Lunedì 6 iniziamo alle ore 9; pomeriggio ore 15,30 - 17,45.
Farò molti esercizi, compresi esercizi a richiesta degli studenti.

$(G, \cdot)$ gruppo, $H \subseteq G$. Si dice che H è un sottogruppo di $(G, \cdot)$ se a sua volta è un gruppo.

Teorema 1. H è un sottogruppo di $(G, \cdot)$ se e solo se

$SG_1)$ $H \neq \emptyset$

$SG_2)$ $\forall a, b \in H \quad a \cdot b \in H$

$SG_3)$ $\forall a \in H \quad a^{-1} \in H$.

Teorema 2. H è un sottogruppo di $(G, \cdot)$ se e solo se

$SG_1')$ $1_G \in H$

$SG_2')$ $\forall a, b \in H \quad a \cdot b^{-1} \in H$.

Esempi 1. $\forall n \in \mathbb{Z}$ $\quad n \cdot \mathbb{Z} = \{ x \in \mathbb{Z} : \exists h \in \mathbb{Z}$ tale che $x = n \cdot h \} =$
$= \{ n \cdot h \; ; \; h \in \mathbb{Z} \} =$ insieme dei multipli di n

è un sottogruppo di $(\mathbb{Z}, +)$

2. $(S_n, \circ)$ il gruppo delle permutazioni su n oggetti che si chiama anche gruppo simmetrico

Il gruppo alterno A_n = insieme delle permutazioni di classe pari =

$= \{ f \in S_n : \Delta f = 1 \}$

$\Delta : S_n \longrightarrow \{-1, 1\}$ tale che $\forall f \in S_n$

$$\Delta(f) = \begin{cases} 1 & \text{se } f \text{ è di classe pari} \\ -1 & \text{" " " " " dispari.} \end{cases}$$

A_n è un sottogruppo di $(S_n, \circ)$.

Def. Sia $(G, \cdot)$ un gruppo. Si dice <u>ordine</u> di G e si indica con $|G|$ la cardinalità di G quando G è finito, oppure $+\infty$ se G è un insieme infinito.

$$|G| = \begin{cases} +\infty & \text{se } G \text{ è un insieme infinito} \\ \text{cardinalità di } G & \text{se } G \text{ è un insieme finito} \end{cases}$$

Teorema di Lagrange Sia $(G, \cdot)$ un gruppo finito con $|G| = n$ e sia H un sottogruppo di $(G, \cdot)$ con $|H| = h$.

Allora $h \mid n$.

Es. $|G| = 15$ H sottogruppo $|H| = 1, 3, 5, 15$.

Prop. Sia $(G, \cdot)$ un gruppo e sia $g \in G$. Si può considerare

$$H = \{ x \in G \,:\, \exists\, h \in \mathbb{Z} \text{ tale che } x = g^h \} =$$
$$= \{ g^h \,:\, h \in \mathbb{Z} \}.$$

Allora H è un sottogruppo di $(G, \cdot)$

Dim (Teorema 1).

$SG_1)$ $H \neq \emptyset$ perché $g = g^1 \in H$

$SG_2)$ siano $x, y \in H$; allora $\exists\, h, k \in \mathbb{Z}$ tali che

$$x = g^h \;\wedge\; y = g^k$$

risulta $\underline{\underline{x \cdot y}} = g^h \cdot g^k = g^{h+k} \underline{\underline{\in H}}$ perché esiste $t = h + k \in \mathbb{Z}$ tale che $x \cdot y = g^t$.

$SG_3)$ sia $x \in H$; allora esiste $h \in \mathbb{Z}$ tale che $x = g^h$; si ha $x^{-1} = (g^h)^{-1} = g^{-h} \in H$ perché esiste $s = -h \in \mathbb{Z}$ tale che $x^{-1} = g^s$, per cui $x^{-1} \in H$.

Osserv. Con le stesse notazioni della Prop. precedente, il sottogruppo H si chiama sottogruppo ciclico generato da g e si indica con

$$\underline{\langle g \rangle} = H$$

e g si dice generatore di H.

Osserv. Sia $(G, \cdot)$ un gruppo. Se esiste $g \in G$ tale che $\langle g \rangle = G$, allora si dice che $(G, \cdot)$ è un gruppo ciclico e che g ne è un generatore.

Esempi 1. $(\mathbb{Z}, +)$ è ciclico perché 1 ne è generatore (anche -1 è un generatore)

$\forall n \in \mathbb{N} \qquad n = n \cdot 1$

$\forall m < 0 \qquad -m > 0 \qquad m = -\big((-m) \cdot 1\big) = \big(-(-m)\big) \cdot 1 = m \cdot 1$

$(G, +) \quad g \in G \quad \langle g \rangle = \{ h \cdot g \ : \ h \in \mathbb{Z} \}$

2. $n \in \mathbb{N}^*$ $\quad (\mathbb{Z}_n, +)$ è un gruppo ciclico

infatti: $[1]_n$ ne è un generatore:

$\mathbb{Z}_n = \{ [0]_n, [1]_n, [2]_n, \dots, [n-1]_n \}$

$\forall [a]_n \in \mathbb{Z}_n \qquad 0 \leq a \leq n-1 \qquad [a]_n = a \cdot [1]_n = \underbrace{[1]_n + \dots + [1]_n}_{a \text{ volte}}$.

Prop. Sia $(G, \cdot)$ un gruppo e sia $g \in G$.

1. $\forall h, k \in \mathbb{Z} \quad g^h \neq g^k \iff \langle g \rangle$ è infinito

2. $\exists\, h,k \in \mathbb{Z}$ tali che $g^h = g^k \iff \langle g \rangle$ è finito.

Def. Sia $(G,\cdot)$ un gruppo e sia $g \in G$. Si dice ordine o periodo di g l'ordine del sottogruppo $\langle g \rangle$ generato da g. Si pone quindi

$$|g| = |\langle g \rangle| = \begin{cases} +\infty & \text{se } \langle g \rangle \text{ è infinito} \\ \text{cardinalità di } \langle g \rangle & \text{se } \langle g \rangle \text{ è finito.} \end{cases}$$

Esempio. $(S_n,\circ)$. Sia $(c_1 \dots c_h)$ un ciclo di lunghezza h. Si verifica allora che $|(c_1 \dots c_h)| = h$.

$$|(3\ 5\ 7\ 8\ 9)| = |\langle (3\ 5\ 7\ 8\ 9) \rangle| = 5 \quad \text{in } (S_{10},\circ)$$

Sia $f \in S_n$, $f = \sigma_1 \circ \sigma_2 \circ \dots \circ \sigma_r$ $\quad \sigma_1, \dots, \sigma_r$ cicli disgiunti

$$|f| = \text{m.c.m.}(|\sigma_1|, |\sigma_2|, \dots, |\sigma_r|)$$

Esercizio. $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 3 & 1 & 10 & 9 & 8 & 7 & 6 & 5 & 4 \end{pmatrix}$

(a) scomporre f in cicli e determinare la classe di permutazione di f

(b) calcolare l'ordine di f nel gruppo $(S_n,\circ)$.

(a) $f = (1\,2\,3) \circ (4\;10) \circ (5\,9) \circ (6\,8)$

f è di classe dispari

$$\Delta f = \Delta\left((1\,2\,3) \circ (4\;10) \circ (5\,9) \circ (6\,8)\right) =$$
$$= \Delta(1\,2\,3) \cdot \Delta(4\;10) \cdot \Delta(5\,9) \cdot \Delta(6\,8) =$$
$$= 1 \cdot (-1)\,(-1) \cdot (-1) = -1$$

$\Delta f = -1 \Rightarrow f$ è di classe dispari.

Altra soluzione.

$$f = (1\,3) \circ (1\,2) \circ (4\;10) \circ (5\,9) \circ (6\,8)$$

5 scambi e quindi f è di classe dispari.

(b) $|f| = \text{m.c.m.}\left(|(1\,2\,3)|, |(4\;10)|, |(5\,9)|, |(6\,8)|\right) =$
$= \text{m.c.m.}(3, 2, 2, 2) = 6.$

Teorema (teorema inverso del Teorema di Lagrange per gruppi ciclici)

Sia $(G, \cdot)$ un gruppo ciclico finito, con $|G| = n$. Allora per ogni k divisore di n esiste un unico sottogruppo di $(G, \cdot)$ avente ordine n.

Esempio: $(G, \cdot)$ gruppo $|G| = 15$, $(G, \cdot)$ ciclico. Allora

esiste un unico sottogruppo di $(G,\cdot)$ di ordine 1 $\{1_G\}$
" " " " " " " " 3
" " " " " " " " 5
" " " " " " " " 15 G

Osserv. $(G,\cdot)$ gruppo $H=\{1_G\}$ è un sottogruppo di $(G,\cdot)$

SG1) $H\neq\emptyset$ perché $1_G\in H$

SG2) $\forall x,y\in H$ $x\cdot y\in H$ vero perché

$\forall x,y\in H$ $x=1_G$ $y=1_G$ e quindi $x\cdot y=1_G\cdot 1_G=1_G$

SG3) $\forall x\in H$ $x^{-1}\in H$ perché

$\forall x\in H$ $x=1_G$ $x^{-1}=(1_G)^{-1}=1_G\in H$

H sottogruppo banale $H=\langle 1_G\rangle=\{1_G^h ; h\in\mathbb{Z}\}$.

<u>Prop.</u> Sia $(G,\cdot)$ un gruppo ciclico finito, $|G|=n$ e sia $g\in G$ un generatore. Allora $\forall x\in G$

$\exists h\in\mathbb{Z}$ tale che $x=g^h$

$$|x|=|g^h|=\frac{n}{M.C.D.(h,n)}.$$

Caso della notazione additiva.

$(G,+)$ gruppo ciclico $\quad |G| = n \qquad G = \langle g \rangle$

$\forall x \in G \ \exists\, h \in \mathbb{Z}$ tale che $\quad x = h \cdot g$

$$|x| = |hg| = \frac{n}{M.C.D.(h,n)}.$$

Esempio $(\mathbb{Z}_{12},+)$ ciclico $\qquad \mathbb{Z}_{12} = \langle [1]_{12} \rangle$

$[6]_{12} = 6 \cdot [1]_{12}$

$$|[6]_{12}| = |\langle [6]_{12} \rangle| \qquad ?$$

$$|[6]_{12}| = |6[1]_{12}| = \frac{12}{M.C.D.(6,12)} = \frac{12}{6} = 2$$

$$\langle [6]_{12} \rangle = \{ 0 \cdot [6]_{12} = [0]_{12},\ 1 \cdot [6]_{12} = [6]_{12} \} =$$
$$= \{ [0]_{12}, [6]_{12} \}$$

	$[0]_{12}$	$[6]_{12}$
$[0]_{12}$	$[0]_{12}$	$[6]_{12}$
$[6]_{12}$	$[6]_{12}$	$[0]_{12}$

$12 \equiv 0 \pmod{12}$

$$[5]_{12} = 5 \cdot [1]_{12}$$

$$|[5]_{12}| = |5[1]_{12}| = \frac{12}{M.C.D.(5,12)} = \frac{12}{1} = 12$$

$[5]_{12}$ è generatore perché $|\langle [5]_{12} \rangle| = 12 = |\mathbb{Z}_{12}|$

$$[9]_{12} = 9[1]_{12}$$

$$|[9]_{12}| = |9[1]_{12}| = \frac{12}{M.C.D.(9,12)} = \frac{12}{3} = 4$$

$$|[3]_{12}| = |3 \cdot [1]_{12}| = \frac{12}{M.C.D.(3,12)} = \frac{12}{3} = 4$$

$$\langle [9]_{12} \rangle = \langle [3]_{12} \rangle$$

$$\overset{\mathbb{Z}}{n} \cdot g \longrightarrow G$$

$$n \cdot g = \underbrace{g + g + \dots + g}_{n\text{-volte}} \qquad n > 0$$

$$n < 0 \qquad ng = -((-n)g).$$

Osserv. Sia $(G, \cdot)$ un gruppo ciclico finito $|G| = n$.

Allora un elemento $a \in G$ è un generatore di G se e solo se $|a| = |\langle a \rangle| = n$.

$\langle a \rangle \subseteq G$

In generale: Sia A insieme finito $|A| = n$
sia $B \subseteq A$ $|B| = n$

allora. $B = A$ $(A \subset B)$