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 $a, b \in H \rightarrow a, b^{-1} \in H$ 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 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 $H' \leq \mathbb{Z}$ $((iii) \to (i))$.
Abbiamo $n, 0 \in H'$ quindi $H' \neq \emptyset$ per i) sappiamo che $H' = d\mathbb{Z}$ per un intero positivo d, Siccome $n \in H'$ $d \mid n$ 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'

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

ii)

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

PRENDO $a \in G$

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

$e' = f(a) * f(a^{-1})$ 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 $(G, \circ)$, $(H, *)$, $f : G \rightarrow H$ (OMOMORFISMO) $\rightarrow Img(f) \leq H$

Dim:

$(i) \rightarrow (iii)$

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

$((i) \rightarrow (iii))$

DA $[S - VG]$

GRUPPO GENERATO

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

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

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 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 è denominato gruppo generato da g.

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

CLASSI LATERALI

Sia $(G, \cdot)$ un e H un sottogruppo, definiamo la seguente relazione:

$$\boxed{a \, \rho_d \, b \iff a \cdot b^{-1} \in H}$$

questo è una relazione di equivalenza, infatti:

è riflessiva

$a \rho_d a$ perché $a \cdot a^{-1} \in H$, $e \in H$ perché sottogruppo di $(G, \cdot)$

è simmetrica

$a \rho_d b \rightarrow b \rho_d a$ perché $a, b^{-1} \in H$, $a \cdot b^{-1} \in H$

per (iii) $\forall a, b \in H$, $ab^{-1} \in H$

prendo $a = b^{-1}$, $b = a^{-1} \rightarrow$ POSSIBILE PERCHÉ H È GRUPPO

$b^{-1} a \in H$

è transitiva

$(a \rho_d b, b \rho_d c) \rightarrow a \rho_d c$ perché $\forall a, b \in H$ $ab^{-1} \in H$

so che $a \in H$, $b \in H$, $c \in H$ (e i loro inversi) perché $ab^{-1} \in H$, $bc^{-1} \in H$

quindi per (iii)

$a = a$ $b = c^{-1} \rightarrow a(c^{-1})^{-1} \in H$

$\rightarrow \boxed{a \rho_d c}$

Il gruppo G viene quindi diviso in classi di equivalenze chiamate laterali destri modulo H.

laterale sinistro = $a \rho_s b \leftrightarrow b^{-1} a \in H$

$\rho_s = \rho_d \leftarrow G$ COMMUTATIVO.

- Sia a un elemento di G e $\rho_d(a)$ la sua classe di equivalenza modulo la relazione.

$$\rho_d(a) = \{b \in G \mid b \rho a\} = \{b \in G \mid ba^{-1} \in H\}$$
$$= \{b \in G \mid ba^{-1} = h,\ h \in H\}$$
$$= \{b \in G \mid b = ha \text{ per qualche } h \in H\} \subseteq Ha$$

$\rightarrow$ POI

Ha (INSIEME DEI MULTIPLI DI a) $= \{b \in G \mid b = ak,\ k \in H\}$

$$= \{ b \in G \mid h \in H = b \cdot a^{-1} \}$$

$$= \{ b \in G \mid (b \cdot a^{-1}) \in H \} \subseteq \rho_d(a)$$

quindi $Ha = \rho_d(a)$

$\forall a \in G \quad aH = \{ a * h, \ \forall h \in H \}$ e questa è una classe laterale sinistra

SAME x DX

Proposizione: (FACOLTATIVO)

tutte le classi laterali hanno la stessa cardinalità, cioè la cardinalità di H

Dim:

Basta dimostrare una corrispondenza biunivoca tra due classi laterali qualsiasi.

Ha e Hb due classi laterali destre.

$\psi : Ha \to Hb$

definita ponendo $\psi(ha) = hb$

a) è iniettiva: $\psi(h_1 a) = \psi(h_2 a)$, allora vuol dire che $h_1 b = h_2 b$, da cui, per la legge della cancellazione, $h_1 = h_2$ e quindi $h_1 a = h_2 a$

b) è suriettiva: dato che un elemento di Hb, sarà del tipo hb per qualche $h \in H$, esso proviene da ha ¿PERCHÈ?

Prop:

(i) $a, b \in G$, $aH = bH \leftrightarrow (a^{-1} * b) \in H$ (DUE CLASSI DI EQUIVALENZA SONO UGUALI SE I RAPPRES. DELLE CLASSI SONO IN RELAZIONE TRA LORO.)

(ii) $a, b \in G \to aH = bH$ o $aH \cap bH = \emptyset$ (DUE CLASSI DI EQUIVALENZA O SONO LA STESSA CLASSE DI EQUIVALENZA O NON HANNO EL IN COMUNE)

(iii) $\forall x \in G \ \exists a \in G \mid x \in aH$ (OGNI VALORE IN G È IN UNA CLASSE DI EQUIVALENZA.)

(STESSO VALE PER DX)

OSS:

tutte le classi laterali sinistre formano una partizione di G, denotata $\mathcal{L}_S$, tale partizione definisce anche una relazione di equivalenza.

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

Analogamente per le classi laterali destre. ($\mathcal{L}_D$)

In generale ps ≠ pd. Se G e' finito, l'indice di H in G e' il numero di classi laterali SX = DX

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 e' 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 e' 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 e' detto normale ed e' denotato con $H \trianglelefteq G$

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