
SE DICE QUE X ES SUBANILLO DE A SI
- X ES CERRADO POR $+$ $(x, y \in X \Rightarrow x+y \in X)$
- X ES CERRADO POR $\cdot$ ($x \in X \Rightarrow -x \in X$)
- $1 \in X$

$\Rightarrow (X, +, \cdot)$ TIENE ESTRUCTURA DE ANILLO

DEF SEA A UN ANILLO, SEA $X \subset A$ UN SUBCONJUNTO,
SE DICE QUE X ES UN IDEAL A IZQUIERDA DE A
(RESP. IDEAL A DERECHA, RESP. IDEAL) SI

= ideal bilatero

- X ES CERRADO POR $+$
- $\forall a \in A, \forall x \in X$ VALE $a.x \in X$

(RESP. $x.a \in A$, RESP. $a.x \in \cancel{A}$ Y $x.a \in X$)

PROP SEA $f: A \to B$ UN MORFISMO DE ANILLOS.
ENTONCES:
a) $\ker(f) = f^{-1}(0) \subset A$ ES UN IDEAL
b) $\operatorname{im}(f) \subset B$ ES UN SUBANILLO.

EJEMPLOS

1) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ SON ANILLOS CONMUTATIVOS
(SE RECUERDA SU CONSTRUCCIÓN EN PRÁCTICA 2)

2) A ANILLO $\rightarrow$ $A[[t]]$ = ANILLO DE SERIES FORMALES CON COEFICIENTES EN A
$(A^{\mathbb{N}}, +, \cdot)$ $+$ SUMA EN CADA COORDENADA:

$f, g: \mathbb{N} \to A$ $\quad (f+g)(n) = f(n) + g(n)$

- DE CAUCHY O DE CONVOLUCIÓN:

$$(f \cdot g)(n) = \sum_{i=0}^{n} f(i) \cdot g(n-i)$$

NOTACIÓN: $t = (0, 1, 0, \ldots, 0, \ldots)$ $\quad t^i(j) = 1 \quad j = i$
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\; = 0 \quad j \neq i$

$\Rightarrow$ "$f = \sum_{i=0}^{\infty} f(i)\, t^i$" VER PRÁCTICA

$A[t] = \{ f \in A[\![t]\!] \ / \ \mathrm{sop}(f) \text{ finito} \}$

SUBANILLO DE $A[\![t]\!]$ $\Rightarrow$ ES ANILLO.

3) A ANILLO, $m \in \mathbb{N}$. DENOTAMOS $[m] = \{ j \in \mathbb{N}, 1 \leq j \leq m \}$

$$A^{m \times m} = A^{[m] \times [m]} = \{ f : [m] \times [m] \to A \}$$

$$[m] \times [m] = \{ (i,j) \in \mathbb{N} \times \mathbb{N} \ / \ 1 \leq i \leq m, 1 \leq j \leq m \}$$

$A^{m \times m}$ = MATRICES $m \times m$ CON COEFICIENTES EN A.

NOTACIÓN: PARA $f : [m] \times [m] \to A$

$$f = (f(i,j))_{1 \leq i,j \leq m} = (f_{ij})_{1 \leq i,j \leq m}$$

PARA $f, g \in A^{m \times m}$

$$(f+g)_{ij} = f_{ij} + g_{ij}, \quad \forall i,j$$

$$(f \cdot g)_{ij} = \sum_{k=1}^{m} f_{ik} \cdot g_{kj}, \quad \forall i,j$$

$\Rightarrow (A^{m \times m}, +, \cdot)$ ANILLO (NO-CONMUTATIVO, SI $m > 1$.)

4) ITERAR, COMBINAR, OPERACIONES ANTERIORES

$A[t][u]$, $A[\![t]\!][u]$, $A[t][\![u]\!]$, $A[\![t]\!]^{m \times m}$, ETC.

5) $A[t,u]$, $A[\![t,u]\!]$, $A[\![t_1, \dots, t_r]\!]$, VER PRÁCTICA.

- Γ MONOIDE, A ANILLO $\Rightarrow$ $A[\Gamma] < A[\![\Gamma]\!] = \{ \sum_{\gamma \in \Gamma} a_\gamma \cdot \gamma, \ a_\gamma \in A \}$

$\Gamma = (\mathbb{N}^r, +) \Rightarrow A[t_1, \dots, t_r] < A[\![t_1, \dots, t_r]\!]$

- VER PRÁCTICA (Γ CON HIPÓTESIS)

6) ANILLO DE CUATERNIONES

$\mathbb{H} = (\mathbb{R}^4, +, \cdot)$
- $+$ HABITUAL EN $\mathbb{R}^4$
- DETERMINADO POR LA TABLA DE MULTIPLICAR $e_i \cdot e_j$
  e_1, e_2, e_3, e_4 BASE CANÓNICA

$e_1 \cdot e_i = e_i, \ \forall i$ (VER AXIOMAS DE ANILLO.)

$e_2^2 = e_3^2 = e_4^2 = -e_1$

$e_2 \cdot e_3 = -e_3 \cdot e_2 = e_4, \quad e_3 \cdot e_4 = -e_4 \cdot e_3 = e_2, \quad e_4 \cdot e_2 = -e_2 \cdot e_4 = e_3$

7) A ANILLO, J CONJUNTO

$A^J = \{ f : J \to A \}$ ES ANILLO, CON $+$ Y $\cdot$ PUNTO A PUNTO:

$(f+g)(j) = f(j) + g(j)$, $(f \cdot g)(j) = f(j) \cdot g(j)$ $\forall j \in J$.

<u>EJ</u> $J = \{1, 2\} \to A^2 = A \times A$

<u>EJ</u> $J = (0,1) \subset \mathbb{R}$, $A = \mathbb{R}$

$A^J = \{ f : (0,1) \to \mathbb{R} \}$

SUBANILLOS: f CONTINUA, f $\mathcal{C}^\infty$, ETC.

$D = J = \{ z \in \mathbb{C} \,/\, |z| < 1 \} \subset \mathbb{C}$, $A = \mathbb{C}$

$A^J = \{ D \xrightarrow{f} \mathbb{C} \}$

SUBANILLOS: f HOLOMORFA, ETC.

ANILLOS DE FUNCIONES.

8) $A_1, \dots, A_r$ ANILLOS $\to$ $A = A_1 \times \dots \times A_r$ ANILLO

($+$, $\cdot$ EN CADA COORDENADA)

$(A_j)_{j \in J}$ FAMILIA DE ANILLOS $\to$ $A = \bigtimes_{j \in J} A_j$ ANILLO.

PROP SEA $(A,+,\cdot)$ UN ANILLO, SEA $I \subset A$ UN IDEAL BILÁTERO.
EN EL GRUPO $(A/_I,+)$ EXISTE UNA ÚNICA ESTRUCTURA DE ANILLO TAL QUE $\pi: A \to A/_I$ ES MORFISMO DE ANILLOS.

DEM $(A,+)$ ES GRUPO CONMUTATIVO, $I \subset A$ ES SUBGRUPO NORMAL
$\Rightarrow$ TENEMOS DEFINIDO $(A/_I,+)$ GRUPO $((a+I)+(b+I)=(a+b)+I)$
AFIRMO: LA OPERACIÓN BINARIA $\cdot : A \times A \to A$ ES COMPATIBLE CON LA RELACIÓN DE EQUIVALENCIA R DEFINIDA POR I.

DEM: $x R y \Leftrightarrow x-y \in I$
QVQ: $xRy \Rightarrow x.z \, R \, y.z$, $z.x \, R \, z.y$
$xRy \Rightarrow x-y \in I \underset{I \text{ IDEAL DER.}}{\Rightarrow} (x-y).z \in I \Rightarrow x.z - y.z \in I$
$\Rightarrow x.z \, R \, y.z$ ✓
LA OTRA ES SIMILAR (I IDEAL IZQ.)

$\Rightarrow \cdot$ INDUCE OPERACIÓN BINARIA (LA DENOTO $\cdot$) EN EL CONJUNTO COCIENTE $A/_R = A/_I = \{a+I\}_{a\in A}$
MEDIANTE $(a+I)\cdot(b+I) = (a.b)+I$

RESULTA: $\pi: A \to A/_I$ SATISFACE
$$\left.\begin{aligned} \pi(a+b) &= \pi(a)+\pi(b) \\ \pi(a.b) &= \pi(a).\pi(b) \end{aligned}\right\} (\cdot)$$

NOTACIÓN $\pi(a) = a+I = \bar{a}$ = "CLASE DE $a \in A$ MÓDULO I". ($\in A/_I$)

$\overline{a+b} = \bar{a}+\bar{b}$, $\overline{a.b} = \bar{a}.\bar{b}$ CON ESTA NOTACIÓN.

YA SABEMOS $(A/_I,+)$ ES GRUPO (NEUTRO: $\bar{0} = I$) $-\bar{a} = \overline{-a}, a \in A$
$(A/_I,\cdot)$ ES MONOIDE (VERIFICAR) (NEUTRO: $\bar{1} = 1+I = \pi(1)$)
DISTRIBUTIVA (VERIFICAR)

$(\cdot)$ π ES MORFISMO DE ANILLOS

UNICIDAD: $(\cdot)$ DETERMINA LAS OPERACIONES $+,\cdot$ EN $A/_I$ YA QUE π ES SOBREYECTIVA ✓

DEF SEA A UN ANILLO, SEA $X \subset A$ UN SUBCONJUNTO. DENOTAMOS $A.X$ EL SUBCONJUNTO DE A CUYOS ELEMENTOS SON LAS SUMAS $\sum_{i=1}^{m} a_i . x_i$ CON $m \in \mathbb{N}$, $a_1, \dots, a_m \in A$, $x_1, \dots, x_m \in X$

SIMILARMENTE, $X.A = \left\{ \sum_{i=1}^{m} x_i . a_i ,\ m \in \mathbb{N},\ a_i \in A,\ x_i \in X \right\}$

$A.X.A = \left\{ \sum_{i=1}^{m} a_i . x_i . b_i ,\ m \in \mathbb{N},\ a_i, b_i \in A,\ x_i \in X \right\}$ $\quad A.\phi = \{0\}$

PROP a) $A.X$ ES IDEAL IZQ. DE A, $X \subset A.X$

b) SI $J \subset A$ ES IDEAL IZQ. TAL QUE $X \subset J$ ENTONCES $A.X \subset J$

SIMILARMENTE CON $X.A$ (IDEAL DER.) Y $A.X.A$ (IDEAL BILÁTERO)

DEM EJERCICIO $\qquad$ **OBS** A CONMUTATIVO $\Rightarrow X.A = A.X = A.X.A$

COR $X \subset A \Rightarrow$ TENEMOS EL ANILLO COCIENTE

$$A/A.X.A$$

EJ $A = \mathbb{Z}$, $X = \{n\} \Rightarrow A.X = \{n.m,\ m \in \mathbb{Z}\} = \mathbb{Z}.n$

$$\cancel{A/A.X} \quad A/A.X = \mathbb{Z}/\mathbb{Z}.n = \mathbb{Z}_n$$

NOTACIÓN ALTERNATIVA: $X = \{x_1, \dots, x_r\}$, $A.X.A = \langle x_1, \dots, x_r \rangle$

EJ/DEF A ANILLO CONMUTATIVO. UN IDEAL PRINCIPAL EN A ES UN IDEAL ~~(BILÁTERO)~~ GENERADO POR UN ELEMENTO $x \in A$:
$A.x\cancel{.A} = \langle x \rangle = \{a.x,\ a \in A\}$

EJ/DEF A ANILLO CONMUTATIVO. UN IDEAL FINITAMENTE GENERADO ES UN IDEAL DE LA FORMA $A.X$ CON $X \subset A$ CONJUNTO FINITO. O SEA, $X = \{x_1, \dots, x_r\}$

$$\langle x_1, \dots, x_r \rangle = \left\{ \sum_{i=1}^{r} a_i . x_i ,\ a_i \in A \right\}$$

EJ: $A = k[X_1, \dots, X_n]$ = POLINOMIOS, k CUERPO (O ANILLO CONMUTATIVO)

$X = \{f_1, \dots, f_r\}$ $\quad f_i \in A$

$$I = A.X = \left\{ \sum_{i=1}^{r} a_i . f_i ,\ a_i \in A \right\} = \langle f_1, \dots, f_r \rangle$$

DEF SEA $(A,+,\cdot)$ UN ANILLO.

UN MÓDULO (A IZQUIERDA) SOBRE A (= A-MÓDULO IZQ.)

ES UN GRUPO CONMUTATIVO $(M,+)$ PROVISTO DE UNA

FUNCIÓN $\mu : A \times M \to M$

(DENOMINADA "LEY DE OPERACIÓN EXTERNA" Y DENOTADA

$\mu(a,m) = a.m$, $\forall a \in A$, $\forall m \in M$) TAL QUE:

1) $a.(m+m') = a.m + a.m'$ $\forall a \in A, \forall m, m' \in M,$

2) $(a.b).m = a.(b.m)$, $\forall a, b \in A, \forall m \in M,$

3) $(a+b).m = a.m + b.m$, $\forall a, b \in A, \forall m \in M,$

4) $1.m = m$, $\forall m \in M.$

OBS SE TIENE ENTONCES $\tilde{\mu}: A \to \mathrm{End}(M)$

$$\tilde{\mu}(a)(m) = \mu(a,m) = a.m$$

$\tilde{\mu}$ MORFISMO DE ANILLOS,

DONDE $\mathrm{End}(M) = \{ f: M \to M, f \text{ MORFISMO PARA } + \}$

CON $+$ DE MORFISMOS, $\cdot$ = COMPOSICIÓN DE MORFISMOS.

OBS MÓDULO A DERECHA: SE REEMPLAZA 2) POR

2') $(a.b).m = b.(a.m)$

(O, ESCRIBIENDO $\mu(a,m) = m.a$, VALE $m.(a.b) = (m.a).b$)

SI A ES CONMUTATIVO, A-MOD. IZQ. = A-MOD. DER.

EJEMPLOS

1) $J \subset A$ IDEAL $\begin{smallmatrix}\text{IZQ.}\\ \text{DER.}\end{smallmatrix}$ $\Rightarrow$ J ES A-MÓDULO $\begin{smallmatrix}\text{IZQ.}\\ \text{DER.}\end{smallmatrix}$

2) SI A ES UN CUERPO, UN A-MÓDULO ES LO MISMO QUE UN A-ESPACIO VECTORIAL

3) SI $A=\mathbb{Z}$, UN $\mathbb{Z}$-MÓDULO ES LO MISMO QUE UN GRUPO ABELIANO $(M,+)$. EN EFECTO, LA ACCIÓN ESCALAR $\mu: \mathbb{Z}\times M \to M$ ESTA DETERMINADA POR $+$ MEDIANTE $m.x = \underbrace{x+\cdots+x}_{m \text{ VECES}}$, PARA $m \in \mathbb{Z}_{>0}$, $x \in M$

$m.x = (-x)+\cdots+(-x)$ PARA $m \in \mathbb{Z}_{<0}$.

4) k CUERPO, G GRUPO FINITO, $A = k[G]$

UN A-MÓDULO (IZQ.) EQUIVALE A UNA REPRESENTACIÓN LINEAL (SOBRE k) DE G. (VER PRÁCTICA)

5) k CUERPO, $A = k[t]$, V k-ESP. VECT.

UNA ESTRUCTURA DE A-MÓDULO EN V EQUIVALE A UN ENDOMORFISMO k-LINEAL $f: V \to V$ ($\Leftrightarrow$ MATRIZ) (VER PRÁCTICA)

6) $J \subset A$ IDEAL A IZQUIERDA $\Rightarrow$ EL GRUPO ABELIANO $(A/J, +)$ TIENE ESTRUCTURA DE A-MOD. IZQ. VIA

$a.(b+J) = a.b + J$ (VERIFICAR)