

(9) Dominio di INTEGRITÀ . è un anello  $(S, \perp, \top)$  t.c.

se e è l'elemento neutro rispetto a  $\perp$ ,

$$a \top b = e \Leftrightarrow a = e \text{ oppure } b = e$$

es  $(\mathbb{Z}, +, \cdot)$   $ab = 0 \Rightarrow a = 0 \text{ o } b = 0$

### ESEMPIO

A insieme, chiamato alfabeto

$A^+$  = insieme delle stringhe di lunghezza finita costruite usando gli elementi di A, gli elementi di  $A^+$  si dicono parole.

$w \in A^+$  è  $a_1 \dots a_n$ ,  $a_1, \dots, a_n \in A$

Consideriamo l'operazione  $\cdot : A^+ \times A^+ \rightarrow A^+$

$$(a_1 \dots a_n) \cdot (b_1 \dots b_m) = a_1 a_2 \dots a_n b_1 \dots b_m$$

- è detta CONCATENAZIONE

$(A^+, \cdot)$  semigruppo

Ha senso aggiungere  $\mu$  = parola vuota

$$A_\mu^+ = A^+ \cup \{\mu\}$$

$(A_\mu^+, \cdot)$  è un monoido, detto MONOIDE delle PAROLE.

DEF -  $(S, \perp)$  struttura algebrica.  $X \subseteq S$  è detto PARTE STABILE per  $\perp$

se  $\forall x, y \in X$ ,  $x \perp y \in X$

$\Rightarrow (X, \perp)$  è sottostruktura di  $(S, \perp)$

Ese -  $(\mathbb{R}, +)$  ha  $(\mathbb{N}, +)$ ,  $(\mathbb{N}_0, +)$ ,  $(\mathbb{Z}, +)$ ,  $(\mathbb{Q}, +)$  sono sottostrutture

$(\mathbb{R} \setminus \{0\}, \frac{x}{y})$  è sottostruttura:  $\frac{a}{b} \in \mathbb{Q} \subseteq \mathbb{R}$

$(\mathbb{N}, -)$  non è sottostruttura, ad es.  $\frac{2}{7} \notin \mathbb{N}$

Ese  $(\mathbb{R}, \cdot)$   $[2, 3] \subseteq \mathbb{R}$

$([2, 3], \cdot)$  non è parte stabile, perché  $2 \cdot 2 = 4 \notin [2, 3]$

$([0, 1], \cdot)$  lo è ( $a \leq 1 \cdot b \leq 1 \Rightarrow ab \leq 1$ )

### Proposizioni

Sia  $(S, \perp)$  s.a., sia  $X \subseteq S$  parte stabile. Allora:

- ① Se  $\perp$  è associativa in  $S \Rightarrow \perp$  è associativa in  $X$
- ② Se  $\perp$  è commutativa in  $S \Rightarrow \perp$  è commutativa in  $X$
- ③ Se  $S$  ha elemento neutro per  $\perp$ , e  $e \in X$   $\Rightarrow e$  è elemento neutro in  $X$
- ④ Se  $S$  ha elemento neutro per  $\perp$  e  $x \in S$  è simmetrico in  $S$  e  $x' \in X$   
 $\Rightarrow x'$  è simmetrico per  $x$  in  $X$

### Esempio

1)  $(\mathbb{N}, \cdot)$  è monoido

$$X = \{n \in \mathbb{N} \mid n \geq 5\}$$

$$\underbrace{a, b \in X}_{a \geq 5 \text{ e } b \geq 5} \Rightarrow ab \in X$$

$$ab \geq 25 \geq 5 \Rightarrow ab \in X$$

Non è monoido perché  $1 \notin X$

2)  $(\mathbb{Z}, +)$  è gruppo

$(\mathbb{N}_0, +)$  non è sottogruppo perché mancano i simmetrici

$(3\mathbb{Z}, +)$        $3\mathbb{Z} \subseteq \mathbb{Z}$

$$a, b \in 3\mathbb{Z} \Rightarrow a = 3h \quad \Rightarrow \quad a+b = 3h+3k = 3(h+k) \in 3\mathbb{Z}$$
$$b = 3k$$

$$0 = 3 \cdot 0 \in 3\mathbb{Z}$$

$$\forall 3h \in 3\mathbb{Z} \quad -3h = 3(-h) \in 3\mathbb{Z}$$

$\Rightarrow (3\mathbb{Z}, +)$  è sottogruppo.

### Proposizione

Sia  $(S, \perp)$  un monoido.

$$U(S) = \{x \in S \mid x \text{ è simmetricabile}\} \subseteq S$$

Allora  $U(S)$  è un gruppo rispetto a  $\perp$ .

#### DIM

1)  $a, b \in U(S) \Rightarrow a \perp b \in U(S)$  ?

2)  $e \in U(S)$  ( $e$  = elem neutro) ?

3)  $\forall a \in U(S)$ , il suo simmetrico  $a' \in U(S)$  ?

2)  $e$  è simmetricabile, con  $e' = e$  (perché  $e \perp e = e$ )

$$\Rightarrow e \in U(S)$$

1)  $a, b \in U(S) \Rightarrow \exists a', b'$  sono simmetrici

$$(a \perp b) \text{ è simmetricabile} \Leftrightarrow (a \perp b)' = b' \perp a'$$

$$\Rightarrow a \perp b \in U(S)$$

3)  $x$  è simmetricabile,  $a' \perp a = e = a \perp a' \Rightarrow a'$  è simmetricabile

con simmetria a  $\Rightarrow a' \in U(S)$  □

### ESEMPI:

①  $(\mathbb{Z}, +)$

$$U(\mathbb{Z}) = \{1, -1\}$$

$$(\mathbb{N}, \cdot), \quad U(\mathbb{N}) = \{1\}$$

$$(\mathbb{Q}, \cdot) \Rightarrow U(\mathbb{Q}) = \mathbb{Q} \setminus \{0\}$$

$(V^*, \circ)$  funzioni  $f: V \rightarrow V$

$U(V^*) = \{ \text{funzioni biettive} \}$

DEF - Data  $(S, \perp)$  s.a., una **CONGRUIENZA** è una relazione  
di equivalenza compatibile con  $\perp$

$R \subseteq S \times S$  è congruente  $\Leftrightarrow$  i)  $R$  è R. equivalenza

ii)  $a_1 R a_2 \text{ e } b_1 R b_2$

$$\Rightarrow (a_1 \perp b_1) R (a_2 \perp b_2)$$

ES - La congruenza modulo  $m$  è congruente di  $(\mathbb{Z}, +, \cdot)$  come  
anello.

DEF - Data  $(S, \perp)$  e  $R \subseteq S \times S$  congruente, l'insieme quoziente  
 $\frac{S}{R}$  è una struttura algebrica con operazione  $\tilde{\perp}$

definita da:  $[x]_R \tilde{\perp} [y]_R := [x \perp y]_R$

"**STRUTTURA QUOTIENTE**"

### PROPOSIZIONE

Sia  $(S, \perp)$  e  $(S/R, \tilde{\perp})$  struttura algebrica e quoziente-

Sia  $(S, \perp)$  e  $(S/R, \tilde{\perp})$  strutture algebriche a quoziente.

- ① Se  $\perp$  è associativa  $\Rightarrow \tilde{\perp}$  è associativa
- ② Se  $\perp$  è commutativa  $\Rightarrow \tilde{\perp}$  è commutativa
- ③ Se esiste elemento neutro  $e \in S$   $\Rightarrow [e]_R$  è elemento neutro per  $\tilde{\perp}$
- ④ Se  $x' \in S$  è simmetrico di  $x \in S$   $\Rightarrow [x']_R$  è simmetrico di  $[x]_R$
- ⑤ Se  $\perp$  ha  $(S, \perp, \top)$  e  $\top$  distribuisce su  $\perp$   $\Rightarrow \tilde{\top}$  distribuisce sulla  $\tilde{\perp}$ .

DIM

①  $\forall [x]_R, [y]_R, [z]_R$

$$\begin{aligned} ([x]_R \tilde{\perp} [y]_R) \tilde{\perp} [z]_R &= [x \perp y]_R \tilde{\perp} [z]_R = \\ &= [(x \perp y) \perp z]_R = \\ &= [x \perp (y \perp z)]_R = \\ &= [x]_R \tilde{\perp} [y \perp z]_R = \\ &= [x]_R \tilde{\perp} ([y]_R \tilde{\perp} [z]_R) \end{aligned}$$

②  $[x]_R \tilde{\perp} [y]_R = [x \perp y]_R = [y \perp x]_R = [y]_R \tilde{\perp} [x]_R$

□

ESEMPIO

$$\mathbb{Z}_{m\mathbb{Z}} = \mathbb{Z}_m = \{[0]_m, [1]_m, \dots, [m-1]_m\}$$

$\mathbb{Z}_m$  è anello quoziente  $[a]_m + [b]_m = [a+b]_m$

$$[a]_m \cdot [b]_m = [a \cdot b]_m$$

$[0]_m$  è elemento neutro per +

$$\hookrightarrow [0]_m + [a]_m = [0+a]_m = [a]_m$$

$[1]_m$  è elemento neutro per ·

$[1]_m$  è elemento neutro per.

$$\hookrightarrow [1]_m \cdot [a]_m = [1 \cdot a]_m = [a]_m$$

$$\mathbb{Z}_4 = \{[0]_4, [1]_4, [2]_4, [3]_4\}$$

$$\text{C'è } -[2]_4? \quad \checkmark \quad [-2]_4 = [2]_4$$

$\downarrow$

$$-2 \equiv 2 \pmod{4}$$

$$-[-3]? \quad \checkmark \quad [-3]_4 = [1]_4$$

$\downarrow$

$$-3 \equiv 1$$

### TEOREMA

$$(\mathbb{Z}_m^*) = \cup(\mathbb{Z}_m) = \{[a]_m \mid \text{MCD}(a, m) = 1\}$$

$[a]_m$  è invertibile in  $\mathbb{Z}_m \Leftrightarrow \text{MCD}(a, m) = 1$

Dm

( $\Rightarrow$ ) Sia  $[a]_m$  invertibile  $\Rightarrow \exists [b]_m \in \mathbb{Z}_m$  t.c.

$$[a]_m \cdot [b]_m = [1]_m \Rightarrow [ab]_m = [1]_m$$

$$\Rightarrow ab \equiv 1 \pmod{m}$$

$$\Rightarrow \exists k \in \mathbb{Z} \text{ t.c. } ab - 1 = km \Rightarrow 1 = ab + km$$

$$\Rightarrow 1 = \text{MCD}(a, m)$$

perché  $\forall t \in \mathbb{Z}$  t.c.  $t \mid a$  e  $t \mid m$ , da  $t \mid 1 \Rightarrow t=1$

( $\Leftarrow$ ) Sia  $\text{MCD}(a, m) = 1$ , allora

$$\mathbb{Z}_m = \{[0]_m, [1]_m, [2]_m, \dots, [m-1]_m\} =$$

$$= \{[0]_m, [a]_m, [2a]_m, \dots, [(m-1)a]_m\}$$

$\hookrightarrow$  Dimostrare su libro

$\Rightarrow$  All  $a_i \in \mathbb{F}_{q^m}$   $\exists k = 1, \dots, m$  to  $\underbrace{[ka]_m}_{\text{in } \mathbb{F}_{q^m}} = [1]_m$

$$[k]_m \cdot [e]_m = [1]_m$$

七

## Corolla Rib

$\mathbb{Z}_m$  é um campo  $\Leftrightarrow m$  é primo -

DEF - Siano  $(S, \sqcap) \in (\mathcal{T}, *)$  due strutture algebriche -

Il prodotto cartesiano  $S \times T$  è una struttura algebrica con  
operazione così definita:

$$(s_1, t_1) \sqsupseteq (s_2, t_2) = (s_1 \perp s_2, t_1 * t_2).$$

## PROPOSITIONE

$(S, +), (T, \times)$  sc.

- 1) Se  $\perp, *$  são associativa  $\Rightarrow \square$  é associativa
  - 2) Se  $+$ ,  $*$  // commutative  $\Rightarrow \square$  é commutativa
  - 3) Se  $e_S$  é elem. neutro em  $S$  e  $e_T$  é neutro em  $T$   $\Rightarrow (e_S, e_T)$  é elementos neutros em  $S \times T$

ii)  $\forall (s,t) \in S \times T$ , se  $s'$  è simmetrico di  $s$  e  $t' \parallel \parallel t$  }  $(s',t')$  è simmetrico per

$ESE H_{P,0} \quad (R, +)$

$$(\mathbb{R} \times \mathbb{R}, \sqsubseteq)$$

$$(a,b) + (c,d) = (a+c, b+d)$$

$$(a, b) \square (0, 0) = (a+0, b+0) = (a, b)$$

$$-(a, b) = (-a, -b)$$

$$(\mathbb{R}, +) \times (\mathbb{D}, \circ)$$

$$(a, b) \square (c, d) = (a+c, b \cdot d)$$

$(0, 1)$  è neutro

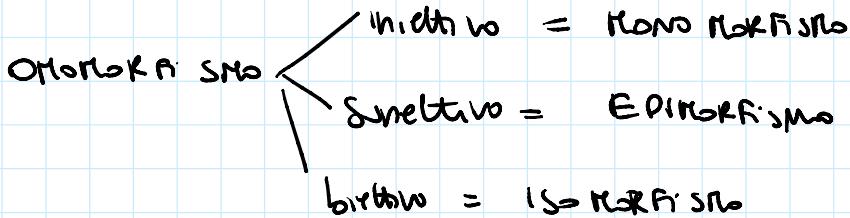
$$(-a, \frac{1}{b}) \quad b \neq 0$$

$(a, 0)$  non è simmetrico  $\forall a \in \mathbb{R}$

Def - Siano  $(S, +)$  e  $(T, *)$  strutture algebriche.

$f: S \rightarrow T$  è detta **OMOAFISMO** se  $\forall a, b \in S$

$$f(a + b) = f(a) * f(b) \Leftarrow$$



Esempio :  $f: (\mathbb{N}, +) \rightarrow (\mathbb{N}, \circ)$

$$n \mapsto 2^n$$

$$\forall n, m \in \mathbb{N} \quad \underbrace{f(n+m)}_{2^{n+m}} = \underbrace{f(n) \cdot f(m)}_{2^n \cdot 2^m} ? \quad \checkmark$$

$$f: (\mathbb{N}, \circ) \rightarrow (\mathbb{N}, +) \quad f(n) = 2^n$$

$$\forall n, m \in \mathbb{N} \quad f(nm) = f(n) + f(m)$$

$$2^{n \cdot m} = 2^n + 2^m \quad \text{FALSO}$$

Esercizio  $(\mathbb{Z}, +)$   $a \perp b = a+b-5$

$$f: (\mathbb{Z}, +) \rightarrow (\mathbb{Z}, +) \quad \text{vedere } f \text{ è Isomorfismo}$$

$$x \mapsto 5-x$$

$f : (\mathbb{Z}, +) \rightarrow (\mathbb{Z}, +)$  vedere  $f \in$  Isomorfismo  
 $x \mapsto 5-x$