ALGEBRA 1 - 30/11/2020

Def.: (1) $\forall$ insieme S, una operazione in S è

$* : S \times S \longrightarrow S$. Scriviamo $s_1 * s_2 := *(s_1, s_2) \quad \forall s_1, s_2 \in S$.

(2) Gruppoide := una coppia $(S; *)$ con S insieme e $*$ operazione in S.

Def.: $\forall$ gruppoide $(S; *)$, si dice che:

(a) $*$ è associativa se $(s_1 * s_2) * s_3 = s_1 * (s_2 * s_3) \quad \forall s_1, s_2, s_3 \in S$

(b) $*$ è commutativa se $s_1 * s_2 = s_2 * s_1 \quad \forall s_1, s_2 \in S$

(c) $\sigma \in S$ si dice elemento neutro se $s * \sigma = s = \sigma * s \quad \forall s \in S$

(d) se $\exists$ in S un elemento neutro σ, un $s \in S$ si dice invertibile se $\exists\, s' \in S$ t.c. $s' * s = \sigma = s * s'$

tale s' si dice inverso di s, e si indica con s^{-1}.

NOTE: $\forall$ gruppoide $(S; *)$

(1) se $\exists\ \sigma \in S$ elemento neutro in S,
allora esso è unico

INFATTI se $\hat{\sigma} \in S$ è un altro elemento neutro,

allora $\sigma = \sigma * \hat{\sigma} = \hat{\sigma}$ (el. neutro; el. neutro)

(2) se $\exists\ \sigma \in S$ elemento neutro,
$\Rightarrow \sigma$ è invertibile, con inverso $\sigma^{-1} = \sigma$

(3) se $\exists\ \sigma \in S$ elemento neutro, $\forall\ s \in S$ invertibile si ha:

(3.1) l'inverso s'di s è invertibile, con inverso s stesso;

(3.2) se $*$ è associativa, allora l'inverso s'di s è unico

INFATTI se $s'' \in S$ è un altro inverso, allora

$$s'' = s'' * \sigma = s'' * (s * s') \overset{\text{ASSOCIATIVITÀ}}{=} (s'' * s) * s' = \sigma * s' = s'$$

Def.: (1) SEMIGRUPPO := gruppoide associativo

(2) MONOIDE := semigruppo in cui $\exists(!)$ elemento neutro

(3) GRUPPO := monoide in cui ogni elemento è invertibile

(4) un gruppoide (/semigruppo/monoide/gruppo) si dice commutativo – o "abeliano" – se la sua operazione è commutativa.

ESERCIZIO: **Hp:** $(M; *)$ è monoide

$U(M) := \{ m \in M \mid m \text{ è invertibile} \}$

Th: (a) $*$ si restringe a un'operazione in $U(M)$

((cioè $m_1 * m_2 \in U(M)$, $\forall m_1, m_2 \in U(M)$))

(b) $(U(M); *)$ è un gruppo

$\Leftarrow$ chiusa

$\exists (m_1 * m_2)^{-1} = ? * ?$

Def.: $\forall$ gruppoidi $(S;*)$, $(T;\bullet)$ si dice

(1) (omo)morfismo da $(S;*)$ a $(T;\bullet)$ ogni funzione $\varphi: S \longrightarrow T$ t.c. $\varphi(s_1 * s_2) = \varphi(s_1) \bullet \varphi(s_2)$ $\forall\, s_1, s_2 \in S$

cioè è "commutativo"

$$\begin{array}{ccc} S \times S & \xrightarrow{*} & S \\ {\scriptstyle \varphi\times\varphi}\downarrow & \circlearrowright & \downarrow{\scriptstyle \varphi} \\ T \times T & \xrightarrow[\bullet]{} & T \end{array} \qquad \varphi \circ * \;=\; \bullet \circ (\varphi \times \varphi)$$

(2) epimorfismo := morfismo surjettivo

(3) monomorfismo := morfismo iniettivo

(4) isomorfismo := morfismo invertibile, cioè $\exists\ \psi: T \longrightarrow S$ che è morfismo t.c. $\varphi \circ \psi = id_T$, $\psi \circ \varphi = id_S$

["iso" $\Leftrightarrow$ "epi" + "mono"]

N.B.: un morfismo φ è iso (morfismo) $\Longleftrightarrow$ φ è funzione invertibile

((vd. dopo))

(5) endomorfismo di $(S;*)$:= morfismo da $(S;*)$ a $(S;*)$

(6) automorfismo di $(S;*)$:= "(iso + endo) − morfismo"

(7) Si dice che $(S;*)$ è isomorfo a $(T;\bullet)$

se $\exists$ un isomorfismo da $(S;*)$ a $(T;\bullet)$

$\Longrightarrow$ si scrive $(S;*) \cong (T;\bullet)$, o $S \cong T$

(8) $End(S;*) := \{\text{endomorfismi di } (S;*)\}$

$Aut(S;*) := \{\text{automorfismi di } (S;*)\}$

PROPOSIZIONE: << morfismi tra loro >>

(1) $\forall$ gruppoide $(S;*)$, id_S è un automorfismo di $(S;*)$

(2) $\forall$ morfismi $S \xrightarrow{\varphi} T$, $T \xrightarrow{\chi} R$
la funzione $\chi \circ \varphi : S \longrightarrow R$ è un morfismo

(3) $\forall$ morfismo $\varphi : S \longrightarrow T$, si ha che
φ è <u>isomorfismo</u> $\Leftrightarrow$ la funzione φ è invertibile

(4) $\forall$ gruppoide S, si ha che
$(End(S); \circ)$ è un monoide,
$(Aut(S); \circ)$ è un gruppo

N.B.: si ha $Aut(S) = \mathcal{U}(End(S); \circ)$

Dim.: (1) BANALE...

(2) $\forall (S;*) \xrightarrow{\varphi} (T;\bullet),\ (T;\bullet) \xrightarrow{\chi} (R;\otimes) \Rightarrow \exists\, \chi\circ\varphi : (S;*) \longrightarrow (R;\otimes)$

Dimostriamo che $\chi\circ\varphi$ è morfismo: $\forall s_1, s_2 \in S$ si ha

$$(\chi\circ\varphi)(s_1 * s_2) := \chi\big(\varphi(s_1 * s_2)\big) \overset{\varphi \text{ è morfismo}}{=}$$

$$= \chi\big(\varphi(s_1)\bullet\varphi(s_2)\big) \overset{\chi \text{ è morfismo}}{=} \chi(\varphi(s_1)) \otimes \chi(\varphi(s_2)) =$$

$$= (\chi\circ\varphi)(s_1) \otimes (\chi\circ\varphi)(s_2) \Rightarrow \chi\circ\varphi \text{ è un morfismo!}$$

(3) $\Leftarrow$ $\varphi : S \longrightarrow T$ è <u>isomorfismo</u> $\Rightarrow$

$\Rightarrow \exists$ morfismo $\psi : T \longrightarrow S$ t.c.

$\psi\circ\varphi = id_S$ & $\varphi\circ\psi = id_T$ $\Rightarrow$

$\Rightarrow$ φ è funzione invertibile, con $\psi = \varphi^{-1}$

$\Leftarrow$ φ è funzione invertibile (ed è morfismo)

$\Rightarrow \exists\ \varphi^{-1}: T \longrightarrow S$ t.c. $\varphi^{-1} \circ \varphi = id_S$, $\varphi \circ \varphi^{-1} = id_T$

FATTO: Vale φ^{-1} è un morfismo

$\forall\ t_1, t_2 \in T$, $\varphi^{-1}(t_1 \bullet t_2) \overset{?}{=} \varphi^{-1}(t_1) * \varphi^{-1}(t_2)$

$\varphi(\varphi^{-1}(t_1 \bullet t_2)) = (\varphi \circ \varphi^{-1})(t_1 \bullet t_2) = t_1 \bullet t_2$

φ è morfismo

$\varphi(\varphi^{-1}(t_1) * \varphi^{-1}(t_2)) = \varphi(\varphi^{-1}(t_1)) \bullet \varphi(\varphi^{-1}(t_2)) =$

$= (\varphi \circ \varphi^{-1})(t_1) \bullet (\varphi \circ \varphi^{-1})(t_2) = t_1 \bullet t_2$

$\Rightarrow \varphi(\varphi^{-1}(t_1 \bullet t_2)) = \varphi(\varphi^{-1}(t_1) * \varphi^{-1}(t_2)) \Rightarrow$

$\Rightarrow \varphi^{-1}(t_1 \bullet t_2) = \varphi^{-1}(t_1) * \varphi^{-1}(t_2)$ ok

$\Rightarrow$ applico φ^{-1}

(4) Per $(End(S); \circ)$, sappiamo che $\circ$ è associativa, $\Rightarrow$ $(End(S); \circ)$ è un semigruppo

Inoltre, $id_S \in End(S)$ ed è elemento neutro per $\circ$ $\Big\}\rightarrow$ $(End(S); \circ)$ è un monoide

Per $(Aut(S); \circ)$, il risultato segue dal fatto che — per (3) — si ha

$$Aut(S) = U((End(S); \circ))$$

e quindi si applica l'ESERCIZIO di pagina 3. □

ESERCIZIO: la relazione $\cong$ tra gruppoidi è una equivalenza

PROPOSIZIONE:

Hp: $\varphi : (S;*) \longrightarrow (T;\cdot)$ è morfismo di gruppoidi

Th: (a) $(\varphi(S);\cdot)$ è un gruppoide

(b) S è commutativo $\Rightarrow$ $\varphi(S)$ è commutativo

(c) S è semigruppo $\Rightarrow$ $\varphi(S)$ è semigruppo

(d) S è monoide $\Rightarrow$ $\varphi(S)$ è monoide

(e) S è gruppo $\Rightarrow$ $\varphi(S)$ è gruppo

(f) S è monoide $\Rightarrow$ $\varphi(U(S)) \subseteq U(\varphi(S))$

Dim.: (1) Basta mostrare che

$\varphi(S)$ è "chiuso per $\cdot$", cioè

$\forall\ t_1, t_2 \in \varphi(S)$, si ha $t_1 \cdot t_2 \in \varphi(S)$

INFATTI $t_1 = \varphi(s_1)$, $t_2 = \varphi(s_2)$ con $s_1, s_2 \in S$

$$\Rightarrow \quad t_1 \cdot t_2 = \varphi(s_1) \cdot \varphi(s_2) = \varphi(\underbrace{s_1 * s_2}_{\in S}) \in \varphi(S)$$

ok

(3) $\forall\ t_i = \varphi(s_i) \in \varphi(S)$, $i = 1, 2, 3$

$$t_1 \cdot (t_2 \cdot t_3) = \varphi(s_1) \cdot (\varphi(s_2) \cdot \varphi(s_3)) = \varphi(s_1) \cdot \varphi(s_2 * s_3) = \varphi(s_1 * (s_2 * s_3))$$

$$(t_1 \cdot t_2) \cdot t_3 = (\varphi(s_1) \cdot \varphi(s_2)) \cdot \varphi(s_3) = \varphi(s_1 * s_2) \cdot \varphi(s_3) = \varphi((s_1 * s_2) * s_3)$$

$$\varphi\big(\; s_1 * (s_2 * s_3) = (s_1 * s_2) * s_3 \;\big)$$

$$\Downarrow$$

$$\varphi(s_1) \cdot \big(\varphi(s_2) \cdot \varphi(s_3)\big) = \big(\varphi(s_1) \cdot \varphi(s_2)\big) \cdot \varphi(s_3)$$

(2) Analogamente

$$s_1 * s_2 = s_2 * s_1 \xrightarrow{\varphi} \varphi(s_1) \cdot \varphi(s_2) = \varphi(s_2) \cdot \varphi(s_1)$$

$$\varphi(s_1 * s_2) = \varphi(s_2 * s_1)$$

(4) S è monoide, con elemento neutro 0 $\Rightarrow$

$\Rightarrow$ $\varphi(S)$ è monoide, con elemento neutro $\varphi(0)$

INFATTI $\forall\, s \in S$ si ha

$$\varphi(s)\cdot\varphi(\sigma) = \varphi(s*\sigma) = \varphi(s)$$

$$\varphi(\sigma)\cdot\varphi(s) = \varphi(\sigma*s) = \varphi(s)$$

$\rightarrow$ OK

(5) S è gruppo, con elemento neutro σ $\Rightarrow$

$\Rightarrow$ $\varphi(S)$ è monoide, con elemento neutro $\varphi(\sigma)$

ORA $\forall\, s \in S$, $\rightsquigarrow$ $\exists\ \varphi(s) \in \varphi(S)$

$\Rightarrow$ $\varphi(s)$ è invertibile, con inverso $\varphi(s^{-1})$:

$$\varphi(s)\cdot\varphi(s^{-1}) = \varphi(s*s^{-1}) = \varphi(\sigma)$$

$$\varphi(s^{-1})\cdot\varphi(s) = \varphi(s^{-1}*s) = \varphi(\sigma)$$

QUINDI $\exists\ \varphi(s^{-1}) = \varphi(s)^{-1}$ in $\varphi(S)$, q.e.d.

(6) S è monoide, con elemento neutro σ,

$\rightsquigarrow \exists \; U(S) := \{ s \in S \mid s \text{ è invertibile} \} =$

$= \{ s \in S \mid \exists\, s^{-1} \in S \} \Rightarrow$

$\Rightarrow \forall\, s \in U(S), \; \exists\, s^{-1} \in S \Rightarrow$

$\Rightarrow \exists\, \varphi(s^{-1}) \in \varphi(S)$, & (come per (5))

si ha che $\varphi(s^{-1})$ è inverso di $\varphi(s)$

QUINDI $\varphi(s) \in U(\varphi(S))$ $(\forall s \in U(S))$.

PERCIÒ $\varphi(U(S)) \subseteq U(\varphi(S))$, q.e.d. $\square$

N.B.: $\forall$ gruppoide $(S;*)$, $\exists$ la funzione

$$\lambda : S \longrightarrow S^S, \quad s \longmapsto \lambda(s) \left(\begin{array}{c} S \longrightarrow S \\ s' \longmapsto \lambda(s)(s') := s * s' \end{array} \right)$$

TEOREMA DI CAYLEY:

Hp: $(S;*)$ è un semigruppo.

Th: (a) $\lambda : S \longrightarrow S^S$ è un morfismo da $(S;*)$ a $(S^S;\circ)$

(b) se $(S;*)$ è un monoide, con elemento neutro e, allora λ in (a) è unitario, cioè $\lambda(e) = id_S$ & λ è iniettivo; in particolare, $(S;*)$ è isomorfo a $(\lambda(S);\circ)$

Dim.: (a) $\forall\, s_1, s_2 \in S$ si ha

$$\lambda(s_1 * s_2) = \lambda(s_1) \circ \lambda(s_2)$$

INFATTI $\forall\, s' \in S$, si ha

$$\lambda(s_1 * s_2)(s') := (s_1 * s_2) * s'$$

$$(\lambda(s_1) \circ \lambda(s_2))(s') := \lambda(s_1)(\lambda(s_2)(s')) =$$

$$= s_1 * (s_2 * s')$$

uguali perché $*$ è associativa

(b) $\forall\, s' \in S$, $\lambda(\sigma)(s') = \sigma * s' = s' = id_S(s') \Rightarrow$

$\Rightarrow \lambda(\sigma) = id_S$, q.e.d.

$\forall\, s_1, s_2 \in S$: $\lambda(s_1) = \lambda(s_2) \Rightarrow \lambda(s_1)(\sigma) = \lambda(s_2)(\sigma)$

$\Rightarrow s_1 = s_1 * \sigma = \lambda(s_1)(\sigma) = \lambda(s_2)(\sigma) = s_2 * \sigma = s_2$ □

ESEMPI 1:

N.B.: $X_+ := \{x \in X \mid x > 0\}$, $X^* := X \setminus \{0\}$

(1) $(\mathbb{N}; +)$ è monoide commutativo, NON gruppo

(2) $(\mathbb{N}_+; +)$ è semigruppo commutativo, NON monoide

(3) $(\mathbb{N}; \cdot)$ è monoide commutativo, NON gruppo

(4) $(\mathbb{N}_+; \cdot)$ è monoide commutativo, NON gruppo

(5) $(\mathbb{N}; \uparrow)$ è monoide commutativo, NON gruppo
con $a \uparrow b := \max_{\leq}\{a, b\}$ $\forall\, a, b \in \mathbb{N}$

(6) $(\mathbb{N}; \downarrow)$ è semigruppo commutativo, NON monoide
con $a \downarrow b := \min_{\leq}\{a, b\}$ $\forall\, a, b \in \mathbb{N}$

(7) $(\mathbb{N}; \wedge)$ è monoide commutativo, NON gruppo
con $a \wedge b := MCD(a, b)$ $\forall\, a, b \in \mathbb{N}$

(7) $(\mathbb{N}; \vee)$ è monoide commutativo, NON gruppo
con $a \vee b := mcm(a, b)$ $\forall\, a, b \in \mathbb{N}$

(8) $(\mathbb{Z}; +)$ è gruppo commutativo

(9) $(\mathbb{Z}; \cdot)$ è monoide commutativo, NON gruppo

(10) $(\mathbb{Z}_n; +)$ è gruppo commutativo, $\forall n \in \mathbb{N}$

(11) $(\mathbb{Z}_n; \cdot)$ è monoide commutativo, NON gruppo, $\forall n \in \mathbb{N}$

(12) $(\mathbb{Z}; -)$ è gruppoide, NON semigruppo e NON commutativo

(13) $(\mathbb{Q}; +)$ è gruppo commutativo

(14) $(\mathbb{Q}; \cdot)$ è monoide commutativo, NON gruppo

(15) $(\mathbb{Q}^*; \cdot)$ è gruppo commutativo

(16) $(\mathbb{Q}_+; \cdot)$ è gruppo commutativo

MEMO $\forall$ insieme E, $\exists\ \mathcal{P}(E) := \{ E' \mid E' \subseteq E \}$

$$\mathcal{R}(E) := \mathcal{P}(E \times E) = \{ \phi \mid \phi : E \dashrightarrow E \}$$

$$E^E := \{ f \mid f : E \longrightarrow E \}, \quad \mathfrak{S}(E) := \{ \sigma \mid \sigma : E \rightarrowtail E \}$$

(17) $(\mathcal{P}(E); \cup)$ è monoide commutativo, NON gruppo

(18) $(\mathcal{P}(E); \cap)$ è monoide commutativo, NON gruppo

(19) $(\mathcal{P}(E); \Delta)$ è gruppo commutativo $F^{-1} = F$, $F \Delta F = \emptyset$

(20) $(\mathcal{P}(E); \setminus)$ è gruppoide, NON semigruppo e NON commutativo $(\forall\ E \neq \emptyset)$

(21) $(\mathcal{R}(E); \circ)$ è monoide, NON gruppo, NON comm. $(\forall\ E \neq \emptyset)$

(22) $(E^E; \circ)$ è $\begin{cases} \text{monoide, NON gruppo, NON comm.} & \forall\ |E| > 1 \\ \text{gruppo commutativo,} & \forall\ |E| \leq 1 \end{cases}$

(23) $(\mathfrak{S}(E); \circ)$ è gruppo $(\text{commutativo} \Leftrightarrow |E| \leq 1)$

N.B.: è $\mathfrak{S}(E) = \mathcal{U}(E^E)$

ESEMPI 2 - MORFISMI :

① $\mathbb{Z} \xrightarrow{\pi_n} \mathbb{Z}_n$, $z \longmapsto [z]_n$ $\forall z \in \mathbb{Z}$ $(\forall n \in \mathbb{N})$

è un epimorfismo sia $(\mathbb{Z}; +)$ a $(\mathbb{Z}_n; +)$ e sia $(\mathbb{Z}; \cdot)$ a $(\mathbb{Z}_n; \cdot)$

② $(\mathcal{P}(E); \cup) \longrightarrow (\mathcal{P}(E); \cap)$, $E' \longmapsto \complement_E(E')$

è un isomorfismo, con inverso $(\mathcal{P}(E); \cap) \longrightarrow (\mathcal{P}(E); \cup)$
$E'' \longmapsto \complement_E(E'')$

QUINDI $(\mathcal{P}(E); \cup) \cong (\mathcal{P}(E); \cap)$

③ $(\mathbb{N}; \vee) \xrightarrow{\ell} (\mathcal{P}(\mathbb{N}); \cap)$, $n \longmapsto \ell(n) := n \cdot \mathbb{N} = \{nk \mid k \in \mathbb{N}\}$

è un monomorfismo unitario di monoidi

(4) **Potenze:** $\forall$ semigruppo $(S;*)$, $\forall\, s \in S$ definiamo

[B] $s^1 := s$ $(n=1)$ [PI] $s^n := s * s^{n-1}$ $(= s^{n-1} * s)$, $\forall\, n \in \mathbb{N} : n > 1$

Inoltre: se $(S;*)$ è monoide, con elemento neutro e_S, si pone

[0] $s^0 := e_S$ [<0] $s^{-n} := (s^{-1})^n$ $\forall\, n \in \mathbb{N}$, $\forall\, s \in U(S)$

Allora: (1) $\forall$ semigruppo $(S;*)$, $\forall\, s \in S$,

$$\rho_s : (\mathbb{N}_+; +) \longrightarrow (S;*) \quad \text{è morfismo di semigruppi}$$
$$n \longmapsto \rho_s(n) := s^n$$

(2) $\forall$ monoide $(S;*)$, $\forall\, s \in S$, ρ_s si estende a

$$\rho_s^0 : (\mathbb{N}; +) \longrightarrow (S;*), \quad n \longmapsto \rho_s^0(n) := s^n$$

che è morfismo unitario di monoidi

(3) $\forall$ monoide $(S;*)$, $\forall\, s \in U(S)$, ρ_s^0 induce

$$\rho_s^G : (\mathbb{Z}; +) \longrightarrow (U(S);*), \quad z \longmapsto \rho_s^G(z) := s^z$$

che è morfismo di gruppi.

(5) $\forall$ insieme E, $\forall F \in \mathcal{P}(E)$, la funzione

$$\phi_F : \mathcal{P}(E) \longrightarrow \mathcal{P}(E), \quad E' \longmapsto \phi_F(E') := E' \cap F$$

è un endomorfismo di $(\mathcal{P}(E); \cap)$ e di $(\mathcal{P}(E); \cup)$

Analogamente, la funzione

$$\phi^F : \mathcal{P}(E) \longrightarrow \mathcal{P}(E), \quad E' \longmapsto \phi^F(E') := E' \cup F$$

è un endomorfismo di $(\mathcal{P}(E); \cap)$ e di $(\mathcal{P}(E); \cup)$