Anillo $(A, +, \cdot)$

$+$: aso
conm
inverso

$\times$: aso

$+$: Distrib.

Un anillo es un anillo de división si es con identidad y $\forall a \in A$ $a \neq 0$ existe un inv. multiplicativo a^{-1}.

Un anillo de div. Conmutativo se llama Campo.

- A anillo conmutativo $a \in A$, $a \neq 0$ se llama divisor del cero si $\exists b \in A$, $b \neq 0$: $ab = 0$
- un Anillo Conmutativo sin divisores del cero, se llama dom. de integridad.

ej: $$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

ej: $\mathbb{Z}_4$, $2 \cdot 2 = 4 \equiv 0$

el intruso es $\mathbb{Z}$

ej: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ $\rightsquigarrow$ No son campos porque en $\mathbb{Z}$ solo se puede invertir 1 y -1

Nota: Vamos a mostrar lo siguiente para practicar inducción fuerte.

Prop: Sea A anillo y sean $a_1, a_2, \ldots, a_n \in A$ luego $a_1 + a_2 + \ldots + a_n$ no depende de como pongo paréntesis en esta expresión:

Dem: Por inducción fuerte sobre n

1) Paso base $n=3$: Se cumple por que $+$ es asociativo.

2) Paso inductivo: Asumamos los resultados $\forall$ los naturales entre 3 y n y mostramos para n:

3) Si partimos con 2 maneras de poner paréntesis en $\sum_{i=1}^{n} a_i$ por hipótesis inductiva

llegamos a:

$$\left(\sum_{i=1}^{K} a_i\right) + \left(\sum_{i=K+1}^{n} a_i\right) \quad (*)$$

y $(**)$ $\left(a_1 + a_2 + \ldots + a_\ell\right) + \left(a_{\ell+1} + a_{\ell+2} + \ldots + a_n\right)$

con $1 \leq K$, $\ell < n$
Si $K = \ell$, no hay nada que hacer
Si no, podemos asumir $K < \ell$.

tenemos:

$$\left(\sum_{i=1}^{K} a_i\right) + \left(\sum_{i=K+1}^{n} a_i\right) = \left(a_1 + \ldots + a_K\right) + \left(\left(a_{K+1} + \ldots + a_\ell\right) + \left(a_{\ell+1} + \ldots + a_n\right)\right)$$

$$\left(a_1 + a_2 + \ldots + a_\ell\right) + \left(a_{\ell+1} + a_{\ell+2} + \ldots + a_n\right) = \left(\left(a_1 + \ldots + a_K\right) + \left(a_{K+1} + \ldots + a_\ell\right)\right) + \left(a_{\ell+1} + \ldots + a_n\right)$$

Si llamamos $x = a_1 + \ldots + a_K$

$y = a_{K+1} + \ldots + a_\ell$

$z = a_{\ell+1} + \ldots + a_n$

$x, y, z \in A$, porque A es anillo y:

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

Por asociatividad y

$$(*) = (**)$$

Sea A anillo, la suma tiene ley de cancelación:

$$a + b = a + c \Rightarrow b = c$$

$a, b, c \in A$.

$$(-a) + (a + b) = (a + c) + (-a)$$

$$(-a + a) + b = (a - a) + c$$

$$0 + b = 0 + c$$

$$b = c$$

esto para hacer enfasis de que en la multiplicación yo no puedo hacer cancelación

No hay ley de canselación para $\mathbb{Z}_4$:

$$0 \cdot 2 = 0 = 2 \cdot 2 \not\Rightarrow 0 = 2$$

Sea A anillo luego $a \cdot 0 = 0 \cdot a = 0$ $\forall a \in A$.

$$\cancel{a0} + 0 = a0 = a(0+0) = \cancel{a0} + a0$$

$$0 = a0 \quad \blacksquare$$

Nota: Solo para mirar

tenemos $-(-a) = a$ y $-(a+b) = -a-b$ $\blacksquare$

$\boxed{\text{Subanillo}}$ → Demostrar que algo es un subanillo es una buena estrategia para decir que algo es un anillo.

Sea A un anillo. Un subconjunto $B \subseteq A$ no vacío es un subanillo.

Si es un anillo con las mismas operaciones de A.

ej: $\mathbb{Z} \subset \mathbb{R}$, $\mathbb{Z}$ subanillo

$\mathbb{Z}$ no es campo

$\mathbb{R}$ sí.

ej: $\{\text{enteros pares}\} \subset \mathbb{Z}$

$\hookrightarrow$ subanillo

$\{\text{enteros impares}\} \subset \mathbb{Z}$

$\hookrightarrow$ No es subanillo

- no tiene neutro (zero)
- $2k+1+2m+1$
  $= 2(m+k)+2$
  $= 2(1+m+k)$ $\rightarrow$ No es cerrado

$B \neq \emptyset$, $B \subset A$ es subanillo si:

1) $+, \cdot$ Son operaciones en B:
   $\forall a, b \in B$, $a+b \in B$, $ab \in B$
2) $0 \in B$.
3) Si $a \in B$, $-a \in B$.

Prop: Sea $B \subset A$, $B \neq \emptyset$
luego B es subanillo si $\forall a, b \in B$:

1) $a+b \in B$
2) $ab \in B$
3) $-a \in B$.
4) $0 \in B$

Dem $a \in B \Rightarrow -a \in B$

luego
$$a + (-a) = 0 \in B \quad \blacksquare$$

Prop: Sea $\emptyset = B \subset A$ luego B es un subanillo si $\forall a, b \in B$:

1) $ab \in B$
2) $a - b \in B$

Dem: tenemos $a \in B \Rightarrow a - a = 0 \in B$

luego $0 - b = -b \in B$

finalmente
$$a - (-b) = a + b \in B. \quad \blacksquare$$

Queremos mostrar que todos los subanillos de $\mathbb{Z}$ son de la forma $m\mathbb{Z}$:

$$m\mathbb{Z} = \{ mx \,,\, x \in \mathbb{Z} \}$$

Aquí digo que esto es sub-anillo y cualquier subanillo es así

$m\mathbb{Z}$ subanillo: ejercicio

ej: Sea B subanillo de $\mathbb{Z}$.

Si $B = \{0\} = 0\mathbb{Z}$

Si $B \neq \{0\}$ existe $b \in B$, $b \neq 0$

luego también $-b \in B$

Sea

$$m = \min\{x \in B, x > 0\}$$

tenemos que $B = m\mathbb{Z}$.

De hecho siendo $m \in B$

$$m\mathbb{Z} \subset B$$

mostramos $B \subset m\mathbb{Z}$

Sea $b \in B$, queremos $m \mid b$, existen $q, r \in \mathbb{Z}$, $0 \leq r < m$:

$$b = qm + r$$

r debe ser 0

luego $r = b - mq$

Siendo $b \in B$, $mq \in m\mathbb{Z} \subset B$ y B, subanillo $r \in B$.

Siendo $0 \leq r < m$ y m mín positivo $r = 0$ y $m \mid b$