GRUPPI (IV PARTE)

Def: $(G,\cdot)$ è un gruppo. H un sottogruppo di G. Fissato $g \in G$, si dice

1) laterale sinistro di H definito da g il sottoinsieme $gH = \{gh \mid h \in H\} \subseteq G$
2) laterale destro " " $Hg = \{hg \mid h \in H\} \subseteq G$

g si dice rappresentante del laterale.

Esempi: 1) $g = e_G$ $\quad e_G H = H = H e_G$

2) $(G,\cdot) = (\mathbb{Z},+)$ $\quad H = n\mathbb{Z}$, fissiamo $k \in \mathbb{Z}$ (laterali destri = laterali sinistri)

perché $(\mathbb{Z},+)$ è abeliano

$$H+k = n\mathbb{Z}+k = \{\ldots, -2n+k, -n+k, k, n+k, 2n+k, \ldots\}$$

laterale (destro) definito da k

$n=5$ $\quad H = 5\mathbb{Z}$

$k=1$ $\quad 5\mathbb{Z}+1 = \{\ldots,-9,-4,1,6,11,\ldots\} = [1]_5$

$k=2$ $\quad 5\mathbb{Z}+2 = \{\ldots,-8,-3,2,7,12,\ldots\} = [2]_5$

$k=-3$ $\quad 5\mathbb{Z}-3 = \{\ldots,-8,-3,2,7,\ldots\} = [-3]_5 = [2]_5$

$k=0$ $\quad 5\mathbb{Z}+0 = \{\ldots,-10,-5,0,5,10,15,\ldots\} = [0]_5$

Sono le classi di resto mod 5

3) $G=(S_3,\circ)$ $\quad H=\{id,(12)\}$ $\quad g=(1\,2\,3)$

$$g\circ H=\{(123)\circ id,\ (123)\circ(12)\}=\{(1\,2\,3),(1\,3)\}$$
$$H\circ g=\{id\circ(1\,2\,3),\ (1\,2)\circ(1\,2\,3)\}=\{(1\,2\,3),(2\,3)\}$$

sono distinti

<u>Prop</u>: Sia $(G,\cdot)$ un gruppo. H un sottogruppo di G. Allora

1) $\forall g\in G$, $f:H\longrightarrow gH$ $f(h)=gh$ è una biezione;
2) $\forall g_1,g_2\in G$ $g_1H=g_2H$ se e solo se $g_2^{-1}g_1\in H$;
3) i laterali sinistri di H formano una partizione di G.

le stesse cose valgono per i laterali destri

<u>Dim</u>: 1) f iniettiva: $f(h)=f(h')\iff gh=gh'\iff g^{-1}gh=g^{-1}gh'\iff h=h'$.
f suriettiva: se $x\in gH$ allora $\exists h\in H$ t.c. $x=g\cdot h=f(h)$.

2) i) Prima mostriamo che $\forall x\in G$ $xH=H\iff x\in H$

Infatti "$\Rightarrow$": se $xH=H$ allora, poiché $e_G\in H$, anche $x\cdot e_G=x\in H$

"$\Leftarrow$" se $x\in H$ allora $\overset{\forall h\in H}{x\cdot h}\in H$ perché H è un sottogruppo, quindi $xH\subseteq H$, quindi $xH=H$

per il punto 1) sono in biezione

3) i) i laterali sono in biezione con H (vedi punto 1)) $\Rightarrow$ non sono vuoti.

ii) $\forall g\in G$, $g\in gH$ perché $e_G\in H$ e $g=ge_G$ $\Rightarrow$ i laterali sono un ricoprimento.

iii) Se $g_1H\cap g_2H\neq\emptyset\Rightarrow\exists g\in g_1H\cap g_2H\Rightarrow\exists h_1,h_2\in H$ t.c. $g=\boxed{g_1h_1=g_2h_2}$ moltiplico $g_2^{-1}\cdot(\quad)\cdot h_1^{-1}$

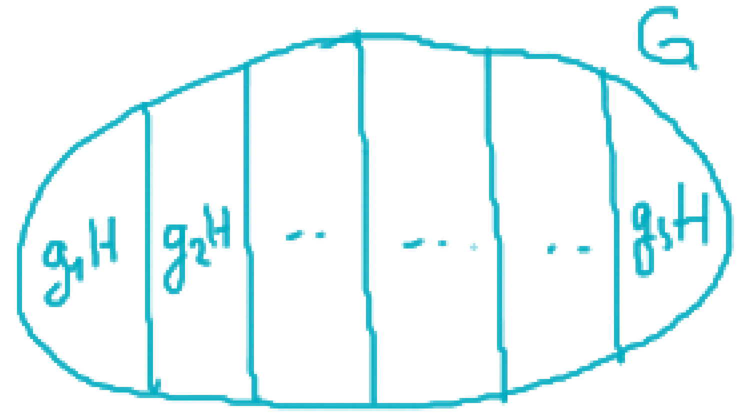
$g_2^{-1}g_1\cancel{h_1h_1^{-1}}=\cancel{g_2^{-1}g_2}h_2h_1^{-1}\Rightarrow g_2^{-1}g_1=h_2h_1^{-1}\in H\Rightarrow$ grazie a 2) $g_1H=g_2H$ $\boxtimes$

Teorema di Lagrange: Sia $(G,\cdot)$ un gruppo finito di ordine (= cardinalità) n e H un sottogruppo di G di ordine d. Allora $d \mid n$.

Dim: Abbiamo visto (proposizione precedente) che i laterali sinistri di H formano una partizione di G. Quindi esistono s laterali distinti tali che:

$$G = g_1 H \cup g_2 H \cup \dots \cup g_s H \quad \text{e poiché} \quad g_i H \cap g_j H = \emptyset \quad \text{per } i \neq j$$

$$n = |G| = |g_1 H| + |g_2 H| + \dots + |g_s H|$$



Inoltre, poiché $\forall i$ $g_i H$ è in biezione con H, allora $|g_i H| = d$

$$n = \underbrace{d + d + \dots + d}_{s \text{ volte}} = s \cdot d$$

$\boxtimes$

Semplici conseguenze:

Es 1: $(\mathbb{Z}_5, +)$ ha ordine 5, che è primo $\Rightarrow$ non ha sottogruppi non banali.

Es. 2 $(S_4, \circ)$ $\quad |S_4| = 4! = 24$ $\quad$ i divisori non banali sono: 2, 3, 4, 6, 8, 12

Ma ciò non significa che esista un sottogruppo di ordine pari a ciascun divisore ....

$H_1 = \{id, (1\,2)\} \leq S_4 \qquad H_2 = \{id, (1\,2\,3), (1\,3\,2)\} \leq S_4 \quad \dots$

Per esempio, non ci sono sottogruppi di ordine 8.

Sottogruppi ciclici

Sia $(G, \cdot)$ un gruppo.

$\forall n \in \mathbb{N}$, $\forall g \in G$ $\quad g^n := \underbrace{g \cdot g \cdot g \cdot \ldots \cdot g}_{n \text{ volte}} \qquad g^{-n} := \underbrace{\overset{\text{l'inverso di } g}{g^{-1}} \cdot g^{-1} \cdot \ldots \cdot g^{-1}}_{n \text{ volte}} \qquad g^0 := e_G \qquad$ OSS: $(g^n)^{-1} = g^{-n}$

$\forall g \in G \quad <g> = \{g^n \in G \mid n \in \mathbb{Z}\}$

Prop: $(G, \cdot)$ gruppo. $\forall g \in G$ $<g>$ è un sottogruppo di G, detto sottogruppo ciclico generato da g.

Dim: Siano $g^r, g^s \in <g> \Rightarrow g^r \cdot (g^s)^{-1} = g^r \cdot g^{-s} = \underbrace{g \cdot g \cdots g}_{r \text{ volte}} \cdot \underbrace{g^{-1} \cdot g^{-1} \cdots g^{-1}}_{s \text{ volte}} = g^{r-s} \in <g>$ $\boxtimes$

Se un certo sottogruppo $H \leq G$ è tale che $H = <g>$ per un certo $g \in G$, allora si dice che H è generato da g e che g è un generatore di H. In tal caso H si dice ciclico.

Esempi: 1) $(\mathbb{Z}, +)$ è un gruppo ciclico perché è generato da 1 : $\mathbb{Z} = <1>$

infatti ogni $n \in \mathbb{Z}$ è multiplo di 1.

2) $(\mathbb{Z}_5, +)$ è un gruppo ciclico generato da $\bar{2}$: $\quad \mathbb{Z}_5 = <\bar{2}>$

$\bar{2} = \bar{2}$, $\quad \bar{4} = \bar{2} + \bar{2}$, $\quad \bar{1} = \bar{2} + \bar{2} + \bar{2}$, $\quad \bar{3} = \bar{2} + \bar{2} + \bar{2} + \bar{2}$, $\quad \bar{0} = \bar{2} + \bar{2} + \bar{2} + \bar{2} + \bar{2}$

L'esempio mostra che il generatore di un gruppo ciclico non è unico ($\mathbb{Z}_5$ è generato anche da $\bar{1}$)

Osservazioni

1) $(G, \cdot)$ gruppo, $g \in G$. $\langle g \rangle$ è sempre abeliano: $g^r \cdot g^s = g^{r+s} = g^{s+r} = g^s \cdot g^r$.
(anche se G non lo è)

2) $(G, \cdot)$ non abeliano non può essere ciclico. Es. $(S_n, \circ)$ non è ciclico per $n > 2$.

3) Non tutti i gruppi abeliani sono ciclici. Es. $(\mathbb{Z} \times \mathbb{Z}, +)$.