• APPUNTI TEORIA DEI GRUPPI

Definizione di gruppo.

una struttura algebrica $(A;+)$ e' un gruppo se e solo se ha un elemento neutro e ogni elemento ha un inverso vale la proprietà associativa.

se vale la proprietà commutativa, il gruppo e' abeliano o commutativo.

- Omomorfismo.

Siano $(G, *_g)$ e $(H, *_h)$ due gruppi.

$\phi : G \to H$ e' un omomorfismo se $\phi(g *_g g') = \phi g *_h \phi g'$

PROPRIETA': se ϕ e' un omomorfismo $\to \phi(1_G) = 1_H$

<u>VERIFICHIAMO</u>

$$\phi(1_G) = \phi(1_G *_g 1_G)$$

$$\bullet \quad 1_H = \phi(1_G) *_h (\phi(1_G))^{-1}$$

$$1_H = \phi(1_G *_g 1_G) *_h (\phi(1_G))^{-1}$$

$$1_H = \phi(1_G) *_h \cancel{\phi(1_G) *_h (\phi(1_G))^{-1}}$$

DIFFERENZA TRA OMOMORFISMO E ISOMORFISMO

Negli isomorfismi abbiamo una applicazione del tipo one to one mapping, cioe' che associa ad ogni elemento in G uno e un solo elemento in H.

Negli omomorfismi abbiamo una applicazione "suriettiva" ogni elemento in G e' mappato dall'omomorfismo ma due elementi distinti in G possono essere mappati nello stesso elemento in H.

[...] ovvero la mappatura f associa a tre elementi del gruppo C_{3v} lo stesso elemento del gruppo C_2. Gli elementi $\{E, C_3, C_3^{-1}\}$ sono mappati nello stesso elemento $E \in C_2$, mentre gli elementi $\sigma_1, \sigma_2, \sigma_3$ sono mappati in $C \in C_2$. f è una corrispondenza 3:1 e scriviamo $C_{3v} \sim C_2$. È facile vedere che la f è un'omomorfismo tra C_{3v} e C_2 dal momento che, per esempio, $f(EC_3) = E = f(E)f(C_3)$, $f(E\sigma_1) = C = f(E)f(\sigma_1)$ ecc. Emerge quindi la sostanziale differenza tra omomorfismo e isomorfismo. Un'omomorfismo tra due set $\mathcal{A}$ e $\mathcal{B}$ è una corrispondenza n:1, con $n \geq 1$, mentre un'isomorfismo è una corrispondenza 1 : 1 (applicazione iniettiva e suriettiva). In particolare, se la mappatura f è un'omomorfismo e la corrispondenza è 1:1, allora la mappatura tra i due set $\mathcal{A}$ e $\mathcal{B}$ è un'isomorfismo, e $\mathcal{A} \cong \mathcal{B}$ [...]

- Sottogruppi

Definizione: un gruppo sia $S \subseteq G$ S è sottogruppo di un altro gruppo G se

(1) - $\forall s, s' \in S$, $s \cdot s' \in S$ ($\cdot$ CHIUSA RISPETTO A S)

(2) - $\forall s \in S$, $s^{-1} \in S$

(3) - l'elemento neutro è di G, $1_G \in S$

Proprietà: $S \subseteq G$ è sottogruppo $\Leftrightarrow \forall (s_1, s_2 \in S), (s_1 \cdot s_2^{-1}) \in S$

Dim:

($\Rightarrow$) se $s_2 \in S \rightarrow s_2^{-1} \in S$ (perché S è gruppo) $\rightarrow (s_1 \cdot s_2^{-1}) \in S$

($\Leftarrow$) considero $s \in S$, $1_G \in S$ perché $s \cdot s^{-1} \in S$ per ipotesi

scelgo $s_1 = 1_G$ e $s_2 = s$, per ipotesi $s_1 \cdot s_2^{-1} \in S$

allora $1_G \cdot s^{-1} \in S \rightarrow s^{-1} \in S$ DIMOSTRATA (2)

considero $s_1, s_2 \in S$, $s_2^{-1} \in S$ e lo so

Ma allora $s_1 \cdot (s_2^{-1})^{-1} \in S$ DIMOSTRATA (1)

Proprietà: Dati 2 gruppi $(G, \cdot), (G', *)$ e un OMOMORFISMO ϕ $G \rightarrow G'$ $\boxed{\mathrm{Img}\,\phi \leq (G', *)}$

1.1 (VERIFICO)

DEVO VERIFICARE CHE: $\mathrm{Img}\,\phi \leq (G', *) \rightarrow \forall y_1, y_2 \in \mathrm{Img}\,\phi\ (y_1 * y_2) \in G'$

$y_1, y_2 \in \mathrm{Img}\,\phi \rightarrow y_1, y_2^{-1} \in \mathrm{Img}\,\phi$ PERCHÈ $\mathrm{Img}\,\phi$ SOTTOGRUPPO DI $(G', *)$

$y_1 = \phi g_1$, $y_2 = \phi g_2 \rightarrow y_1 * y_2^{-1} = \phi g_1 * \phi g_2^{-1} = \phi(g_1 \cdot g_2) \longrightarrow$ elemento di $\mathrm{Img}\,\phi$

"0" risulta soddisfatto.

- Sottogruppi di $\mathbb{Z}$ e $\mathbb{Z}_n$

Proposizione (1)

Se H e' sottogruppo di $(\mathbb{Z},+) \rightarrow \exists\, n \mid n\mathbb{Z} = H$

PER IPOTESI SO CHE $H \leq (\mathbb{Z},+)$ quindi: $H \cap \mathbb{N} \neq 0$
PERCHÉ SE $a \in H$ PURE $-a \in H$ perché?
[perché H e' un gruppo, ogni elemento nel gruppo ha il suo inverso / $a+(-a) = e$ (elemento neutro)]
QUINDI, ESSENDO SOTTOINSIEME DI $\mathbb{N}$ AVRÀ UN MINIMO PER IL PRINCIPIO DEL BUON ORDINAMENTO.
$\text{MINIMO}(H) = m$, SICCOME H È UN GRUPPO, OGNI MULTIPLO DI m È IN H, PERCHÉ?
[PERCHÈ DATO CHE H È UN SOTTOGRUPPO, $\forall (h, h_1) \in H$, $h * h_1^{-1} \in H$
QUINDI SE HO $m \in H$, $m+(m^{-1}) \in H$ QUINDI $2m \in H$
SE $2m \in H \rightarrow 2m + (m^{-1})^{-1} = 3m$ [...]
VALE A DIRE CHE
[$m\mathbb{Z} \subset H$

- AFFERMIAMO ORA CHE OGNI ELEMENTO IN H SIA DIVISIBILE PER m, POSSIAMO INFATTI DIRE CHE $\forall a \in H$, $a = qm + r$ con $0 \leq r < m$ MA m È IL MINIMO POSITIVO QUINDI r DEVE ESSERE PER FORZA 0 DATO CHE NON PUÒ ESSERE $< m$ (CIOÈ r NON ESISTE, NON C'È)
DATO CHE OGNI ELEMENTO È DIVISIBILE PER m
[$H \subset m\mathbb{Z}$

$* \; m\mathbb{Z} = H \; *$

PROPOSIZIONE ②

Se $H \leq (\mathbb{Z}_n, +) \rightarrow \exists d : d | n$, $H = H_d = \{[0], [d], [2d], \dots, [0]\}$

DIMOSTRAZIONE:

$[0] \in H$, $[n] \in H$ perché è (elemento neutro), considero $H' = \{a \in H' \mid [a] \in H\}$ quindi $0 \in H'$, $n \in H'$.

H' è sottogruppo di $(\mathbb{Z}, +)$ DIM e questo $H' = d\mathbb{Z}$ (1)

$n \in H'$ quindi quindi $d | n$ o

n è multiplo di d

la struttura di $H' = \{ 1d, 2d, 3d, \dots, n\}$

QUINDI: $H = \{[d], [2d], [3d], \dots, [n]\}$

DIM $H' \subseteq \mathbb{Z}$

DOBBIAMO FAR VEDERE CHE $\forall (a, b) \in H'$, $(a - b) \in H'$

$[a], [b] \in H$ se $a, b \in H'$ quindi $[a] - [b] \in H$ SCRITTURA EQUIVALENTE

$[a - b] \in H$

$a - b \in H'$

$H' \leq (\mathbb{Z}, +)$

Gruppo Ciclico e Classi Laterali

***GRUPPO GENERATO**

Sia $(G,*)$ un gruppo, preso $g \in G$ e $t \in \mathbb{Z}$, si ha la seguente notazione:

$$g^t = \begin{cases} 1_G \text{ se } t=0 \\ g*g*g*g \text{ per } t\text{-volte se } t>0 \\ g^{-1}*g^{-1}*g^{-1}*g^{-1} \text{ per } t\text{-volte se } t<0 \end{cases}$$

Ne segue:

- $g^s * g^t = g^{s+t}$
- $g^{-t} = (g^{-1})^t = (g^t)^{-1}$

L'insieme $\{g^t, t \in \mathbb{Z}\}$ è un sotto-gruppo di G, dato che presi g^{t_1} e g^{t_2} si ha che

$$g^{t_1}*(g^{t_2})^{-1} = g^{t_1}*g^{-t_2} = g^{t_1-t_2} \in \{g^t, t \in \mathbb{Z}\}$$

*questo sottogruppo ha simbolo $\langle g \rangle$ ed è denominato gruppo generato da g

CLASSI LATERALI Dx e Sx

Sia H un sottogruppo di $(G,*)$, dove G non è necessariamente finito, l'insieme H ha una classe laterale sinistra associata ad ogni $a \in G$, ed è l'insieme $aH = \{a*h, h \in H\}$ la classe laterale destra invece è $Ha = \{h*a, h \in H\}$ $Ha \neq aH$ ammenochè il gruppo non sia commutativo.

NOTA CHE:

(1) $a, b \in G$, $aH = bH \iff a^{-1}*b \in H$

(2) $a, b \in G \rightarrow aH = bH$ oppure $aH \cap bH = \emptyset$

(3) $\forall x \in G \; \exists a \in G \mid x \in aH$ [...]