

RESUMEN ALGEBRA

CAONA

l.c.i $\Leftrightarrow$ función $\Leftrightarrow$ operación $\Leftrightarrow$ cerrada en el cto.

- Si una operación es l.c.i. sobre un conjunto al par $(A, *)$ le llamamos estructura algebraica

dr. $(A, *, \Delta) \Leftrightarrow *, \Delta \rightarrow$ leyes de comp. interna sobre A

- De $(A, *)$ e.a. puede pasar que:

- $\rightarrow *$ sea asociativa, conmutativa
- $\rightarrow$ puede existir un neutro (unio)
- $\rightarrow$ puede haber inverso único $\Leftrightarrow *$ es asoc. $\wedge$ $\exists$ neutro
- $\rightarrow$ " " " un absorbente $\rightarrow x+a=a \quad \forall x \in A$
- $\rightarrow$ " " " idempotente $\rightarrow a*a=a$

Import $\rightarrow \mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, \dots, [n-1]_n\}$
conjunto de clases de equivalencias de módulo n

Sea $(G, *)$ una e.a.

$(G, *)$ es grupo $\Leftrightarrow *$ es asociativa, $(G, *)$ tiene neutro $\wedge$
todo elemento de G tiene inverso

ademas
- Si $*$ es conmut. $\Rightarrow (G, *)$ es un grupo abeliano

dr. $\rightarrow$ todos elementos de G es cancelable

$\rightarrow$ único idempotente de un grupo es el neutro

Sea $(G, *)$ un grupo, $H \subseteq G$
 - Diremos que H es subgrupo de G si $(H, *)$ es grupo

*** TEOREMA ***

$(H, *)$ es subgrupo de $(G, *) \Leftrightarrow (\forall x, y \in H) x * y^{-1} \in H$

sea $n \geq 2 \rightarrow (\mathbb{Z}_n, +_n)$ es un grupo

- Sea $(G, *)$ un grupo
 Diremos que $(G, *)$ es un grupo finito si G es un conjunto finito
 a $|G|$ se le llama orden del grupo (por ej. $\mathbb{Z}_3 \rightarrow$ orden 3)

*** TEOREMA DE LAGRANGE ***

Sea $(G, *)$ un grupo finito y $(H, *)$ un subgrupo cualquiera de G
 $\Rightarrow |H|$ divide a $|G|$

Una función $f: A \rightarrow B$ es un morfismo si:
 $(\forall x, y \in A) f(x * y) = f(x) \Delta f(y)$

$\rightarrow$ si f es biyectiva $\Rightarrow f$ es isomorfa

semana 11

- Una estructura $(A, +, \cdot)$ se llamara anillo $\Leftrightarrow$

- 1) $(A, +)$ es un grupo abeliano
- 2) $\cdot$ es asociativa
- 3) $\cdot$ distribuye c/resp. a $+$

Obs: si 1 es neutro en A diremos que $(A, +, \cdot)$ es un anillo con unidad

- si $\cdot$ es conmut. $\Rightarrow (A, +, \cdot)$ se dira anillo conmutativo

- $(\mathbb{Z}_m, +_m, \cdot_m)$ es un anillo conmutativo con unidad

- Sea $(A, +, \cdot)$ un anillo. Sea $a \in A \setminus \{0\}$

$\Rightarrow$ a es divisor de 0 $\Leftrightarrow a$ no es cancelable

Obs:	$x \cdot y = 0 \quad \forall x \neq 0$ $\Rightarrow x, y$ divisores de 0
------	---

- Sea $(K, +, \cdot)$ una e.a. es cuerpo si:

- 1) $(K, +, \cdot)$ es anillo conmutat. con unidad
- 2) $\forall x \in K \setminus \{0\}$ es invertible para $\cdot$

$\Leftrightarrow$	$\begin{cases} \text{i) } (K \setminus \{0\}, +) \text{ grupo abeliano} \\ \text{ii) } \cdot \text{ distrib. c/resp. a } + \\ \text{iii) } \cdot \text{ invertible para } \forall x \neq 0 \end{cases}$
-------------------	---

- Un cuerpo no tiene divisores de 0 $\Rightarrow$ todos los elementos son cancelables.

- Sea $(A, +, \cdot)$ un anillo conmutativo con unidad. Si $|A|$ es finito entonces $(A, +, \cdot)$ no tiene divisores de 0 $\Leftrightarrow (A, +, \cdot)$ es cuerpo

- con $m \geq 2$ $(\mathbb{Z}_m, +_m, \cdot_m)$ es cuerpo $\Leftrightarrow (\mathbb{Z}_m, +_m, \cdot_m)$ no tiene divisores de 0 $\Leftrightarrow m$ es Primal