Álgebra Moderna II. Martes 14 Feb. 2015

Anillos: $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$, $M_{2\times 2}(\mathbb{C})$

conjuntos con: 1) operación de grupo abeliano
$0 =$ iden.

2) Multiplicación, con 1
(no necesariamente conmutativa)

Sub anillos $R' \subseteq R$:

* Subconjuntos contienen $0, 1$
* Cerrados bajo $+$
* Cerrados bajo $\cdot$

Subanillos de $R = \mathbb{C}$

$\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$, CONMUTATIVOS

$\mathbb{Z} + \mathbb{Z}[i]$ Enteros Gaussianos

$\hookrightarrow$ $(a+bi)(c+di) = ab - bd + (bc+ad)i$

$R = \{$todos los polinomios en 1 variable$/\mathbb{C}\}$

$= \{a_0 + a_1 x + \dots + a_n x^n \mid a_i \in \mathbb{C}\}$

Ejer: Si R es un anillo conmutativo, entonces $R[x]$ lo es también.

<u>EJEM:</u> $R = \mathbb{Z}/2\mathbb{Z}$ $\quad R[x] \quad (x+1)^2 = x^2 + 2x + 1$

$= x^2 + 1$

<u>EJEM:</u> $R[x][y] = R[x,y]$

- ¿Cuáles son las propiedades que tienen en común todos los anillos?

- ¿Qué tan pequeño puede ser un anillo?

↳ El anillo más pequeño

$R = \{0\}$ $\quad 1 = 0$

Si $R \neq \{0\}$, entonces $1 \neq 0$ en R.

Demostración: Sea $a \in R$ y supongamos $1 = 0$.

$$a = 1 \cdot a = 0 \cdot a = (0+0) \cdot a$$ entonces

$$0 \cdot a = 0 \Rightarrow a = 0.$$

Por lo tanto $R = \{0\}$ $\blacksquare$

Siguiente anillo más pequeño $R = \mathbb{Z}/2\mathbb{Z}$

De hecho $\mathbb{Z}/n\mathbb{Z}$ es un anillo con n elementos.

¿Cómo obtener un anillo a partir de un grupo abeliano?

Sea $(A, +, 0)$ grupo abeliano

$$R = \mathrm{End}(A) := \{f : A \to A \mid \text{homomorfismos}\}$$

$$(f \underset{R}{+} g)(a) = f(a) \underset{A}{+} g(a) = g(a) + \dots$$

$$0_R(a) = 0_A$$

$$\underset{R}{-} f(a) = \underset{A}{-}\big(f(a)\big)$$

EJER:

$$f \overset{R}{-} f =$$

$$f + 0 = f$$

$$f \cdot g(a) = f(g(a))$$

EJER:

$$f \cdot 1 = f$$

(no necesariamente $f \cdot g \neq g \cdot \cancel{f}$)

EJEMPLOS: $\mathbb{Z} = \mathrm{End}(\mathbb{Z}, +, 0)$

$$\begin{aligned} f : \mathbb{Z} &\longrightarrow \mathbb{Z} \\ 1 &\longmapsto f(1) \end{aligned}$$

homo de gps

entonces

$$(f : \mathbb{Z} \to \mathbb{Z}) \longmapsto f(1)$$

$$\mathrm{End}(\mathbb{Z}) \longrightarrow \mathbb{Z}$$

EJER: $(-)(-) = +$

$$\mathrm{End}(\mathbb{Z}/n\mathbb{Z}, +, \circ) \cong \mathbb{Z}/n\mathbb{Z}$$

$$f \longmapsto \boxed{f(1)}$$

(Esto funciona para cualquier gp cíclico (finito))

<u>EJER</u>: ¿Qué está mal aquí?

en $R = \mathbb{Z}/6\mathbb{Z}$

$$\cancel{2}\cdot 4 = 8 = 2 = \cancel{2}\cdot 1$$

$$\Rightarrow \underline{\underline{4 = 1}} \text{ en } R \text{ ¿?}$$

$A = (\mathbb{Z}/p\mathbb{Z})^2$ $\quad \mathrm{End}(A, +, \circ) = M_2(\mathbb{Z}/p\mathbb{Z})$

$= \{ (a,b) \mid a,b \in \mathbb{Z}/p\mathbb{Z} \}$

$B = \begin{pmatrix} \alpha & \beta \\ \gamma & \theta \end{pmatrix}$

$f(a) = B \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}$

NO <u>commutativo</u>

<u>EJER</u>: si n no es primo $\mathrm{End}(\mathbb{Z}/n\mathbb{Z}, +, \circ)$
¿es un anillo?
¿Qué propiedades tiene?

EJER: $A = (\mathbb{Z}/p\mathbb{Z})^n$ $\quad \mathrm{End}(A) \cong M_{n\times n}(\mathbb{Z}/p\mathbb{Z})$