INSIEMI con OPERAZIONI

Def.: sia S un insieme. Poniamo:

(1) $\forall\, n \in \mathbb{N}$, si dice operazione n-aria in S ogni funzione $S^n \longrightarrow S$, dove $S^n := \underbrace{S \times S \times \cdots \times S}_{n \text{ volte}}$

(2) se $n = 2$ ("operazione binaria")
e $* : S \times S \longrightarrow S$ è operazione binaria in S, scriveremo
$s_1 * s_2 := *(s_1, s_2) \quad \forall\, s_1, s_2 \in S$

(3) se $n = 0$ ("operazione nullaria") una operazione nullaria $\zeta : \{\bullet\} =: S^0 \longrightarrow S$ equivale alla scelta di un elemento in S
precisamente $\zeta(\bullet) = s_0 \in S$

Def.: (1) gruppoide := coppia $(S; *)$ in cui $*$ è operazione binaria nell'insieme S. In tal caso, si dice che:

(2) $*$ è associativa se
$\forall\, s', s'', s''' \in S$ si ha $(s' * s'') * s''' = s' * (s'' * s''')$ $\left(=: s' * s'' * s'''\right)$

(3) $*$ è commutativa se
$\forall\, s', s'' \in S$ si ha $s' * s'' = s'' * s'$

(4) un $\sigma \in S$ si dice elemento neutro se
$\forall\, s \in S$ si ha $s * \sigma = s$, $\sigma * s = s$

(5) se $(S; *)$ ha elemento neutro σ, allora
se $s \in S$ si dice inverso di s ogni elemento $s' \in S$
tale che $s * s' = \sigma$, $s' * s = \sigma$; se tale s' esiste,
allora s si dice invertibile.

NOTA – ESERCIZI: Sia $(S; *)$ un gruppoide. Allora:

(I) Se esiste un elemento neutro $\sigma \in S$, allora esso è unico

(II) Se $\exists$ elemento neutro $\sigma \in S$, allora σ è invertibile, con inverso σ stesso.

(III) Se $\exists$ elemento neutro $\sigma \in S$, e se $s \in S$ è invertibile, l'inverso s' di s è unico, indicato con s^{-1}.

$*$ è associativa

(CIOÈ: se $s', s'' \in S$ sono inversi di s, allora $s' = s''$)

INFATTI $\quad s * s' = \sigma \,, \quad s' * s = \sigma$

$\quad\quad s * s'' = \sigma \,, \quad s'' * s = \sigma$ $\Big\}\longrightarrow$

$$\longrightarrow \quad s' = s' * \sigma = s' * (s * s'') = (s' * s) * s'' = \sigma * s'' = s''$$

(IV) Se $\exists$ elemento neutro $\sigma \in S$, e $s \in S$ è invertibile, allora s^{-1} è anch'esso invertibile, con inverso

$$(s^{-1})^{-1} = s$$

TERMINOLOGIA:

- semigruppo := gruppoide associativo (cioè $*$ è associativa)
- monoide := semigruppo in cui $\exists$ (!) elemento neutro
- gruppo := monoide in cui ogni elemento sia invertibile
- un gruppoide / semigruppo / monoide / gruppo si dice commutativo (o abeliano) se la sua operazione è commutativa

OSSERVAZIONI: Sia $(S; *)$ un gruppoide. Allora:

(1) l'esistenza di un elemento neutro $\sigma \in S$ è equivalente all'esistenza di un'operazione 0-aria $\xi : \{\bullet\} =: S^0 \longrightarrow S$
$\bullet \longmapsto \xi(\bullet) = \sigma$

(2) se S è un gruppo, allora l'$\exists!$ inverso $s^{-1} \in S$, $\forall s \in S$ è equivalente ad una operazione 1-aria $i : S \longrightarrow S$
$s \longmapsto i(s) = s^{-1}$

ESERCIZIO: Sia $(M; *)$ un monoide e sia

$$U(M) := \{m \in M \mid \exists\, m^{-1} \in M\} = \{m \in M \mid m \text{ è invertibile}\} \quad (\subseteq M)$$

Dimostrare che:

(a) l'operazione $*$ di M si restringe ad una operazione $*$ di $U(M)$, cioè: $\forall\, u_1, u_2 \in U(M)$, si ha $u_1 * u_2 \in U(M)$

((SUGGER.: $\exists\, (u_1 * u_2)^{-1} = u_2^{-1} * u_1^{-1} \in M$))

(b) $(U(M); *)$ è un gruppo (con lo stesso elemento neutro di M)

ESEMPI: nel seguito

- $\mathbb{N} / \mathbb{Z} / \mathbb{Q}$:= numeri naturali / interi / razionali
- $\forall X \in \{\mathbb{N}, \mathbb{Z}, \mathbb{Q}\}$ poniamo

  $X_+ := \{x \in X / x > 0\}$, $X^* := X \setminus \{0\}$

  $+$ e $\cdot$ sono le operazioni "somma" e "prodotto"

  $\wedge$ e $\vee$ sono le operazioni "minimo" e "massimo"

- E un insieme, $S(E) := \{f \in E^E / f \text{ è invertibile}\} = \{\text{permutazioni di } E\}$

Consideriamo ora i seguenti gruppoidi, dove σ := elemento neutro:

$(\mathbb{N}_+; +)$ è semigruppo, non monoide (né gruppo), commutativo

$(\mathbb{N}; +)$ è monoide, non gruppo, commutativo, con $\sigma = 0$

$(\mathbb{N}_+; \cdot)$ è monoide, non gruppo, commutativo, con $\sigma = 1$

$(\mathbb{N}; \cdot)$ è monoide, non gruppo, commutativo, con $\sigma = 1$

$(\mathbb{N}; \vee)$ è monoide, non gruppo, commutativo, con $\sigma = 0$

$(\mathbb{N}_+; \vee)$ è semigruppo, non monoide (né gruppo), commutativo

$(\mathbb{N}; \wedge)$ è semigruppo, non monoide (né gruppo), commutativo

$(\mathbb{Z}; +)$ è gruppo, commutativo, con $\sigma = 0$

$(\mathbb{Z}; \cdot)$ è monoide, non gruppo, commutativo, con $\sigma = 1$

$(\mathbb{Z}^*; \cdot)$ è monoide, non gruppo, commutativo, con $\sigma = 1$

$(\mathbb{Q}; +)$ è gruppo, commutativo, con $\sigma = 0$

$(\mathbb{Q}_+; +)$ è semigruppo, non monoide (né gruppo), commutativo

$(\mathbb{Q}; \cdot)$ è monoide, non gruppo, commutativo, con $\sigma = 1$

$(\mathbb{Q}^*; \cdot)$ è gruppo, commutativo, con $\sigma = 1$

N.B.: $\mathbb{Q}^* = U(\mathbb{Q}; \cdot)$

$(\mathbb{Q}_+; \cdot)$ è gruppo, commutativo, con $\sigma = 1$

$(\mathcal{P}(E); \cap)$ è monoide, non gruppo, commutativo, con $\sigma = E$

$(\mathcal{P}(E); \cup)$ è monoide, non gruppo, commutativo, con $\sigma = \emptyset$

$(\mathcal{P}(E); \oplus)$ è gruppo, commutativo, con $\sigma = \emptyset$

N.B.: qui ogni $F \in \mathcal{P}(E)$ è inverso di sé stesso ...

$(E^E; \circ)$ è monoide, con $\sigma = id_E$; inoltre, posto $|E| :=$ num. di elem. di E

$|E| \leq 1 \Rightarrow (E^E; \circ)$ è gruppo, ed è commutativo

$|E| > 1 \Rightarrow (E^E; \circ)$ non è gruppo, e non è commutativo

$(\mathfrak{S}(E); \circ)$ è gruppo - infatti, $\mathfrak{S}(E) = \mathcal{U}(E^E)$ - e si ha

$(\mathfrak{S}(E); \circ)$ è commutativo $\iff |E| \leq 2$

ESEMPIO: **Linguaggio libero su un alfabeto**

A = insieme non vuoto (= "alfabeto"); "lettera" := elemento di A

$A^n := \underbrace{A \times \cdots \times A}_{n}$ $\forall n \in \mathbb{N}_+$, $A^0 := \{1\}$ "parola vuota"

$$L_A = A^* := \bigcup_{n \in \mathbb{N}} A^n = A^0 \cup A^1 \cup A^2 \cup \cdots \cup A^n \cup \cdots$$

si dice linguaggio libero su A

N.B.: ogni $(a_1, \ldots, a_n) \in A^n$ la scrivo anche $a_1 a_2 \ldots a_n$

"parola in A^* (o su A)" := elemento di A^*

1 = "parola vuota" = stringa nulla di lunghezza 0

$\forall\, p := a_1 a_2 \dots a_n \in A^n$, $\forall\, q := a'_1 a'_2 \dots a'_\ell \in A^\ell$ $(n, \ell \in \mathbb{N}_+)$

definisco giustapposizione di p con q la parola

$$p \cdot q := a_1 a_2 \dots a_n a'_1 a'_2 \dots a'_\ell \in A^{n+\ell} \quad (\subseteq A^*)$$

INOLTRE

$$p \cdot 1 := p, \qquad 1 \cdot p := p$$

$$1 \cdot 1 := 1$$

QUESTO definisce una operazione $A^* \times A^* \longrightarrow A^*$

ALLORA $(A^*; \cdot)$ è monoide, con elemento neutro $e = 1$

N.B.: (1) se $|A| \geq 1$, $\Rightarrow$ A^* non è commutativo

(2) $(A^*; \cdot)$ non è gruppo.