

ALGEBRA 1 - 04/12/2020

POTENZE: $\forall$ semigrups $(S; *)$, $\forall s \in S$ definiamo

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

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

$$\boxed{\circledast} \quad s^0 := \ell_s \quad \boxed{<0} \quad s^{-n} := (s^{-1})^n \quad \forall n \in \mathbb{N}, \quad \forall s \in \mathcal{U}(S)$$

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

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

$\Rightarrow$ valgono le regole delle potenze: $s^{a+b} = s^a * s^b$, $(s^a)^c = s^{a*c}$

(2) A moniale $(S; *)$, $\forall s \in S$, p_s n'est étendu à

$$P_S^0 = (N; +) \longrightarrow (S; *), \quad n \longmapsto P_S^0(n) := s^n$$

che è morfismo unitario di monoidi ($p_s^0(\emptyset) = e_s$)

(3) $\forall$ monioide $(S; *)$, $\forall s \in U(S)$, p_s^* induce il morfismo

$$P_\lambda^G: (\mathbb{Z}_\lambda; +) \longrightarrow (U(1); *), \quad z \longmapsto P_\lambda^G(z) := \lambda^z$$

NOTAZIONE $\forall$ gruppo G , indichiamo

- | | |
|--|---|
| (a) l'operazione con $(x, y) \mapsto xy$ | (d) $X^{-1} := \{x^{-1} \mid x \in X\}$
$\forall X \subseteq G$ |
| (b) l'elemento neutro con 1_G , o 1 | (e) $X \cdot Y := \{xy \mid x \in X, y \in Y\}$
$\forall X, Y \subseteq G$ |
| (c) l'inverso di $g \in G$ con g^{-1} | |

Def. 1: $\forall$ gruppo G , si dice sottogruppo di G , e si scrive $H \leq G$, ogni sottoinsieme H di G tale che H sia gruppo per la restrizione ad H stesso della operazione di G . QUESTO EQUIVALE A

(1) $H \cdot H \subseteq H$ (cioè $h_1 h_2 \in H, \forall h_1, h_2 \in H$)

(2) $1_G \in H$

(3) $H^{-1} \subseteq H$ (cioè $h^{-1} \in H, \forall h \in H$)

ESEMPIO 2: $H := G$ e $H = \{1_G\}$ sono sottogruppi,
detti banali

PROPOSIZIONE 3: [Hp: G è gruppo, $H \subseteq G$

[Th: $H \leq G \iff$

① $H \neq \emptyset$ & $H^{-1} \cdot H \subseteq H$

② $H \neq \emptyset$ & $H \cdot H^{-1} \subseteq H$

Dim.:

(①) $H \leq G \Rightarrow H \ni 1_G \Rightarrow H \neq \emptyset$

$\iff H \ni H \cdot H \supseteq H^{-1} \cdot H \Rightarrow H^{-1} \cdot H \subseteq H$

$H \ni H^{-1} \xrightarrow{\text{VI}} H^{-1} \xrightarrow{\text{VI}} H^{-1} \xrightarrow{\text{VI}} H \ni H \cdot H^{-1}$ (ok)

(②) analogo

$$(\Leftarrow^{\textcircled{1}}) \quad H \neq \emptyset \Rightarrow \exists h_0 \in H \Rightarrow H \supseteq H^{-1} \cdot H$$

$$\forall h \in H$$

$$(2) \quad \boxed{1 \in H} \Leftrightarrow h_0^{-1} \cdot h_0 = 1$$

$$H \supseteq H^{-1} \cdot H \ni h^{-1} \cdot 1 = h^{-1} \Rightarrow h^{-1} \in H, \forall h \in H$$

$$\forall h_1, h_2 \in H$$

$$\text{cioè } \boxed{H^{-1} \subseteq H} \quad (3)$$

$$\boxed{h_1 \cdot h_2 = (h_1^{-1})^{-1} \cdot h_2 \in H^{-1} \cdot H \subseteq H} \rightarrow$$

$$h_1 \in H \Rightarrow h_1^{-1} \in H \Rightarrow (h_1^{-1})^{-1} \in H^{-1} \quad h_1 \cdot h_2 \in H$$

$$(1) \quad \boxed{H \cdot H \subseteq H}$$

$$(\Leftarrow^{\textcircled{2}}) \quad \text{La dimostrazione è analoga!}$$

□

ESEMPLI / CONTROESEMPLI 4:

$$\textcircled{1} \quad G := (\mathbb{Z}; +) \Rightarrow d\mathbb{Z} := \{dz \mid z \in \mathbb{Z}\} \leq \mathbb{Z}, \forall d \in \mathbb{Z}$$

$$\Leftrightarrow (d\mathbb{Z} + 1) \not\leq \mathbb{Z} \quad \text{se } d \notin \{1, -1\}$$

$$\textcircled{2} \quad G := (S(E); \circ), \quad F \subseteq E$$

$$H_F := \{ \sigma \in S(E) \mid \sigma(F) = F \} \Rightarrow H_F \leq S(E)$$

$$K_F := \{ \nu \in S(E) \mid \nu(F) \subseteq F \} \Rightarrow K_F \not\leq S(E)$$

(in generale)

P.es., per $E := \mathbb{R}, F := [-1, +1]$

$$\nu: \mathbb{R} \rightarrow \mathbb{R}, x \mapsto 3^{-1} \cdot x \Rightarrow \nu \in S(E)$$

$$\nu([-1, +1]) = [-3^{-1}, +3^{-1}] \subseteq [-1, +1] \Rightarrow \nu \in K_F$$

MA $\nu^{-1}: \mathbb{R} \rightarrow \mathbb{R} \Rightarrow \nu^{-1}([-1, +1]) = [-3, +3] \not\subseteq [-1, +1]$

$y \mapsto 3 \cdot y$ QUINDI $\nu^{-1} \in K_F$

③ $\forall$ ~~gruppoide~~ $\Gamma \mapsto \exists$ gruppo $(\text{Aut}(\Gamma); \circ)$

$\exists$ gruppo $(\mathcal{S}(\Gamma); \circ) \rightarrow \boxed{\text{Aut}(\Gamma) \leq \mathcal{S}(\Gamma)}$

④ $\forall$ gruppo G , n -ha $Z(G) \leq G$, dove

$\text{CENTRO di } G = Z(G) := \{z \in G \mid z \cdot g = g \cdot z, \forall g \in G\}$

⑤ $\forall$ gruppo G , $\forall g \in G$, n -ha $C_G(g) \leq G$, dove

$\text{CENTRALIZZATORE di } g \text{ in } G = C_G(g) := \{g \in G \mid g \cdot g = g \cdot g\}$

$$\boxed{\text{N.B.:}} \bigcap_{g \in G} C_G(g) = Z(G)$$

NOTA: in generale, $\forall$ gruppo G ,

$H_i \leq G, \forall i \in I \not\Rightarrow \bigcup_{i \in I} H_i \leq G$

Esempio: $G = (\mathbb{Z}; +)$,

$H_1 = 3\mathbb{Z}, H_2 = 5\mathbb{Z}$

MA $H_1 \cup H_2 \not\leq \mathbb{Z}$

Lemma 5: $\forall$ famiglia $\{H_i\}_{i \in I}$ di sottogruppi di un gruppo G , si ha che anche $\bigcap_{i \in I} H_i$ è sottogruppo.

Dim.: (2) $H_i \leq G, \forall i \in I \Rightarrow 1 \in H_i, \forall i \in I$

$$(1) \forall h', h'' \in \bigcap_{i \in I} H_i \Rightarrow h', h'' \in H_i \quad \forall i \in I$$

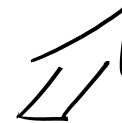
$$\text{OK} \quad h' \cdot h'' \in \bigcap_{i \in I} H_i$$



$$(h' \cdot h'') \in H_i \cdot H_i \subseteq H_i, \forall i \in I$$

$$1 \in \bigcap_{i \in I} H_i \quad \text{OK}$$

$$h^{-1} \in \bigcap_{i \in I} H_i$$



$$(3) \forall h \in \bigcup_{i \in I} H_i \Rightarrow h \in H_i \Rightarrow h^{-1} \in H_i \quad \forall i \in I$$

Def. 6: $\forall$ gruppo, $\forall Y \subseteq G$ si dice

SOTTOGRUPPO (di G) GENERATO da Y

il sottogruppo $\langle Y \rangle$ di G che contenga Y
e sia minimo (per questa proprietà) rispetto a $\subseteq$,

Cioè ① $\langle Y \rangle \leq G$

② $\langle Y \rangle \supseteq Y$

③ $\forall H \leq G : H \supseteq Y, \Rightarrow H \supseteq \langle Y \rangle$

IN BREVE

$$\langle Y \rangle := \min_{\subseteq} \{ H \in \mathcal{P}(G) \mid H \leq G, H \supseteq Y \}$$

NOTA: essendo un minimo, tale $\langle Y \rangle$,
se esiste, è unico.

PROPOSIZIONE 7: $[Hp:]$ G è gruppo, $Y \subseteq G$.

$[Th:]$ $\langle Y \rangle$ esiste, ed è dato da

$$\langle Y \rangle \stackrel{①}{=} \bigcap_{\substack{H \leq G \\ H \supseteq Y}} H \quad \& \quad H \stackrel{②}{=} \left\{ y_1 \dots y_s \mid \begin{array}{l} s \in \mathbb{N}, y_i \in (Y \cup Y^{-1}) \\ \forall i=1, \dots, s \end{array} \right\}$$

Dim.: ① Sia $H_0 := \bigcap_{\substack{H \leq G \\ H \supseteq Y}} H$; $\Rightarrow$ tale H_0 è una

intersezione di sottogruppi $\Rightarrow$ per il Lemma 5,

H_0 è sottogruppo di G ; $\Rightarrow$ $H_0 \leq G$, $H_0 \supseteq Y$ e

$$\forall H \leq G : H \supseteq Y \Rightarrow H_0 \leq H$$

(perché H è uno dei sottogruppi in " $\cap$ ")

H_0 ha le 3 proprietà che definiscono $\langle Y \rangle$

QUINDI

$$H_0 = \langle Y \rangle$$

OK

② Sia $H_- := \left\{ y_1 \cdots y_s \mid s \in \mathbb{N}, y_i \in (Y \cup Y^{-1}) \right\}$
 $\forall i=1, \dots, s$

ALLORA: [I] $H_- \geq Y$, perché ogni $y \in Y$ è un prodotto di tipo $*$ con $s=1$

[II] $\forall H \leq G$ k.c. $H \geq Y$ si ha $H \geq H_-$, perché

$$\begin{aligned} \left. \begin{array}{l} H \geq Y \\ H \geq H^{-1} \end{array} \right\} &\Rightarrow H \geq (Y \cup Y^{-1}) \\ &\Rightarrow H \geq y_1 \cdots y_s \text{ con } y_1, \dots, y_s \in (Y \cup Y^{-1}) \\ H \geq H \cdot H &\Rightarrow H \geq \underbrace{H \cdot H \cdots H}_s \end{aligned}$$

$H \geq H_-$ OK

[III] $H_- \leq G$, perché

$H_- \geq 1$ $\because$ prodotto di $s=0$ fattori

$H_- \supseteq H_- \cdot H_-$, perché

$$\begin{array}{l} H_- \ni y'_1 \cdots y'_{s'} \\ H_- \ni y''_1 \cdots y''_{s''} \end{array} \mapsto y'_1 \cdots y'_{s'} y''_1 \cdots y''_{s''} \in H_- \quad \text{OK}$$

$\nwarrow \quad \uparrow \quad \uparrow \quad \nearrow$
 $(Y \cup Y^{-1})$

$H_- \supseteq H_-^{-1}$, perché

$$H_- \ni y_1 \cdots y_s \Rightarrow (y_1 \cdots y_s)^{-1} = y_s^{-1} \cdots y_1^{-1} \in H_-$$

$\nwarrow \quad \uparrow$
 $Y \cup Y^{-1}$

$(Y^{-1} \cup Y)$
 $\swarrow \quad \searrow$

QUINDI $\boxed{\text{I}} + \boxed{\text{II}} + \boxed{\text{III}} \Rightarrow H_-$ ha le proprietà che
 definiscono $\langle Y \rangle \Rightarrow H_- = \langle Y \rangle$, q.e.d. $\square$

Def. 8: (SOTTO)GRUPPI CICLICI

$\forall$ gruppo G , un sottogruppo H di G (in particolare, G stesso, se $H=G$) si dice ciclico se può essere generato con un singolo elemento
 $e \neq e^{-1}$

$$\text{se } \exists h \in H : H = \langle \{h\} \rangle =: \langle h \rangle$$

ESEMPLI 9: ① $G := (\mathbb{Z}; +)$, $H := \{z \in \mathbb{Z} \mid z \text{ è pari}\}$

$$\Rightarrow G \text{ è ciclico, } G = \langle +1 \rangle = \langle -1 \rangle$$

$$\& H \text{ è ciclico, } H = \langle +2 \rangle = \langle -2 \rangle$$

$$\textcircled{2} \forall n \in \mathbb{N}, G := (\mathbb{Z}_n; +) \text{ è ciclico,}$$

$$\text{con } G = \langle +\bar{1} \rangle = \langle -\bar{1} \rangle$$

③ $(U(\mathbb{Z}_7); \cdot)$ è ciclico, con

$$U(\mathbb{Z}_7) = \langle \bar{3} \rangle = \langle \bar{5} \rangle$$

INVECE $\langle \bar{2} \rangle = \{\bar{1}, \bar{2}, \bar{4}\} \subsetneq U(\mathbb{Z}_7)$

con $\bar{2}$ non è generatore di $(U(\mathbb{Z}_7); \cdot)$

④ $(U(\mathbb{Z}_8); \cdot)$ NON è ciclico.

⑤ $(S(\underline{3}); \circ)$ NON è ciclico.

$\underline{3} := \{0, 1, 2\}$

PROPOSIZIONE 10: G è gruppo ciclico, $G = \langle g \rangle$

Th: (a) $G = \{ g^z \mid z \in \mathbb{Z} \}$

(b) G è commutativo

(c) $|G| \in \mathbb{N}_+$ oppure $|G| = \infty =: |\mathbb{N}|$

(d) $G = \langle g^{-1} \rangle$, cioè anche g^{-1} genera G .

Dim.:

Esiste funzione

$$p_g: (\mathbb{Z}; +) \longrightarrow (G; \cdot), \quad z \longmapsto g^z$$

che è morfismo di gruppi.

allora $G = \langle g \rangle \Rightarrow \text{Im}(p_g) = \langle g \rangle = G$

$$\{ g^z \mid z \in \mathbb{Z} \}$$

vale (a)

OK

(b) VERA, perché

$$g^{z'} \cdot g^{z''} = g^{z'+z''} = g^{z''+z'} = g^{z''} \cdot g^{z'}$$
$$\forall z', z'' \in \mathbb{Z}$$

$$(c) \quad G = \langle g \rangle = \{ g^z \mid z \in \mathbb{Z} \} = \text{Im}(p_g) \Rightarrow$$

$$\Rightarrow |G| = |\text{Im}(p_g)| \leq |\mathbb{Z}| = \aleph_0$$

$$(d) \quad G = \langle g \rangle = \{ g^z \mid z \in \mathbb{Z} \} =$$
$$= \{ (g^{-1})^{-z} \mid z \in \mathbb{Z} \} =$$

$$= \{ (g^{-1})^z \mid z \in \mathbb{Z} \} = \langle g^{-1} \rangle$$

sfruttando l'identità $g^z = (g^{-1})^{-z}$, $\forall z \in \mathbb{Z}$. $\square$

Def. 11: $\forall$ gruppo G , $\forall g \in G$, poniamo:

(a) ORDINE di $G := |G| \stackrel{\Delta}{=} \omega(G)$

(b) $E_g := \{e \in \mathbb{N}_+ \mid g^e = 1\} = \{\text{esponenti di } g\}$

(c) $\omega(g) = \text{ordine di } g := \begin{cases} +\infty, & \text{se } E_g = \emptyset \\ \min(E_g), & \text{se } E_g \neq \emptyset \end{cases}$

Lemma 12: [Hp:] G gruppo, $g \in G : \omega(g) \in \mathbb{N}_+$

[Th:] $\forall z \in \mathbb{Z}, \quad g^z = 1 \iff \omega(g) \mid z$

QUINDI

$$E_g = \omega(g) \cdot \mathbb{N}_+$$

Dim.: Operando la divisione con resto (in $\mathbb{Z}$)

di z per $\omega(g)$ si trovano $q, r \in \mathbb{Z}$

K.L. $z = \omega(g) \cdot q + r$, con $0 \leq r < \omega(g)$

ORA

$$g^z = g^{\omega(g) \cdot q + r} = (g^{\omega(g)})^q \cdot g^r = 1^q \cdot g^r = g^r$$

$\parallel$
1

MA

$$g^z = 1 \Rightarrow g^r = 1 \quad \text{con } 0 \leq r < \omega(g)$$

$r = 0$ $\leftarrow r \leq \min(E_g)$

$\Downarrow$

$$z = \omega(g) \cdot q \Rightarrow \omega(g) \mid z, \text{ q.e.d.} \quad \square$$

TEOREMA 13

[Hp]: G gruppo, $g \in G$.

[Th]: (a) $p_g: (\mathbb{Z}; +) \rightarrow (G; \cdot)$, $z \mapsto g^z$, è morfismo

(b) $\text{Im}(p_g) = \langle g \rangle$

(c) Il Teorema Fondamentale di Omomorfismo per gruppi ci dà un isomorfismo (di gruppi)

$$p_{g*}: \left(\frac{\mathbb{Z}}{\rho_{p_g}}; \oplus \right) \xrightarrow{\cong} \text{Im}(p_g) = \langle g \rangle$$

$$[z]_{\rho_{p_g}} \mapsto p_g(z) = g^z$$

per il quale si ha:

(c.1) $\omega(g) = +\infty \iff \rho_{p_g} = \text{id}_{\mathbb{Z}} \iff p_{g*}: \mathbb{Z} \cong \langle g \rangle$

(c.2) $\omega(g) \in \mathbb{N}_+ \iff \rho_{p_g} = \equiv_{\omega(g)} \iff p_{g*}: \mathbb{Z}_{\omega(g)} \cong \langle g \rangle$

In particolare, $\omega(\langle g \rangle) = \omega(g)$

con

$$\langle g \rangle = \begin{cases} \{g^z \mid z \in \mathbb{Z}\} & \text{se } \omega(g) = +\infty \\ \{1, g^1, g^2, \dots, g^{\omega(g)-1}\} & \text{se } \omega(g) \in \mathbb{N}_+ \end{cases}$$

tutti elementi diversi

$\omega(g)$ elementi diversi

Dim.:

(a) & (b) on (già dimostrate)

(c) $\forall z', z'' \in \mathbb{Z}$ si ha

$$z' \rho_g z'' \stackrel{\Delta}{\iff} p_g(z') = p_g(z'') \iff g^{z'} = g^{z''} \iff$$

$$\iff g^{z'} \cdot (g^{z''})^{-1} = g^{z''} \cdot (g^{z''})^{-1} \iff g^{z'-z''} = 1$$

$//$
 $g^{z'-z''}$

$//$
 1

*

1° caso: $\omega(g) = +\infty$ Da $\circledast$ segue $\left\{ \begin{array}{l} g^{|z'-z''|} = 1 \\ |z'-z''| \in \mathbb{N} \end{array} \right.$

$$z' = z''$$

QUINDI

$$z' \rho_{p_g} z'' \iff z' = z''$$

q.e.d.

2° caso: $\omega(g) \in \mathbb{N}_+$ (per il Lemma 12)

Ora, $\circledast \quad g^{z'-z''} = 1 \iff \omega(g) \mid (z'-z'')$

QUINDI in conclusione



$$z' \equiv_{\omega(g)} z''$$

$$z' \rho_{p_g} z'' \iff z' \equiv_{\omega(g)} z''$$

q.e.d.

□

COROLLARIO 14

Le classi di isomorfismo dei gruppi ciclici sono in biiezione con $\mathbb{N}$, mediante

$$\begin{array}{ccc} \mathbb{Z}^c / \cong & \xrightarrow{\phi} & \mathbb{N} \\ & & \downarrow \\ [G = \langle g \rangle]_{\cong} & \mapsto & \begin{cases} \omega(G) = \omega(g) & \text{se } \omega(G) \in \mathbb{N}_+ \\ \emptyset & \text{se } \omega(G) = +\infty \end{cases} \end{array}$$

con inversa

$$\begin{array}{ccc} \mathbb{N} & \xrightarrow{\psi} & \mathbb{Z}^c / \cong \\ (\forall n > 0) & n \mapsto & [(\mathbb{Z}_n; +)]_{\cong} \\ & 0 \mapsto & [(\mathbb{Z}_1; +)]_{\cong} \end{array}$$