Anillos y módulos   Clase 17/08/23   PRIMERA CLASE

Estructuras algebraicas

Espacios vectoriales, Grupos, Cuerpos, Anillos, Álgebras, Módulos

Estructuras básicas.

1. MAGMA

Un conjunto X y una función $m: X \times X \to X$ (llamada operación)

La función a priori no verifica ninguna condición.

MAGMA CON UNIDAD

Un magma (X, m) tiene unidad si $\exists\, e \in X$:

$$m(e,x) = m(x,e) = x$$

MAGMA Asociativo

Si $m(x,y) = x \cdot y$ (notación) m es asociativo si

$$m(x, m(y,z)) = m(m(x,y), z)$$

o sea $x \cdot (y \cdot z) = (x \cdot y) \cdot z$

De las siete estructuras básicas hay 2 — las rojas que permiten definir las otras.

Grupo   Magma (G, m) asociativo con unidad y con inversa

o sea $\forall x \in G \ \exists\, x^{-1} \in G$ $m(x, x^{-1}) = m(x^{-1}, x) = e$; $x \cdot x^{-1} = x^{-1} \cdot x = e$

Otra

$(x \cdot y) \cdot z = x \cdot (y \cdot z)$ Asociativa

$\exists e : e \cdot x = x \cdot e = x$ Neutro

$\forall x \in G \ \exists\, x^{-1} \in G : \ x^{-1} \cdot x = x \cdot x^{-1} = e$ inversa

Def Un magma se dice $\begin{cases} \text{abeliano} \\ \text{conmutativo} \end{cases}$ si $m(x,y)=m(y,x)$

o sea $x\cdot y = y\cdot x$

Un grupo se dice conmutativo si el magma m (producto del grupo) es conmutativo.

Obs Un conjunto puede tener dos operaciones y ser un bimagma

(X,f,g) dos operaciones que se llaman suma y producto

$\left.\begin{array}{l} f=+ \\ g=\cdot \end{array}\right\}$ (X,f) es un grupo abeliano

o sea $f(x,y)=x+y$

(X,f,g) anillo (X,g) es un magma asociativo y con neutro. $g(x,y)=x\cdot y$

Axiomas hasta ahora

(X,f) $(x+y)+z = x+(y+z)$ Magma asociativo

$\exists\, 0\in X:$ $x+0=0+x=x$ con neutro

$\forall x \Rightarrow \exists -x:$ $x+(-x)=(-x)+x=0$ con inverso

(X,g) $(x\cdot y)\cdot z = x\cdot(y\cdot z)$ magma asociativo

$\exists\, 1\in X:$ $x\cdot 1 = 1\cdot x = x$ con neutro

Relación de las operaciones de un bimagma

$(a+b)\cdot c = a\cdot c + b c$

$x\cdot(y+z) = x\cdot y + x\cdot z$ distributiva

equivalente

$g(x,f(y,z)) = f(g(x,y),g(x,z))$

Z (curva peligrosa)

La relación entre ambas operaciones ley distributiva

NO es simétrica obre

Vale $x.(y+z) = x.y + x.z$ y no vale

$x+(y.z) = (x+y).(x+z)$

Resumen. Un anillo tiene dos operaciones $+, \cdot$

y dos neutros 0 y 1. Uno inversa de la suma.

Axiomas $(x+y)+z = x+(y+z)$ $(xy)z = x(yz)$ (As)

$\exists 0, 1 : x+0 = 0+x = x$ $x.1 = 1.x = x$ (Neutro)

$\forall x \exists -x : x+(-x) = (-x)+x = 0$ (opuesto)

$\forall x, y$ $x+y = \cancel{x+y}$ $y+x$ (abeliano)

$x.(y+z) = x.y + x.z$ (ley distributiva)

$(y+z).x = y.x + z.x$

Cuerpo Un anillo $(X, +, \cdot, 0, 1)$: $X^* = X - \{0\}$

no conmutativo

el $\cdot$ restringido a $X-\{0\} \times X-\{0\} \to X$

tiene inversa $\forall x \neq 0 \; \exists x^{-1} : x.x^{-1} = x^{-1}.x = 1$

Nos quedan 3 estructuras espacios vectoriales, módulos y álgebras que trataremos más adelante

Anillo conmutativo

$$\begin{cases} (X, +, \cdot, 0, 1) \quad \ldots\ldots\ldots \\ x, y \in X \qquad x \cdot y = y \cdot x \end{cases}$$

Cuerpo (conmutativo) es cuando el anillo que lo origina es conmutativo.

$M_2(\mathbb{R})$ son un anillo no conmutativo

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a+a', & b+b' \\ c+c', & d+d' \end{pmatrix} \qquad \begin{pmatrix} \cdot & \cdot \\ \cdot & \cdot \end{pmatrix}\begin{pmatrix} * & * \\ * & * \end{pmatrix} \text{ producto.}$$

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$$

$AB \neq BA$ matrices

$A + B = B + A$.

$$A \cdot (B + C) = A \cdot B + A \cdot C \leftarrow$$

$$A + (BC) \neq (A+B) \cdot (A+C)$$

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad C = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

$$\boxed{A + BC = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}} \qquad BC = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

$$A + B = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \qquad A + C = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$$

$$(A+B)(A+C) = \begin{pmatrix} 1 & \\ & \end{pmatrix}$$

ANILLOS.

Ejemplos $\mathbb{Z} = (+, \cdot, 0, 1)$

$\mathbb{Z}[t]$ (polinomios en la variable t.

$(\mathbb{Z}[t], +, \cdot, 0, 1)$

Estos dos son ejemplos de anillos conmutativos.

$(M_n(\mathbb{R}), +, \cdot, 0, 1)$ no es conmutativo. $\begin{pmatrix} f & g \\ h & k \end{pmatrix} \in M_2(k[t])$ $\begin{pmatrix} f' & g' \\ h' & k' \end{pmatrix}$ $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

Si R es un anillo $M_n(R)$ es un anillo (Ejercicio)

Anillo trivial $R = \{0\}$ $0 = 1$ $0 + 0 = 0$

$0 \cdot 0 = 0$ etc.

Polinomios sobre un anillo

$R[x]$ con las operaciones iguales que para $(\mathbb{Z}[x])$

$(r + r'x)(s + s'x) = rs + (rs' + r's)x + r's'x^2$

Si R es un anillo y S un conjunto cualquiera

$\Rightarrow$ $\mathrm{Func}(S, R)$ es un anillo

$f: S \to R$ $g: S \to R$ $fg: S \to R$ $(fg)(s) = f(s)g(s)$, etc.

Anillo de los números duales $\{(a, b) : a \in R \ b \in R\}$

$(a, b) \cdot (c, d) = (ac, ad + bc)$ $(a, b) + (c, d) = (a + c, b + d)$

Si escribimos $a = (a, 0)$ $\varepsilon = (0, 1)$ es claro que

$(a, 0) + (b, 0)(0, 1) = (a, 0) + (b \cdot 0, b \cdot 1 + 0 \cdot 0) = (a, 0) + (0, b) = (a, b)$ $(a, b) = a + b\varepsilon$.

$\mathbb{Q}[X] = (a_0, a_1, a_2 \dots a_n)$ $a_0 + a_1 X + \dots + a_n X^n$

$(a_0, a_1) \cdot (b_0, b_1)$

$a_0 + a_1 X$

$b_0 + b_1 X$

$X \in \mathbb{Q}[X]$

$R[X] = \left\{ \sum_{i}^{n} r_i X^i : r_0 \dots r_n \in R \right\}$

R anillo

$(M_n(R)[X])[Y]$ $(R[X])[Y]$

$M_2(\mathbb{R})[X]$ $(a_0 + a_1 X)(b_0 + b_1 X)$ $a_0 b_0 \neq b_0 a_0$

Propiedades básicas. Ejercicio

1. 0 y 1 son únicos. 0 to si $0'$ es: $0'+a = a+0' = a$

$a = 0+a = a+0 \quad \forall a \Rightarrow$ si $a=0$

$0 = 0'+0 = 0'$ etc

2. $\forall a,b \quad (-a)b = -(ab) = a(-b)$; $(-a)(-b) = ab$

3. Sea uso y $\underbrace{a+a+\dots+a}_{n} = na$ y $(-n)a = \underbrace{(-a)+\dots+(-a)}_{n}$
$= n(-a)$

Si $n \in \mathbb{Z}$ $(na)b = n(ab) = a(nb)$

Morfismo de anillos. Sean R y S anillos $f: R \to S$ función:

$f(ab) = f(a)f(b)$ $f(a+b) = f(a)+f(b)$ $f(1_A) = 1_B$

Siempre vale que $f(0_A) = 0_B$

$f(a) = f(a+0_A) = f(a)+f(0_A)$. Luego $f(a) = f(a)+f(0_A)$

luego como $a = a+b \Rightarrow b=0$ (sumando $-a$)

$\Rightarrow f(0_A) = 0_B$.

$f: A \to B$ es monomorfismo si es inyectiva
epi " " " sobreyectiva
isomorfismo si es biyectiva

Si $A=B$ $f: A \to A$ morfismo se llama endomorfismo y $\mathrm{End}(A)$ se llama el conj. de endomorfismos