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 sottogruppo 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 $a, b \in H \rightarrow a, b^{-1} \in H$ 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 $a \neq 0$ $\in H \to a^{-1} \in H$ 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 $d \in H$, $d+d = 2d \in H$ quindi $3d \in H$ [...]

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 è sottogruppo di $\mathbb{Z}_n$ contiene l'elemento neutro di $\mathbb{Z}_n$, cioè $[0]=[n]$ quindi H' contiene $0, n$. $0, n \in H'$. Siano $a, b \in H' \to [a], [b] \in H$, siccome H è un sottogruppo di $\mathbb{Z}_n$, $[a-b] \in H$ quindi $(a-b) \in H'$ quindi $H' \leq \mathbb{Z}$ ((iii) $\to$ (i)).

Abbiamo $n, 0 \in H'$ quindi $H' \neq \emptyset$ per i) sappiamo che $H' = d\mathbb{Z}$ per un intero positivo d, Siccome $n \in H'$ $d \mid n$ perché 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 è suriettiva, se è 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'ASSOCIATIVITÀ

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

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) $\to Img(f) \leq H$

Dim:

(i) $\to$ (iii)

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

$J_1 * J_2 \in Img(f)$

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

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

se $J_2 \in Img(f)$, $J_2^{-1} \in Img(f)$ perché $Img(f)$ 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 $Img(f)$

((i) $\to$ (iii))

DA $[S - VG]$

GRUPPO GENERATO

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

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

Ne segue:

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

L'insieme $\{g^t, t \in \mathbb{Z}\}$ e' un sottogruppo di G dato che presi g^{t_1} e g^{t_2} si ha che $g^{t_1} * (g^{t_2})^{-1} = g^{t_1 - t_2} \in \{g^t, t \in \mathbb{Z}\}$

questo sottogruppo ha simbolo $\langle g \rangle$ ed e' denominato gruppo generato da g.

C_2		C_3	
Classi Laterali Sinistre	Classi Laterali Destre	Classi Laterali Sinistre	Classi Laterali Destre
$IC_2 = \{I, f\}$ $rC_2 = \{r, rf\}$ $= \{r, fr^2\}$ $r^2C_2 = \{r^2, r^2f\}$ $= \{r^2, fr\}$	$C_2I = \{I, f\}$ $C_2r = \{r, fr\}$ $= \{r, r^2f\}$ $C_2r^2 = \{r^2, fr^2\}$ $= \{r^2, rf\}$	$IC_3 = \{I, r, r^2\}$ $fC_3 = \{f, fr, fr^2\}$	$C_3I = \{I, r, r^2\}$ $C_3f = \{f, rf, r^2f\}$ $= \{f, fr^2, fr\}$

CLASSI LATERALI

Sia H un sottogruppo di $(G *)$, dove G non e' necessariamente finito, l'insieme H ha una classe laterale sinistra associata ad ogni $a \in G$

$$aH = \{a*h \; ; \forall h \in H\}$$

la classe laterale destra associata ad ogni

$a \in G$ sono $Ha = \{h * a, \forall h \in H\}$

- $aH = Ha \Leftrightarrow G$ commutativo

PROP:

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

(ii) $a, b \in G \to aH = bH$ o $aH \cap bH = \emptyset$

(iii) $\forall x \in G \; \exists a \in G \mid x \in aH$

OSS:

tutte le classi laterali sx formano una partizione di G, denotate $\mathcal{L}_s$ e definisce la relazione

$a \rho_s b \Leftrightarrow \exists g \in G \mid a \in gH, b \in gH \Leftrightarrow a^{-1} * b \in H$

Analogamente per le classi laterali destre abbiamo $\mathcal{L}_D$ e definisce la relazione

$a \rho_D b \Leftrightarrow b * a^{-1} \in H$

- In generale $\rho_s \neq \rho_d$
- Il numero delle classi laterali sinistre è uguale al numero delle classi laterali destre.

GRUPPO CICLICO

def: Sia $(G; *)$ un gruppo e $H \leq (G, *)$, H è detto ciclico se

$\exists h \in H \mid \langle h \rangle = H$

G può essere ciclico se:

$\exists g \in G \mid \langle g \rangle = G$

e oltre a essere ciclico è anche commutativo visto che:

$$g^s * g^t = g^{t+s} = g^t * g^s$$

Teorema di Lagrange.

Sia G un gruppo finito e H un suo SOTTOGRUPPO, vale che la cardinalità di H divide la cardinalità di G, l'ordine di H è un divisore dell'ordine di G

$$|G| = i \cdot |H|$$

Dim: Sia $H \leq (G, *)$

osserviamo che $\exists\ \phi : H \to aH$ $\forall a$ quindi $|H| = |aH|$

$$h \to ah$$

Consideriamo ora $\{a_1H, a_2H, a_3H \dots a_iH\}$ l'insieme delle classi sinistre distinte. Dato che ogni classe è una partizione di G

$$|G| = \sum_{j=1}^{i} |a_j H|$$

le classi laterali hanno tutte la stessa cardinalità

i classi laterali $\Rightarrow i|H| = |G|$

PROP: $ps = pd \Leftrightarrow aH = Ha \quad \forall a \in G$

DEF: se $ps = pd$ il sottogruppo è detto normale ed è denotato con $H \trianglelefteq G$

PROP: $H \trianglelefteq G \Leftrightarrow a * h * a^{-1} \in H \quad \forall a \in G$