GRUPPI (II PARTE)

Abbiamo indicato un gruppo con $(G,*,e)$. A volte si scrive solo $(G,*)$

Si usa abitualmente la notazione moltiplicativa: $g^3 = g*g*g \quad (g\in G)$

Ma in alcuni casi si usa anche l'additiva: es. $(\mathbb{Z},+,0)$ $\quad 3+5 \quad$ $n\cdot x = \underbrace{x+x+x+\ldots+x}_{n \text{ volte}}$

(in questa notazione le potenze di un elemento sono in realtà i suoi multipli)

<u>Osservazione</u>: i concetti di elemento neutro e inverso sono di per sé asimmetrici (se l'operazione non è commutativa). Si può parlare di el. neutro e di inverso "a sinistra" o "a destra".

Quando si dice "elemento neutro" si intende che la proprietà vale da entrambi i lati.

" " "inverso" " " "

<u>Es.</u> $(\mathbb{Z},-)$ ha elemento neutro <u>a destra</u>: 0. Infatti $\forall x\in\mathbb{Z}\quad x-0=x$

Ma 0 non è el. neutro a sinistra: $0-x\neq x$.

In $(\mathcal{F}_{\mathbb{Z}},\circ)$ $\quad f:\mathbb{Z}\longrightarrow\mathbb{Z}$, $n\longmapsto 2n$ ha <u>inverso sinistro</u>: $g:\mathbb{Z}\longrightarrow\mathbb{Z}$

$$n \longmapsto \begin{cases} n/2 & \text{se } n \text{ pari} \\ 0 & \text{se } n \text{ dispari} \end{cases}$$

tutte le funzioni $\mathbb{Z}\to\mathbb{Z}$

composizione

$$g\circ f = id_{\mathbb{Z}}$$
$$f\circ g \neq id_{\mathbb{Z}}$$

Prop: Sia $(G,*)$ insieme con un'operazione binaria.

1) Se esiste un elemento neutro per $*$, allora è unico.

Se in più $(G,*,e)$ è un monoide

2) Se $g \in G$ ha inverso, allora l'inverso è unico
3) Se $g,h \in G$ hanno inversi, allora $(g*h)^{-1} = h^{-1} * g^{-1}$
4) Se $g \in G$ ha inverso, allora $\forall h_1, h_2 \in G$: i) $g*h_1 = g*h_2 \iff h_1 = h_2$ leggi di cancellazione
   ii) $h_1 * g = h_2 * g \iff h_1 = h_2$

dim: 1) Siano e, e' due elementi neutri: $e \underset{\substack{\uparrow \\ \text{perché } e' \\ \text{è neutro}}}{=} e * e' \underset{\substack{\uparrow \\ \text{perché } e \\ \text{è neutro}}}{=} e'$.

2) Siano h, h' due inversi di g, cioè $g*h = h*g = e$, $g*h' = h'*g = e$

Allora $h = h*e = h*(g*h') \underset{\substack{\uparrow \\ \text{associatività}}}{=} (h*g)*h' = e*h' = h'$

3) $(h^{-1}*g^{-1})*(g*h) = h^{-1}*(g^{-1}*(g*h)) = h^{-1}*((g^{-1}*g)*h) = h^{-1}*(e*h) = h^{-1}*h = e$

$(g*h)*(h^{-1}*g) = \ldots = e$ in modo analogo.

4) i) $g * h_1 = g * h_2 \overset{?}{\Rightarrow} h_1 = h_2$

$g * h_1 = g * h_2 \Rightarrow g^{-1} * (g * h_1) = g^{-1} * (g * h_2) \Rightarrow (g^{-1} * g) * h_1 = (g^{-1} * g) * h_2$

$\Rightarrow e * h_1 = e * h_2 \Rightarrow h_1 = h_2$.

ii) analoga.

Corollario: Se $(G, *, e)$ è un gruppo, le proprietà 2), 3), 4) valgono $\forall g, h \in G$.

Es: Principio di equivalenza delle equazioni in $\mathbb{R}$:
"moltiplicando o dividendo ambo i membri di un'equazione per una stessa quantità $\neq 0$ si ottiene un'equazione equivalente a quella data".
Questo vale perché $(\mathbb{R}^\times = \mathbb{R} - \{0\}, \cdot, 1)$ è un gruppo $\Rightarrow$ valgono le leggi di cancellazione.

Sottogruppi

Def: Sia $(G, *, e)$ è un gruppo. Un sottogruppo H di G è un sottoinsieme $H \subseteq G$ tale che $(H, *, e)$ è un gruppo. In tal caso scriviamo: $H \leq G$

Concretamente: 1) $e \in H$, in particolare $H \neq \emptyset$.
2) $\forall h, h' \in H$, allora $h * h' \in H$ (cioè H è chiuso rispetto a $*$)
3) $\forall h \in H$, $h^{-1} \in H$. (h^{-1} esiste in G)

Non esempi: 1) $(\mathbb{Z},+,0)$ $\quad S=\{1,2,3\}$ non è un sottogruppo, perché $0 \notin S$.
$\mathbb{Z} \setminus \{0\}$ " per lo stesso motivo.

2) $(\mathbb{N},+,0)$ non è un sottogruppo di $(\mathbb{Z},+,0)$ ... mancano gli inversi.

3) $(S_3, \circ, id_{I_3})$ $\quad H=\{id, (12), (13)\}$ non è un sottogruppo perché non è chiuso rispetto all'operazione: $(12)\circ(13)=(1\,3\,2) \notin H$.

Esempi: 1) Per ogni gruppo $(G,*,e)$ ci sono sempre i sottogruppi (banali) G e $\{e\}$
massimo sottogruppo
minimo sottogruppo.

2) $(\mathbb{Z},+,0) \leq (\mathbb{Q},+,0) \leq (\mathbb{R},+,0)$

3) $(\{+1,-1\},\cdot,1) \leq (\mathbb{Q}^\times,\cdot,1) \leq (\mathbb{R}^\times,\cdot,1)$

4) $(S_n,\circ,id_{I_n})$ possiamo considerare il sottoinsieme $A_n=\{\sigma \in S_n \mid \sigma \text{ è pari}\}$

È un sottogruppo? Sì, perché:
1) esiste l'elemento neutro: $id \in A_n$
2) $\forall \sigma \in A_n \Rightarrow \sigma^{-1} \in A_n$
3) $\forall \sigma,\tau \in A_n \Rightarrow \sigma\circ\tau \in A_n$ (pari + pari = pari)

Prop: Sia $(G,*,e)$ un gruppo e $\emptyset \neq H \subseteq G$. Allora

$$H \text{ è sottogruppo di } G \iff \forall h_1, h_2 \in H \quad h_1 * h_2^{-1} \in H .$$

dim: "$\Rightarrow$" ovvia.

"$\Leftarrow$" Poiché $H \neq \emptyset$ $\exists h \in H$. Applichiamo la proprietà con $h_1 = h_2 = h$ e otteniamo:

$$h * h^{-1} \in H \quad , \text{ma} \quad h * h^{-1} = e \Rightarrow e \in H .$$

Se $H = \{e\}$ abbiamo finito. Se invece $\exists h \in H$, $h \neq e$, possiamo applicare la proprietà con $h_1 = e$, $h_2 = h$ e otteniamo: $e * h^{-1} \in H \Rightarrow h^{-1} \in H$.

Infine, dati $h, h' \in H$, possiamo applicare la proprietà con $h_1 = h$, $h_2 = (h')^{-1}$ (che sta in H) e otteniamo: $h * ((h')^{-1})^{-1} \in H \Rightarrow h * h' \in H$. $\boxtimes$

Sottogruppi di $\mathbb{Z}$

Fissato $n \in \mathbb{N}$: $\quad n\mathbb{Z} = \{ m \in \mathbb{Z} \mid m = n \cdot k, \text{ con } k \in \mathbb{Z} \}$

Es. $2\mathbb{Z} = \{\text{pari}\}$ $\quad 3\mathbb{Z} = \{ \dots -6, -3, 0, 3, 6, \dots \}$

$(n\mathbb{Z}, +, 0)$ è un sottogruppo di $\mathbb{Z}$. Basta far vedere che $\forall m_1, m_2 \in n\mathbb{Z}$ $m_1 - m_2 \in n\mathbb{Z}$.

Ma $m_1 - m_2 = n \cdot k_1 - n \cdot k_2 = n(k_1 - k_2) \in n\mathbb{Z}$.

<u>Teorema</u>: I sottogruppi di $(\mathbb{Z},+,0)$ sono tutti e soli i sottoinsiemi della forma $n\mathbb{Z}$ per $n \in \mathbb{N}$.

<u>Dim</u>: Abbiamo appena visto che $\forall n \in \mathbb{N}$, $n\mathbb{Z}$ è un sottogruppo.

Sia ora H sottogruppo di $(\mathbb{Z},+,0)$. Se $H=\{0\}$ allora $H = 0 \cdot \mathbb{Z}$.

Se invece $H \neq \{0\}$, allora $\exists h \in \mathbb{Z}$ tale che $h \neq 0$ e $h \in H$. Inoltre, poiché H è un gruppo, $-h \in H$, quindi H ha almeno un elemento positivo (h o $-h$).

Siano $H^+ = H \cap (\mathbb{N} \setminus \{0\}) = \{h \in H \mid h > 0\} \neq \emptyset$ e $n = \min H^+$.

Poiché H gruppo ed $n \in H \Rightarrow n\mathbb{Z} \subseteq H$ Sono i multipli di n, che sta in H

Sia ora $h \in H$. Per la divisione euclidea, $\exists q, r \in \mathbb{Z}$, $0 \leq r < n$ tali che:

$$h = q \cdot n + r \qquad \text{ovvero} \qquad r = \underbrace{h}_{\in H} - \underbrace{qn}_{\in H}$$

Perciò $r \in H$. Ma poiché $0 \leq r < n$ ed n è il minimo tra gli elementi positivi di H, non può che essere $r = 0 \Rightarrow h = qn \in n\mathbb{Z}$.

Il ragionamento vale $\forall h \in H \Rightarrow H \subseteq n\mathbb{Z} \Rightarrow H = n\mathbb{Z}$. $\boxtimes$