

Dato  $S_4$ , consideriamo l'insieme  $H = \{\tau \in S_4 \mid \tau(4) = 4\}$  (permutazioni di  $S_4$  che permutano solo 1, 2, 3 e mantengono fisso il 4). H ha qualche legame con  $S_3$ ? Osserviamo che:

- H è un gruppo di permutazioni
- H contiene ()
- se  $\tau \in H$ ,  $\tau^{-1} \in H$

$\Rightarrow$  Si dice che H è sottogruppo di  $S_4$

Def. (Sottogruppo):

Dato G gruppo, un insieme  $H \subseteq G$  è SOTTOGRUPPO di G se:

- 1)  $1 \in H$
- 2)  $\forall a \in H, a^{-1} \in H$
- 3)  $\forall a, b \in H, a \cdot b \in H$

esempi:

$U = \{z \in \mathbb{C} \mid |z| = 1\}$  è un sottogruppo di  $(\mathbb{C} \setminus \{0\}, \cdot)$

Teorema (Caratterizzazione del sottogruppo):

Dato  $H \subseteq G$  con G gruppo, H è sottogruppo di G se e solo se:

- 1)  $H \neq \emptyset$
- 2)  $\forall a, b \in H, a \cdot b^{-1} \in H$

Dim.:

- $\Rightarrow$
- 1)  $1 \in H \Rightarrow H \neq \emptyset \vee$
  - 2)  $a, b \in H \Rightarrow a^{-1}, b^{-1} \in H \Rightarrow a \cdot b^{-1} \in H \vee$

$\Leftarrow$  Verifichiamo le 3 proprietà dei sottogruppi:

1) sia  $c \in H$  ( $H \neq \emptyset$ )  $\Rightarrow c \cdot c^{-1} \in H \Rightarrow 1 \in H \checkmark$

2) sia  $a \in H \Rightarrow 1 \cdot a^{-1} \in H \Rightarrow a^{-1} \in H \checkmark$

3) siamo  $a, b \in H \Rightarrow b^{-1} \in H \Rightarrow a \cdot (b^{-1})^{-1} = a \cdot b \in H \checkmark$

q.e.d.

Teorema (Caratterizzazione dei sottogruppi finiti):

Un sottouscupo **Finito**  $H \subseteq G$  (con  $G$  gruppo) è sottogruppo se e solo se:

1)  $H \neq \emptyset$

2)  $\forall a, b \in H, a \cdot b \in H$

Dim.:

$\Rightarrow$  ovvio  $\checkmark$

$\Leftarrow$  Dobbiamo sfruttare il fatto che  $|H| < +\infty$

[Ricordiamo che, dato  $A$  t.c.  $|A| < +\infty$ , si ha che  $f: A \rightarrow A$  è iniettiva se e solo se  $f$  è suriettiva.]

Dato  $a \in H$ , sia  $\mu_a: H \rightarrow H$  con  $\mu_a(x) = ax$   
 $\Rightarrow \mu_a$  è iniettiva perché  $\mu_a(x) = \mu_a(y) \Leftrightarrow ax = ay$   
 $\Leftrightarrow a^{-1}(ax) = a^{-1}(ay) \Leftrightarrow x = y$

$\Rightarrow \mu_a$  è suriettiva  $\Rightarrow \exists x \in H$  t.c.  $\mu_a(x) = a \Leftrightarrow ax = a$   
 $\Leftrightarrow a^{-1}ax = a^{-1}a \Leftrightarrow x = 1 \in H$ .

$\Rightarrow$  per la suriettività  $\exists y \in H$  t.c.  $\mu_a(y) = 1 \Leftrightarrow ay = 1$   
 $\Leftrightarrow y = a^{-1} \in H$

q.e.d.

La cardinalità di un gruppo finito si dice **ORDINE** del gruppo.

Teorema (di Lagrange per i gruppi):

Dati  $G$  gruppo finito e  $H$  sottogruppo di  $G$ , si ha che l'ordine di  $H$  è divisore dell'ordine di  $G$ .

Dim. (**IMPORTANTISSIMA !!!**):

Definiamo  $a \sim_H b$  su  $G$  (!!!) t.c.:

$$a \sim_H b \Leftrightarrow ab^{-1} \in H \quad (\text{misura la "distanza" tra } a, b)$$

$\sim_H$  è relazione di equivalenza su  $G$ :

1)  $\sim_H$  è riflessiva:

$$a \in G \Rightarrow aa^{-1} = 1 \in H \Rightarrow a \sim_H a \quad \forall a \in G$$

2)  $\sim_H$  è simmetrica:

$$\begin{aligned} a \sim_H b &\Rightarrow ab^{-1} \in H \Rightarrow (ab^{-1})^{-1} \in H \Rightarrow ba^{-1} \in H \\ &\Rightarrow b \sim_H a \end{aligned}$$

3)  $\sim$  è transitiva:

$$\begin{aligned} a \sim_H b \wedge b \sim_H c &\Rightarrow ab^{-1}, bc^{-1} \in H \Rightarrow (ab^{-1})(bc^{-1}) \in H \\ &\Rightarrow ac^{-1} \in H \Rightarrow a \sim_H c \end{aligned}$$

$\Rightarrow \sim_H$ , tramite le sue classi di equivalenza, partiziona  $G$ !

$\Rightarrow$  chi sono le classi di equivalenza? Dato  $g \in G$  si ha:

$$[g] = \{a \in G \mid a \sim_H g\} = \{a \in G \mid ag^{-1} \in H\}$$

- $$= \{a \in G \mid a \in Hg\} = Hg \quad (ag^{-1} = h \Leftrightarrow a = hg)$$
- $\Rightarrow$  in particolare  $[1] = H_1 = H$
- $\Rightarrow$  le classi di equivalenza hanno tutte la stessa cardinalità
- $\Rightarrow$  data  $g \in G$ , sia  $f: H \rightarrow Hg$  con  $f(x) = x \cdot g$ , allora tale  $f$  è biettiva (suriettiva per costruzione, iniettiva:  $f(x) = f(y) \Rightarrow x \cdot g = y \cdot g \Rightarrow x = y$ )
- $\Rightarrow G$  è finito, quindi tutte le classi di equivalenza hanno cardinalità  $|H|$ .
- $\Rightarrow$  indichiamo con  $[G:H]$  il numero di classi di equivalenza, allora si ha  $|G| = |H| \cdot [G:H]$

q.e.d.

N.B.

$[G:H]$  è detto indice di  $H$  in  $G$ .

Gli elementi  $Hg, gh$  si dicono classi laterali (cosets) e sono generalmente diversi!!!

Osservazione:

Se definissons  $a_H \sim b \Leftrightarrow a^{-1}b \in H$ ? In generale, le 2 relazioni non sono la stessa, tuttavia il teorema si può dimostrare ugualmente con le classi di equivalenza  $gH$ . Inoltre, le 2 relazioni hanno in comune il numero di elementi della partizione associata (ovvero il numero delle classi di equivalenza) e la classe di equivalenza  $H^c = 1H = H$ .

$$\Rightarrow [G:H] = |G/\sim_H| = |G/H|$$

esercizio:

Trovare  $f: G/\sim_H \rightarrow G/H$  biiettiva senza ipotesi di finitività su  $G$

esempio (classi laterali distinte):

$H = \{(1), (12)\} \subseteq S_3 \Rightarrow H$  è sottogruppo:

$$1) ()() = () \in H \quad \checkmark$$

$$2) ()(12) = (12) = (12)() \in H \quad \checkmark$$

$$3) (12)(12) = () \in H \quad \checkmark$$

$$\Rightarrow \text{sia } H(13) = \{(1)(13), (12)(13)\} = \{(13), (132)\}$$

una classe laterale, e sia  $(13)H = \{(13), (13)(12)\}$

$$= \{(13)(123)\}$$

$$\Rightarrow H(13) \neq (13)H$$

N.B.

Se  $G$  è abeliano, le classi laterali sono uguali!!!

Applicazione del Teorema di Lagrange:

sia  $g \in G$  e  $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\} \Rightarrow \langle g \rangle$  è sottogruppo di  $G$ :

$$1) 1 = g^0 \in \langle g \rangle$$

$$2) (g^n)^{-1} = g^{-n} \in \langle g \rangle$$

$$3) g^m g^n = g^{(m+n)} \in \langle g \rangle$$

$\Rightarrow \langle g \rangle$  si dice **gruppo ciclico** generato da  $g$ . Un gruppo  $G$  si dice **ciclico** se esiste  $g \in G$  t.c.  $G = \langle g \rangle$

$\Rightarrow$  dal teorema di Lagrange si ha che:

$|G|$  è un numero primo  $\Rightarrow G$  è ciclico.

$\Rightarrow$  infatti:

$|G| = p$  primo,  $g \in G$ ,  $g \neq 1$

$\Rightarrow \langle g \rangle \neq \{1\}$  ma  $|\langle g \rangle|$  è un divisore di  $p$

$\Rightarrow |\langle g \rangle| = p \wedge \langle g \rangle = G \quad \checkmark$

Un altro esempio:

Sia  $\langle (123\dots n) \rangle$  con  $(123\dots n) \in S_n$

$\Rightarrow \langle (123\dots n) \rangle$  ha  $n$  elementi ed è un gruppo ciclico.

N.B.

Ogni gruppo ciclico è abeliano (non vale il viceversa)

Esempio:

$(\mathbb{Q}, +)$  non è ciclico, ma è abeliano:

• certamente  $\langle 0 \rangle \neq \mathbb{Q}$

• sia  $a, b \neq 0 \in \mathbb{Q}$ , allora  $\frac{a}{2b} \notin \langle \frac{a}{b} \rangle$

$$\left( \frac{a}{2b} = n \frac{a}{b} \Rightarrow 1 = 2n \Rightarrow n \notin \mathbb{Z} \right)$$

---

Sottogruppi di  $\mathbb{Z}$ :

$\mathbb{Z}$  è un gruppo ciclico:  $\mathbb{Z} = \langle 1 \rangle$

Moltre, ogni sottogruppo di  $\mathbb{Z}$  è ciclico !!!

Infatti, sia  $H \subseteq \mathbb{Z}$  sottogruppo con  $H \neq \{0\}$ .

$\Rightarrow H$  contiene elementi positivi:

$$x \in H, x \neq 0 \Rightarrow -x \in H \Rightarrow x > 0 \vee -x > 0$$

$\Rightarrow$  sia  $n := \min_{x \in H} \{x \mid x > 0\} > 0$ . Se  $h \in H$ , si ha:

$h = nq + r$  con  $0 \leq r < n$  (divisione con resto)

$\Rightarrow r = h - qn$  con  $h, n \in \mathbb{N} \Rightarrow -qn \in \mathbb{N} \Rightarrow r \in \mathbb{N}$

$\Rightarrow$  se fosse  $r > 0$  si avrebbe una contraddizione:

sarebbe  $0 < r < n = \min_{x \in \mathbb{N}} \{x \mid x > 0\}$

$\Rightarrow r = 0 \Rightarrow h = nq \Rightarrow H = \langle n \rangle = \underbrace{n\mathbb{Z}}$   
notazione tradizionale

$\Rightarrow \{0\} = 0\mathbb{Z}$

$\Rightarrow$  i sottogruppi di  $\mathbb{Z}$  sono tutti e soli i sottovisori della forma  $n\mathbb{Z}$ ,  $n > 0 \in \mathbb{Z}$ . Inoltre:

$$m \neq n \Rightarrow m\mathbb{Z} \neq n\mathbb{Z}$$

(dato  $n\mathbb{Z}$ , si ha che  $n = \min_{x \in n\mathbb{Z}} \{x \mid x > 0\}$ )

$\Rightarrow$  la lista è completa e senza ripetizioni, quindi si ha una bizione tra  $\mathbb{Z}$  ed  $\mathbb{N}$ .

Cosa significa  $m\mathbb{Z} \subseteq n\mathbb{Z}$ ?

$\Rightarrow$  deve essere  $m \in n\mathbb{Z} \Rightarrow n \mid m$

$\Rightarrow$  se  $n \mid m$  allora ogni multiplo di  $m$  è multiplo di  $n$ , quindi  $m\mathbb{Z} \subseteq n\mathbb{Z}$ .

Siamo ora  $G$  gruppo abeliano,  $H, K$  sottogruppi di  $G$  t.c.

$HK = \{\alpha \cdot b \mid \alpha \in H, b \in K\}$  è sottogruppo abeliano di  $G$ :

$$1) \underset{H}{\frac{1}{1}} \cdot \underset{K}{\frac{1}{1}} \in HK$$

$$2) \alpha \in H, b \in K \Rightarrow (\alpha b)^{-1} = b^{-1} \underset{\substack{\uparrow \\ \in H}}{\alpha^{-1}} = \underset{\substack{\in H \\ \in K}}{\alpha^{-1} b^{-1}} \in HK$$

$b$  abeliano

$$3) \alpha_1, \alpha_2 \in H, b_1, b_2 \in K \Rightarrow (\alpha_1 b_1)(\alpha_2 b_2) = (\alpha_1 \alpha_2)(b_1 b_2) \in HK$$

Nel caso di  $(\mathbb{Z}, +)$  scriviamo:

$$H+K = \{a+b \mid a \in H, b \in K\}$$

Chi è  $m\mathbb{Z} + n\mathbb{Z}$ ?

$\Rightarrow m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$  ( $\subseteq \mathbb{Z}$ , quindi è della forma  $k\mathbb{Z}$ ,  $k \in \mathbb{Z}$ )

$\Rightarrow$  sicuramente si ha:

$$\cdot m\mathbb{Z} \subseteq m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$$

$$\cdot n\mathbb{Z} \subseteq m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$$

$\Rightarrow d|m$  e  $d|n$  ( $d$  divide sia  $m$  che  $n$ )

$$\Rightarrow d = \text{MCD}(m, n)$$

$\Rightarrow$  per dim. ciò, sia  $c$  t.c.  $c|m$ ,  $c|n$ , allora:

$$\begin{aligned} m &= cx, \quad n = cy \Rightarrow ma + nb = cax + cbx \\ &= c(ax + bx) \end{aligned}$$

$$\Rightarrow m\mathbb{Z} + n\mathbb{Z} \subseteq c\mathbb{Z} \Rightarrow d\mathbb{Z} \subseteq c\mathbb{Z} \Rightarrow c|d \quad \checkmark$$

$$\Rightarrow m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z} \quad \text{con } d = \text{MCD}(m, n)$$

$\Rightarrow$  dato che  $d \in d\mathbb{Z}$ ,  $\exists x, y \in \mathbb{Z}$  t.c.  $d = mx + ny$   
(Teorema di Bézout)

esercizio:

Caratterizzare  $\text{mcm}(m, n)$  mediante i sottogruppi di  $\mathbb{Z}$

$\Rightarrow$  si ha che:

$$m\mathbb{Z} \cap n\mathbb{Z} = l\mathbb{Z} \quad \text{con } l = \text{mcm}(m, n)$$