Teoria dei gruppi

Cos'è un gruppo?

Un gruppo è un insieme G dotato di una operazione binaria $\circ : G \times G \to G$ e un elemento neutro $e \in G$ per cui valgono i seguenti assiomi:

1) $\forall a \in G, \exists a^{-1} \mid a \circ a^{-1} = e \in G$ (INVERSO)
2) $\forall a \in G, a \circ e = a$ (NEUTRO)
3) $a \circ (b \circ c) = (a \circ b) \circ c \quad \forall a, b, c \in G$ (ASSOCIATIVITÀ)
4) $\forall a, b \in G, a \circ b \in G$ (CHIUSURA)

Sottogruppi, Omomorfismi, Prodotti

SOTTOGRUPPO

def: Sia G un gruppo $(G, \circ)$, H sottoinsieme di G. Se H è un gruppo con la stessa operazione di G e lo stesso elemento neutro di G allora è sottogruppo di G

ESEMPI: $\mathbb{Z} \leq \mathbb{R}$ $\boxed{\leq \text{(SOTTOGRUPPO)}}$

Teorema per capire se un sottoinsieme H sia o meno un sottogruppo di un gruppo G.

i) H è un sottoinsieme di G

ii) $H \neq \emptyset$ e
- per ogni $a, b \in H$ si ha $ab \in H$
- per ogni $a \in H$ si ha $a^{-1} \in H$

iii) $H \neq \emptyset$ e per ogni $a, b \in H$ si ha $ab^{-1} \in H$

le tre definizioni sono equivalenti.

$(i) \leftrightarrow (ii) \leftrightarrow (iii)$

DIMOSTRAZIONE:

Supponiamo (iii). $H \neq \emptyset$ prendiamo $x \in H$. pongo $a = x$ e $b = x$, troviamo che $e = x \cdot x^{-1}$ L'ELEMENTO NEUTRO E' IN H.
prendo $a = e$ $b = x$, troviamo che $x^{-1} = ex^{-1} \in H$ e questo vale prendendo un qualsiasi elemento L'INVERSO DI OGNI VALORE E' IN H. Sapendo che $x, y \in H \rightarrow x, y^{-1} \in H$ quindi $a = x$, $b = y^{-1}$, $ab = xy \in H$ CHIUSURA DI H

$\boxed{iii \rightarrow ii}$

Supponiamo (ii). Siccome $ab \in H$ $\forall a, b$ H è chiuso per la composizione di G che è una composizione associativa 3)4) L'elemento neutro è in H dato che ($\forall a \in H$ anche l'inverso $a^{-1} \in H$) 2)1)

Dim:

dato che $\forall a \in H$ si ha $a^{-1} \in H$
e che $\forall a, b \in H$, $a \cdot b \in H$
prendendo $a = x$ e $b = x^{-1}$
$x \cdot x^{-1} \in H$ quindi $e \in H$

$\boxed{ii \rightarrow i}$

Dimostriamo ora che $i \rightarrow ii \rightarrow iii$
Supponiamo (i), $H \leq G$, H è sottogruppo di G quindi $e \in H$ e H risulta chiuso sull'operazione di G quindi:
$H \neq \emptyset$, infatti contiene almeno e.
$\forall a, b \in H$ $ab \in H$
$\forall a \in H$ $\exists a^{-1} \mid a \cdot a^{-1} = e$ perché H è un gruppo.

$\boxed{i \rightarrow ii}$

Supponiamo (ii), $\forall a, b \in H$, $ab \in H$ e $\forall a \in H$ $\exists a^{-1} \in H$
se $a, b \in H \rightarrow a, b \in H$ quindi $a \cdot b^{-1} \in H$

$\boxed{ii \rightarrow iii}$

IN DEFINITIVA: (i) $\Leftrightarrow$ (ii) $\Leftrightarrow$ (iii)

CENTRO DI UN GRUPPO

def: Sia G un gruppo. Il centro $Z(G)$ di G è un sottogruppo.

$$Z(G) = \{ g \in G : gh = hg \ \forall h \in G \}$$

teorema

i) I sottogruppi di $\mathbb{Z}$ sono $\{0\}$ e $d\mathbb{Z}$

ii) I sottogruppi di $\mathbb{Z}_n$ sono $H_d = \{[d],[2d],[3d],\dots,[n]=[0]\}$

DIM:

i) Sia H sottogruppo di $\mathbb{Z}$. allora $0 \in H$ perché elemento neutro additivo di $\mathbb{Z}$, se H non contiene altri elementi abbiamo $H = \{0\}$. Supponiamo $a \neq 0 \in H \rightarrow a^{-1} \in H$ perché H è un gruppo, H contiene elementi positivi e $H \cap \mathbb{N}^+ \neq \emptyset$ quindi per il PRINCIPIO DEL BUON ORDINAMENTO esisterà un minimo positivo in H che chiamiamo d. Siccome H è un gruppo, ogni multiplo di d è in H, infatti $\forall a,b \in H$, $ab^{-1} \in H \rightarrow a, b^{-1} \in H$, $ab \in H$ prendendo $a = d$ e $b \in H$, $db \in H \ \forall b \in H$.

quindi: $d\mathbb{Z} \subset H$

Affermiamo poi che $H \subset d\mathbb{Z}$ cioè che $\forall a \in H$ $d | a$ infatti:

$a = qd + r \qquad q, r \in \mathbb{Z}, \quad 0 \leq r < d$

se r non fosse nullo dovrebbe essere $< d$ ma dato che d = MINIMO DI H questo non è possibile quindi r è nullo quindi $H \subset d\mathbb{Z}$

DIM:

ii) $H \leq \mathbb{Z}_n$, $H' = \{ a \in \mathbb{Z} \mid [a] \in \mathbb{Z}_n \}$

Siccome H e' sottogruppo di $\mathbb{Z}_n$ contiene l'elemento neutro di $\mathbb{Z}_n$, cioe' $[0]=[n]$ quindi H' contiene $0, n$.
$0, n \in H'$. Siano $a, b \in H' \to [a], [b] \in H$, siccome H e' un sottogruppo di $\mathbb{Z}_n$, $[a-b] \in H$ quindi $(a-b) \in H'$ quindi $H' \leq \mathbb{Z}$ ((iii) → (i)).
Abbiamo $n, 0 \in H'$ quindi $H' \neq \emptyset$ per i) sappiamo che $H' = d\mathbb{Z}$ per un intero positivo d, Siccome $n \in H'$ $d \mid n$ perche' n deve essere multiplo di d

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

$$H = \{[d], [2d], \dots, [n=0]\}$$

OMOMORFISMI

Siano $(G, \circ)$ e $(G', *)$ due gruppi. Una applicazione $f: G \to G'$ si chiama omomorfismo se $f(a \circ b) = f(a) * f(b)$ $\forall a, b \in G$
questa applicazione e' suriettiva, se e' BIETTIVA si tratta di un isomorfismo.

teorema

Sia $(G, \circ)$ un gruppo con elemento neutro e e sia $(G', *)$ un gruppo con elemento neutro e'. $f: G \to G'$ omomorfismo. Allora

i) $f(e) = e'$

ii) $f(a^{-1}) = f(a)^{-1}$

Dim: (ESERCIZI FOGLIO 4)

i) $e = e \circ e$

$f(e) = f(e \circ e)$

$f(e) = f(e) * f(e)$

$e' = f(e) * (f(e))^{-1}$

$e' = f(e) * f(e) * (f(e))^{-1}$ USANDO L'ASSOCIATIVITA'

$e' = f e * (f(e) * (f(e))^{-1}) \Rightarrow e' = f(e)$

ii)

$f(a^{-1}) = (f(a))^{-1}$

PRENDO $a \in G$

$e = a \circ a^{-1} \to e' = f(e) \to e' = f(a \circ a^{-1}) \to$

$e' = f(a) * f(a^{-1})$ ma e' può essere scritto anche

$e' = f(a) * (f(a))^{-1}$

$f(a) * f(a^{-1}) = f(a) * (f(a))^{-1} = e'$

$f(a^{-1})$ è l'inverso di $f(a)$ ma anche $(f\,a)^{-1}$ è l'inverso di $f(a)$, dato che in un gruppo ogni elemento ha un solo inverso $(f(a))^{-1} = f(a^{-1})$.

Teorema

Dato $(G, \circ)$, $(H, *)$, $f: G \to H$ (OMOMORFISMO) $\to \mathrm{Img}(f) \leq H$

Dim:

(i) → (iii)

$\mathrm{Img}(f) \leq H$ DEVO DIMOSTRARE CHE $\forall J_1, J_2 \in \mathrm{Img}(f)$

$J_1 * J_2 \in \mathrm{Img}(f)$

so che $\mathrm{Img}(f) \neq \phi$ perché sottogruppo di H.

$J_1, J_2 \in \mathrm{Img}(f)$ quindi $\exists g_1 \mid f(g_1) = J_1$, $\exists g_2 \mid f(g_2) = J_2$

se $J_2 \in \mathrm{Img}(f)$, $J_2^{-1} \in \mathrm{Img}(f)$ perché $\mathrm{Img}(f)$ è un gruppo.

$(J_1 * J_2^{-1}) = f(g_1) * f(g_2^{-1}) = f(g_1 \circ g_2^{-1})$ che è un elemento di $\mathrm{Img}(f)$

((i) → (iii))