

Estratti sul calcolo combinatorio.

- Quante parole di lunghezza 5 (anche più di significato) si possono formare con le lettere dell'alfabeto inglese?

26 lettere

Corrisponde al numero delle disposizioni con ripetizioni di 26 oggetti di classe 5

$$26^5 =$$

- Il numero delle targhe è:

$$\underline{26} \cdot \underline{26} \cdot 10 \cdot 10 \cdot 10 \cdot \underline{26} \cdot \underline{26} =$$

- Quanti numeri con cifre tutte diverse e con 5 cifre si possono formare con le cifre da 1 a 9?

Disposizioni semplici di 9 oggetti di classe 5

$$(9)_5 = 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 = 15.120.$$

- Quanti numeri con cifre tutte diverse e con 5 cifre si possono formare con le cifre da 0 a 9?

5. In quanti modi si può scegliere tra le 12 persone che formano un'associazione una rosa di 3 per le cariche di presidente, vicepresidente e segretario, se si vuole che una persona non ricopra più di una delle 3 cariche?

$$\begin{matrix} 4 & 4 & 4 \\ 1 & 2 & 3 \end{matrix}$$

Disposizioni semplici di 12 oggetti di classe 3.

$$12 - 3 + 1 = 10$$

$$(12)_3 = 12 \cdot 11 \cdot 10 = 1.320$$

6. Se ci sono 3 tipi di panini e 6 tipi di affettati, in quanti modi si possono fare dei sandwich?

$$3 \cdot 6 = 18 \text{ tipi}$$

(corrisponde alla cardinalità del prodotto cartesiano di un insieme di 3 elementi su un insieme di 6 elementi)

7. Se ci sono 3 tipi di panini 6 tipi di affettati e 2 tipi di formaggi, in quanti modi si possono preparare dei sandwich?

$$3 \cdot 6 \cdot 2 = 36$$

8. Un bambino deve colorare 6 fiori e ha a disposizione 8 colori. In quanti modi lo può fare se vuole colorare i fiori con colori tutti diversi? E se non vuole colorare i fiori con colori tutti diversi?

La prima risposta: è il numero delle disposizioni semplici di 8 oggetti di classe 6

$$\begin{matrix} \text{U} & \text{U} & \text{U} & \text{U} & \text{U} & \text{U} \\ 8 & 7 & 6 \end{matrix}$$

$$8 - 6 + 1 = 3$$

$$(8)_6 = 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 = 20.160.$$

Le seconde risposte: è il numero delle disposizioni con ripetizioni di 8 oggetti di classe 6:

$$8^6 = 262.144.$$

9. Un insegnante chiede di formare un gruppo di studio di 5 ragazzi in una classe di 25 alunni. In quanti modi si può formare tali gruppi?

Il numero cercato corrisponde alle combinazioni senza ripetizioni

di 25 oggetti di classe 5.

$$\binom{25}{5} = \frac{(25)_5}{5!} = \frac{\cancel{25}^5 \cdot \cancel{24}^6 \cdot \cancel{23}^7 \cdot \cancel{22}^8 \cdot \cancel{21}^9}{\cancel{5} \cdot \cancel{4} \cdot \cancel{3} \cdot \cancel{2} \cdot \cancel{1}} = 5 \cdot 6 \cdot 23 \cdot 11 \cdot 7 =$$

$25 - 5 + 1 = 21$  = 53.130.

$$(k)_n = k \cdot (k-1) \cdot \dots \cdot (k-n+1)$$

10. Determinare il numero degli anagrammi delle parole

CALESSE

$$\frac{7!}{2!2!} = \frac{7 \cdot 6 \cdot 5 \cdot \cancel{4}^2 \cdot \cancel{3}^2 \cdot \cancel{2} \cdot \cancel{1}}{(\cancel{7})(\cancel{2})} = 7 \cdot 6 \cdot 5 \cdot 2 \cdot 3 = 1.260$$

11. Determinare il numero degli anagrammi delle parole

VERCINGETORIGE

$$\frac{14!}{3!2!2!2!} = \frac{14 \cdot 13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot \cancel{7}^3 \cdot \cancel{6}^2 \cdot \cancel{5}^3 \cdot \cancel{4}^2 \cdot \cancel{3}^2 \cdot \cancel{2}^2 \cdot \cancel{1}}{3 \cdot \cancel{2} \cdot \cancel{1} \cdot \cancel{2} \cdot \cancel{1} \cdot \cancel{2} \cdot \cancel{1}} =$$

$$= 14 \cdot 13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 5 \cdot 3 =$$

12. Quante combinazioni con ripetizioni si possono formare con i 3 elementi  $\{a, b, c\}$  di classe 4

$$6-4+1 = 3$$

$$\binom{k+n-1}{n} = \binom{3+4-1}{4} = \binom{6}{4} = \frac{(6)_4}{4!} =$$

$$= \frac{6 \cdot 5 \cdot 4 \cdot 3}{4 \cdot 3 \cdot 2} = 15$$

$a, a, a, a$

0,1 di lunghezza 6 ciascuna combinazione

$$k+n-1 = 3+4-1$$

1 1 1 1 0 0

a a a a

1 1 1 0 1 0

a a a b

1 1 0 1 1 0

a a b b

1 0 1 1 1 0

a b b b

0 1 1 1 1 0

b b b b

1 1 0 1 0 1

a a b c

1 0 1 1 0 1

a b b c

0 1 1 1 0 1

b b b c

Escrivre com l'exercice 12 {a,b,c,d} la lunghezza 5

Mutno :  $\binom{4+5-1}{5} = \binom{8}{5} = \frac{(8)_5}{5!} =$

$$k+n-1 = 4+5-1 = 8$$

1 1 1 1 1 0 0 0

a a a a a

1 1 0 0 1 0 1 1

a a c d d

1 0 1 0 1 1 0 1

a b c c d

$(G, \cdot)$  gruppo,  $a \in G$

$$\langle a \rangle = \{a^h : h \in \mathbb{Z}\}$$

è un sottogruppo di  $G$   
che si dice sottogruppo  
ciclico generato da  $a$

ordine o periodo di  $a$

$$|a| = |\langle a \rangle| = \begin{cases} +\infty & \text{se } \langle a \rangle \text{ è infinito} \\ n \in \mathbb{N}^* & \text{se } \langle a \rangle \text{ è finito.} \end{cases}$$

$$(G, +) \quad \langle a \rangle = \{ha : h \in \mathbb{Z}\}.$$

Osserv. Si possono avere sottogruppi (anche ciclici)  
finiti di un gruppo infinito: per esempio  
 $(\mathbb{Q}^*, \cdot)$  è un gruppo non ciclico (si dimostri)

$$\langle -1 \rangle = \{(-1)^h : h \in \mathbb{Z}\} = \{1, -1\} \subset \mathbb{Q}^*$$

$$|-1| = 2 \text{ finito.}$$

$(\mathbb{Z}, +)$ ,  $(\mathbb{Z}_n, +)$  sono ciclici  
 $\stackrel{\downarrow}{1}$   $\stackrel{\uparrow}{[1]_n}$  genera  $\mathbb{Z}_n$

$$\mathbb{Z} = \langle 1 \rangle$$

$$\mathbb{Z}_n = \langle [1]_n \rangle$$

Osserv. Sia  $(G, \cdot)$  un gruppo finito  $|G| = n$ . Allora un elemento  $g \in G$  è un generatore se e solo se  $|g| = |\langle g \rangle| = n$ . In conclusione possiamo dire che  $(G, \cdot)$  è un gruppo ciclico se e solo se esiste un elemento  $g \in G$  tale che  $|g| = n$ .

### Esercizio

1. Dimostrare che se  $(G, \cdot)$  è un gruppo tale che  $|G| = p$  numero primo, allora  $(G, \cdot)$  è un gruppo ciclico.
2. Dimostrare che un gruppo ciclico è abeliano.

Dim. 1.  $p \neq 1$        $|G| = p$  e quindi se

$$g \in G \quad |g| = \begin{cases} 1 \\ p \end{cases}$$

questo per il Teorema di Lagrange  $((G, \cdot) \text{ gruppo } |G| = n; H \text{ sottogruppo di } (G, \cdot) \text{ con } |H| = h. \text{ Allora } h \mid n)$

$$|g|=1 \Rightarrow g = 1_G$$

Se  $g \neq 1_G$  allora  $\langle g \rangle \neq \{1_G\}$  perché

$g \in \langle g \rangle$  ma  $g \neq g^1$  e quindi  $|g| \neq 1$ ; quindi

$|g|=p$  e quindi per l'osserv.  $g$  è generatore di  $(G, \cdot)$  per cui  $(G, \cdot)$  è un gruppo ciclico.

2. Sia  $(G, \cdot)$  un gruppo ciclico di cui  $g \in G$  sia un generatore. Allora

$$\langle g \rangle = \{g^h : h \in \mathbb{Z}\} = G$$

$(G, \cdot)$  è abeliano:  $\forall a, b \in G \quad a \cdot b = b \cdot a$

Siamo  $a, b \in G = \{g^h : h \in \mathbb{Z}\}$ : allora esistono  $h, k \in \mathbb{Z}$

tali che  $a = g^h, b = g^k$ . Allora:

$$a \cdot b = g^h \cdot g^k = g^{h+k} = g^{k+h} = g^k \cdot g^h = b \cdot a$$

Conseguenza: Sia  $(G, \cdot)$  un gruppo con  $|G|=p$  numero

mino. Allora  $(G, \cdot)$  è abeliano.

$(S_2, \circ)$  è ciclico perché  $|S_2| = 2! = 2$  mino e quindi è ciclico:

$$S_2 = \{ \text{id}_2, (12) \} = \langle (12) \rangle = \left\{ (12)^0 = \text{id}_2, (12)^1 = (12) \right\}$$

$$\text{id}_2 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \quad (12) = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

$$(S_3, \circ) \text{ non è abeliano: } (12) \circ (13) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} =$$
$$= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (132)$$

$$(13) \circ (12) = (123)$$

$$(12) \circ (13) \neq (13) \circ (12)$$

$\forall n \in \mathbb{N}^*, n \neq 1, 2 \quad (S_n, \circ) \text{ non è abeliano e quindi non è ciclico.}$

Prop. Sia  $(G, \cdot)$  un gruppo,  $a \in G$ ,  $|a| = m \in \mathbb{N}$ :

allora  $m = \min \{ h \in \mathbb{N}^* : a^h = \frac{1}{a} \}$ .

Abbiamo visto che se  $(G, \cdot)$  è un gruppo ciclico finito,  $|G| = n \in \mathbb{N}^*$ , con  $G = \langle g \rangle$ .  $g \in G$ .

Ha  $\forall a \in G \exists h \in \mathbb{Z}$  tale che  $a = g^h$

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

Pn esempio  $(\mathbb{Q}^*, \cdot)$  non è ciclico

$$|-1| = 2$$

$$(-1)^2 = 1$$

cioè 2 è il più piccolo intero positivo tale che  $(-1)^2 = 1$

$$\left\langle \frac{1}{2} \right\rangle = \left\{ \frac{1}{2^n} ; n \in \mathbb{Z} \right\} = \left\{ \dots, 4, 2, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \dots \right\}$$

$$2 = \left(\frac{1}{2}\right)^{-1} \quad n = \left(\frac{1}{2}\right)^{-2} - - -$$

$$\left(\frac{1}{2}\right)^h \neq \left(\frac{1}{2}\right)^k \quad \text{e} \quad h \neq k$$

Esempio<sup>3</sup>  $(\mathbb{Z}_n, \circ)$   $|f| = m \cdot c - m \cdot (|\sigma_1|, \dots, |\sigma_n|)$  dove  
 $f = \sigma_1 \circ \dots \circ \sigma_n$   $\sigma_1, \dots, \sigma_n$  ordini disgiunti

$$f = id_n \circ f^1 \circ f^2 \circ f^3 \circ \dots \circ f^{\text{ord}} = id_m$$

$$h = |f| = |\langle f \rangle|.$$

Q.  $(\mathbb{Z}_8, +)$   $[\langle \rangle]_8$  ~~è~~ ordine?

$$[6]_8, 2 \cdot [6]_8 = [12]_8 = [4]_8, 3 \cdot [6]_8 = [18]_8 = [2]_8,$$

$$4 \cdot [6]_8 = [24]_8 = [0]_8$$

$$\text{Allora: } |\langle 6 \rangle_8| = 4$$

$$\text{Altro modo } |\langle 6 \rangle_8| = |\text{GCD}(1, 8)| = \frac{8}{\text{M.C.D.}(6, 8)} = \frac{8}{2} = 4.$$

Prop. Consideriamo il monoido  $(\mathbb{Z}_n, \circ)$   $n \in \mathbb{N}^*, n \neq 1$ .  
Se  $[a]_n \in \mathbb{Z}_n$ ,  $[a]_n$  è invertibile se e solo se  
 $\text{M.C.D.}(a, n) = 1$ .

Dim.  $[a]_n \in \mathbb{Z}_n$  è invertibile se e solo se esiste  $[x]_n \in \mathbb{Z}_n$  tale che  $[a]_n \cdot [x]_n = [1]_n$ .  
 ovvero  $[a \cdot x]_n = [1]_n$   $\underbrace{x \cdot a = 0}_{\text{e } a \neq 0} \quad 0 \cdot x \equiv 1 \pmod{n}$ ,

cioè  $a \cdot x \equiv 1 \pmod{n}$

esiste  $[x]_n \in \mathbb{Z}_n$  inverso di  $[a]_n$  se e solo se esiste una soluzione delle congruenze lineare  $a \cdot x \equiv 1 \pmod{n}$ .

e ciò avviene se e solo se  $\text{M.C.D.}(a, n) = 1$ .

Più esempio  $(\mathbb{Z}_8, \cdot)$

gli elementi invertibili sono  $[1]_8, [3]_8, [5]_8, [7]_8$

$$[1]_8^{-1} = [1]_8$$

$$[3]_8^{-1} = [3]_8$$

$$[3]_8 \cdot [3]_8 = [9]_8 = [1]_8$$

$$[5]_8^{-1} = [5]_8$$

$$[5]_8 \cdot [5]_8 = [25]_8 = [1]_8$$

$$[\mathbb{F}]_g^{-1} = [\mathbb{F}]_g$$

$$[\mathbb{F}]_g \cdot [\mathbb{F}]_g = [49]_g = [1]_g.$$

Esempio:  $(\mathbb{Z}_7, \cdot)$

$$[1]_7, [2]_7, [3]_7, [4]_7, [5]_7, [6]_7$$

Sono tutt' e invisiibili

$$[1]_7^{-1} = [1]_7$$

$$[2]_7^{-1} = [4]_7$$

$$[3]_7^{-1} = [5]_7$$

$$[6]_7^{-1} = [6]_7$$

$$[2]_7 \cdot [4]_7 = [8]_7 = [1]_7$$

$$[3]_7 \cdot [5]_7 = [15]_7 = [1]_7$$

$$[6]_7 \cdot [6]_7 = [36]_7 = [1]_7.$$

$(\mathbb{Z}_7^*, \cdot)$  è un gruppo abeliano.

Prop. Sia  $p$  un numero primo. Allora  $\mathbb{Z}_p^*$  è chiuso nel monoido  $(\mathbb{Z}_p, \cdot)$ .

$$\text{Dim. } \forall [a]_p, [b]_p \in \mathbb{Z}_p^* \quad [a]_p \cdot [b]_p \in \mathbb{Z}_p^*$$

in altri termini se  $[a]_p \neq [0]_p$  e  $[b]_p \neq [0]_p$ ,  
allora  $[a]_p \cdot [b]_p \neq [0]_p$ .

Se fosse  $[a]_p \cdot [b]_p = [0]_p$ , allora si potrebbe moltiplicare per  $[a]_p^{-1}$  - che esiste perché M.C.D.  $(a, p) = 1$

$$[a]_p^{-1} \cdot ([a]_p \cdot [b]_p) = [a]_p^{-1} \cdot [0]_p = [a \cdot 0]_p = [0]_p$$

$$([a]_p^{-1} \cdot [a]_p) \cdot [b]_p = [0]_p$$

$$[1]_p \cdot [b]_p = [0]_p$$

$$[b]_p = [0]_p \quad \text{contraddizione}$$

Le proposizioni precedente ci permette di considerare

$$\cdot : \mathbb{Z}_p^* \times \mathbb{Z}_p^* \rightarrow \mathbb{Z}_p^*$$

$$([a]_p, [b]_p) \mapsto [a]_p \cdot [b]_p$$

Osserv.  $(\mathbb{Z}_p^*, \cdot)$  è un gruppo abeliano.

Abbiamo  $(\mathbb{Z}_2^*, \cdot)$   $\mathbb{Z}_2^* = \{[1]_2\}$

$$(\mathbb{Z}_3^*, \cdot) \quad \mathbb{Z}_3^* = \{[1]_3, [2]_3\}$$

$$(\mathbb{Z}_5^*, \cdot) \quad \mathbb{Z}_5^* = \{[1]_5, [2]_5, [3]_5, [4]_5\}$$

$$(\mathbb{Z}_7^*, \cdot) \quad \mathbb{Z}_7^* = \{[1]_7, [2]_7, [3]_7, [4]_7, [5]_7, [6]_7\}$$

⋮

$\forall p \in \mathbb{N}_1$  per primo  $(\mathbb{Z}_p^*, \cdot)$  è un gruppo ciclico.

Esempio (1)  $(\mathbb{Z}_3^*, \cdot)$   $\mathbb{Z}_3^* = \{[1]_3, [2]_3\}$

$$\langle [1]_3 \rangle = \{[1]_3\} \neq \mathbb{Z}_3^*$$

$$\begin{aligned} \langle [2]_3 \rangle &= \{[2]_3^1 = [2]_3, [2]_3^2 = [4]_3 = [1]_3\} = \\ &= \{[2]_3, [1]_3\} = \mathbb{Z}_3^* \end{aligned}$$

(2)  $(\mathbb{Z}_5^*, \cdot)$   $\mathbb{Z}_5^* = \{[1]_5, [2]_5, [3]_5, [4]_5\}$

$[1]_5$  non può essere generatore

$$\langle [2]_5 \rangle = \{[2]_5^1 = [2]_5, [2]_5^2 = [4]_5, [2]_5^3 = [8]_5 = [3]_3,$$

$$[2]_5^4 = [16]_5 = [1]_5\} = \mathbb{Z}_5^*$$

$[2]_5$  è un generatore di  $\mathbb{Z}_5^*$ .  $|\mathbb{Z}_5^*| = 4$

$$|[2]_5| = 4$$

$$|[4]_5| = |[2]_5^2| = \frac{4}{\text{M.C.D.}(2, 4)} = \frac{4}{2} = 2$$

$$|[3]_5| = |[2]_5^3| = \frac{4}{\text{M.C.D.}(3, 4)} = \frac{4}{1} = 4$$

Anche  $[3]_5$  è un generatore di  $(\mathbb{Z}_5^*, \cdot)$

$$|[1]_5| = 1$$

$$(3) (\mathbb{Z}_7^*, \cdot) \quad |\mathbb{Z}_7^*| = 6$$

Cerchiamo un generatore

$$\langle [2]_7 \rangle = \left\{ [2]_7^1 = [2]_7, [2]_7^2 = [4]_7, [2]_7^3 = [8]_7 = [1]_7 \right\}$$

Allora  $|[2]_7| = 3$  perché

$$3 = \min \left\{ h \in \mathbb{N}^* : [2]_7^h = [1]_7 \right\}$$

Affirme  $[2]_7$  non è generatore.

$$\langle [3]_7 \rangle = \{ [3]_7^1 = \underline{\underline{[3]}}_7, [3]_7^2 = [9]_7 = \underline{\underline{[2]}}_7, [3]_7^3 = [27]_7 = \underline{\underline{[6]}}_7,$$

$$[3]_7^4 = [3]_7^3 \cdot [3]_7 = [6]_7 \cdot [3]_7 = [18]_7 = \underline{\underline{[4]}}_7,$$

$$[3]_7^5 = [3]_7^4 \cdot [3]_7 = [6]_7 \cdot [3]_7 = [12]_7 = \underline{\underline{[5]}}_7,$$

$$[3]_7^6 = [3]_7^5 \cdot [3]_7 = [5]_7 \cdot [3]_7 = [15]_7 = \underline{\underline{[1]}}_7 \} =$$

$$6 = \min \{ h \in \mathbb{N}^* : [3]_7^h = [1]_7 \} \Rightarrow |[3]_7| = 6 = |\mathbb{Z}_7^*|.$$

Affirme  $[3]_7$  è un generatore di  $(\mathbb{Z}_7^*, \cdot)$

$$|[1]_7| = 1$$

$$|[2]_7| = |[3]_7^2| = \frac{6}{\text{M.C.D.}(2,6)} = \frac{6}{2} = 3$$

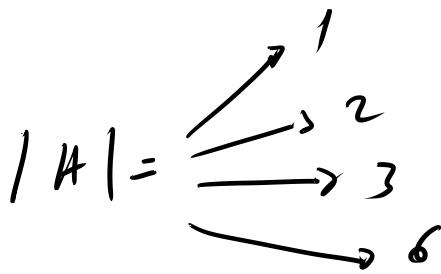
$$|[3]_7| = 6 \quad (\text{non si può usare } \frac{m}{\text{M.C.D.}(1,m)})$$

$$|[4]_7| = |[3]_7^4| = \frac{6}{\text{M.C.D.}(4,6)} = \frac{6}{2} = 3$$

$$|[5]_7| = |[3]_7^5| = \frac{6}{\text{M.C.D.}(5,6)} = \frac{6}{1} = 6$$

generatori  $[3]_7, [5]_7$ .

$$H \subset \mathbb{Z}_7^*$$



Teorema. Ogni sottogruppo di un gruppo ciclico è ciclico.

Esercizio (Luglio 2021)

E' assegnato il gruppo abeliano  $(\mathbb{Z}_8, +)$ .

(a) calcolare  $[2]_8 - [7]_8 = [2]_8 + (-[7]_8)$

(b) determinare i generatori di  $(\mathbb{Z}_8, +)$

(c) determinare gli ordini  $[2]_8, [5]_8$  in  $(\mathbb{Z}_8, +)$ .

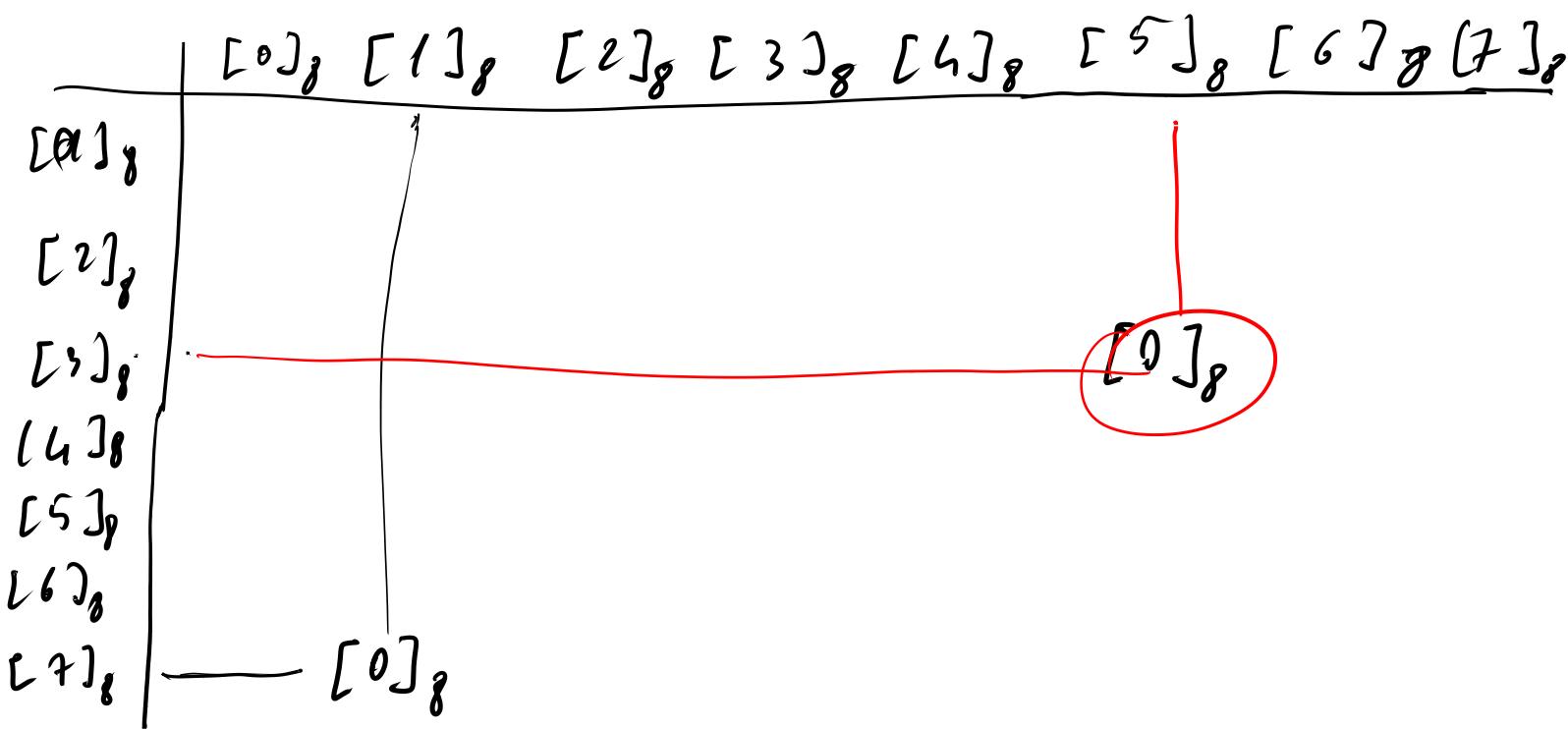
(a)  $[2]_8 - [7]_8 \in [2]_8 + (-[7]_8)$

$-[7]_8$  è l'opposto di  $[7]_8$  in  $(\mathbb{Z}_8, +)$

$$-[7]_8 = [1]_8 \quad \text{perché} \quad [7]_8 + [1]_8 = [8]_8 = [0]_8$$

Quindi  $[2]_8 - [7]_8 = [2]_8 + [1]_8 = [3]_8$ .

Per esercizio scrivete la tabella di  $(\mathbb{Z}_8, +)$ .



(b) Un elemento  $[a]_n \in \mathbb{Z}_n$  è generatore di  $(\mathbb{Z}_n, +)$  se e solo se  $\text{M.C.D.}(a, n) = 1$ .

Quindi sono generatori:  $[1]_8, [3]_8, [5]_8, [7]_8$ .

$$(c) |[2]_8| = |\cancel{2}|_{\cancel{8}} = \frac{8}{\text{M.C.D.}(2, 8)} = \frac{8}{2} = 4$$

$|[5]_8| = 8$  perché sappiamo che è generatore

$$|[4]_8| = |\cancel{4}|_{\cancel{8}} = \frac{8}{\text{M.C.D.}(4, 8)} = \frac{8}{4} = 2$$

$$|[6]_8| = |\underline{\underline{6}} \cdot [1]_8| = \frac{8}{\text{H.C.D.}(6, 8)} = \frac{8}{2} = 4$$

$$\langle [h]_8 \rangle = \{ 1 \cdot [h]_8 = [h]_8, 2 \cdot [h]_8 = [8]_8 = [0]_8 \}$$

$$\langle [2]_8 \rangle = \{ 1 \cdot [2]_8 = [2]_8, 2 \cdot [2]_8 = [4]_8, 3 \cdot [2]_8 = [6]_8, 4 \cdot [2]_8 = [8]_8 = [0]_8 \}$$

$$h = \min \{ h \in \mathbb{N}^*: h \cdot [2]_8 = [0]_8 \} = \underline{\underline{\langle [6]_8 \rangle}}$$

calcolo  
per esercizio

Esercizi  $\left[ (S_{n,0}) \text{ è un gruppo non abeliano} \right]$

1. E' assegnata la permutazione su 8 oggetti

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 3 & 2 & 1 & 6 & 7 & 5 & 4 \end{pmatrix},$$

- (a) scrivere  $f$  come prodotto di cicli disgiunti di scambi e calcolare la classe di permutazione  
(b) calcolare l'ordine di  $f$  come elemento del gruppo  $(S_{8,0})$   
(c) determinare gli elementi del sottogruppo ciclico  $\langle f \rangle$  generato da  $f$   
(d) calcolare  $f^2, f^{-1}$ .

(a)  $f = (\underline{1 \ 8 \ 4}) \circ (2 \ 3) \circ (\underline{5 \ 6 \ 7})$   $f$  come prodotto di cicli disgiunti

la classe di permutazione può essere pari o dispari

$$f = (\underline{1 \ 4}) \circ (\underline{1 \ 8}) \circ (2 \ 3) \circ (\underline{5 \ 7}) \circ (\underline{5 \ 6})$$

$\uparrow$   
 $\}$

$$(c_1 c_2 \dots c_n) = (c_1 c_n) \circ (c_1 c_{n-1}) \circ \dots \circ (c_1 c_2)$$

$f$  si può scrivere come prodotto di 5 scambi e quindi  $f$  è di classe dispari.

$$f = (\underline{1 \ 4}) \circ (\underline{1 \ 8}) \circ (\underline{2 \ 5}) \circ (\underline{2 \ 5}) \circ (\underline{id_8}) \circ (2 \ 3) \circ (\underline{5 \ 7}) \circ (\underline{5 \ 6})$$

7 scambi  
dispari

$$(b) \quad f \in S_m \quad f = \tilde{\sigma}_1 \circ \dots \circ \tilde{\sigma}_n \quad \tilde{\sigma}_1, \dots, \tilde{\sigma}_n \text{ sono cicli disgiunti} \\ |f| = \text{m.c.m. } (|\tilde{\sigma}_1|, \dots, |\tilde{\sigma}_n|)$$

inoltre  $|(c_1 \dots c_r)| = r$  lunghezza del ciclo

Un ciclo di lunghezza  $r$  ha ordine  $r$  in  $(S_m)$   
 cioè il sottogruppo ciclico da esso generato ha ordine  
 (ovvero cardinalità)  $r$ .

$$(c_1 \dots c_r)^r = \text{id}_S$$

$$|f| = \text{m.c.m.} \left( |(184)|, |(23)|, |(567)| \right) = \text{m.c.m.}(3, 2, 3) = 6$$

ciò vuol dire che  $|\langle f \rangle| = 6$ .

$$(c) \quad \langle f \rangle = \{ f^h : h \in \mathbb{Z} \} = \{ f^1 = f, f^2, f^3, f^4, f^5, f^6 = \text{id}_8 \} \quad +$$

perché  $|f| = \min \{ h \in \mathbb{Z} : f^h = \text{id}_8 \}$

$$f^2 = f \circ f = ((184) \circ (23) \circ (567))^2 = (184)^2 \circ (23)^2 \circ (567)^2 =$$

$\downarrow$   
"id<sub>8</sub>

$$(184) \circ (23) \circ (567) \circ (184) \circ (23) \circ (567)$$

in generale, se  $(G, \cdot)$  non è abeliano, se  $a, b \in G$  e  $n \in \mathbb{Z}$

$$\underbrace{(a \cdot b)}_{}^n \neq a^n b^n$$

può se  $a \cdot b = b \cdot a$ , altrimenti  $(a \cdot b)^n = (b \cdot a)^n$

$$= (148) \circ \text{id}_8 \circ (576) = \underline{(148) \circ (576)}$$

$$f^3 = (184)^3 \circ (23)^3 \circ (567)^3 = \text{id}_8 \circ (23) \circ \text{id}_8 = (23)$$

$(23)^3 = (23)^2 \circ (23) = (23)$

$$f^4 = f^3 \circ f = (23) \circ (184) \circ (23) \circ (567) = (184) \circ (567)$$

$$f^5 = f^4 \circ f = (184) \circ (567) \circ (184) \circ (23) \circ (567) = \\ = (184)^2 \circ (23) \circ (567)^2 = (148) \circ (23) \circ (576)$$

$$f^6 = (184)^6 \circ (23)^6 \circ (567)^6 = \text{id}_8 \circ \text{id}_8 \circ \text{id}_8 = \text{id}_8 - \\ (184)^6 = ((184)^3)^2 = \text{id}_8^2 = \text{id}_8$$

$$\langle f \rangle = \{ (184) \circ (23) \circ (567), (148) \circ (576), (23), (184) \circ (567), \\ (148) \circ (23) \circ (576), \text{id}_8 \} .$$

$$(d) \quad f^2 = (148) \circ (576) \quad f^{-1} = f^5 = (148) \circ (23) \circ (576)$$

we have  $f^5 \circ f = f^6 = \text{id}_8$

$$f^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 3 & 2 & 1 & 6 & 7 & 5 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 3 & 2 & 1 & 6 & 7 & 5 & 4 \end{pmatrix} = \\ = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 2 & 3 & 8 & 7 & 5 & 6 & 1 \end{pmatrix} = (148) \circ (576) \quad \}$$

another mode

$$f^2 = ((184) \circ (23) \circ (567))^2 = (\underline{184})^2 \circ (\underline{23})^2 \circ (\underline{567})^2 = \\ = (148) \circ \text{id}_8 \circ (576) = (148) \circ (576)$$

## ANELLI

Def. Si dice anello una terna ordinata  $(A, +, \cdot)$  dove  $A$  è un insieme non vuoto che si dice sostegno;  $+$  e  $\cdot$  sono leggi di composizione interne su  $A$  in modo che la struttura algebrica  $(A, +)$  sia un gruppo abeliano e la struttura algebrica  $(A, \cdot)$  sia associativa. Valgono inoltre le proprietà distributive:  $\forall a, b, c \in A$  risulta

$$(a+b) \cdot c = a \cdot c + b \cdot c$$

$$c \cdot (a+b) = c \cdot a + c \cdot b.$$

Se esiste l'elemento neutro rispetto a  $\cdot$ , allora si dice che  $(A, +, \cdot)$  è un anello con unità; se vale le proprietà commutative rispetto a  $\cdot$ , allora  $(A, +, \cdot)$  si dice anello commutativo.

Studiamo solo gli anelli con unità: li chiameremo semplicemente anelli. Si indica con  $0$  (oppure con  $0_A$ ) l'elemento neutro del gruppo abeliano  $(A, +)$ ; si indica con  $1$  (oppure con  $1_A$ ) l'elemento neutro della struttura algebrica  $(A, \cdot)$ .

Esempio (1)  $(\mathbb{Z}, +, \cdot)$  è un anello commutativo

purché:  $(\mathbb{Z}, +)$  è un gruppo abeliano

$(\mathbb{Z}, \cdot)$  è un monoido commutativo

l'elemento neutro di  $(\mathbb{Z}, +)$  è 0; l'elemento neutro  
di  $(\mathbb{Z}, \cdot)$  è 1.

$$\forall a, b, c \in \mathbb{Z} \quad (a+b) \cdot c = a \cdot c + b \cdot c; \quad c \cdot a + c \cdot b = c(a+b)$$

(2)  $(\mathbb{Q}, +, \cdot)$  anello commutativo

(3)  $(\mathbb{R}, +, \cdot)$  " "

(4)  $(\mathbb{Z}_n, +, \cdot)$  " "

$(\mathbb{Z}_n, +)$  gruppo abeliano con elemento neutro  $[0]_n$

$(\mathbb{Z}_n, \cdot)$  monoido commutativo con elem. neutro  $[1]_n$ .

$$\forall [a]_n, [b]_n, [c]_n \in \mathbb{Z}_n$$

$$([a]_n + [b]_n) \cdot [c]_n = [a+b]_n \cdot [c]_n = [(a+b) \cdot c]_n =$$

$$= [a \cdot c + b \cdot c]_n = [a \cdot c]_n + [b \cdot c]_n = [a]_n \cdot [c]_n + [b]_n \cdot [c]_n.$$

Prop. Sia  $(A, +, \cdot)$  un anello. Allora  $\forall a \in A$

$$a \cdot 0 = 0 \cdot a = 0$$

Dim.  $a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a \cdot 0 \Rightarrow a \cdot 0 = a \cdot 0 + a \cdot 0$

Per le leggi di cancellazione in  $(A, +)$  risulta  $a \cdot 0 = 0$ .

$$a \cdot 0 + \underline{0} = a \cdot 0 + \underline{a \cdot 0} \Rightarrow 0 = a \cdot 0.$$

Osserv.  $(\mathbb{Z}_2, +, \cdot)$  è un anello per cui risulta

$$[2]_8 \cdot [4]_8 = [8]_8 = [0]_8$$

Def. Sia  $(A, +, \cdot)$  un anello. Un elemento  $a \in A$  si dice divisione dello zero se

1.  $a \neq 0$

2.  $\exists b \in A, b \neq 0$  tali che  $a \cdot b = 0_A$ .

Per esempio in  $(\mathbb{Z}, +, \cdot)$  questo non si verifica mai

$\forall a, b \in \mathbb{Z}$

$$a \cdot b = 0 \Rightarrow a = 0 \vee b = 0$$

legge di annullamento del prodotto.

Quindi in  $(\mathbb{Z}, +, \cdot)$  non ci sono divisioni dello zero, per cui si dice che  $(\mathbb{Z}, +, \cdot)$  è un dominio d'integrità.

$(\mathbb{Z}_8, +, \cdot)$        $[2]_8$  è divisore dello zero  
 $[4]_8$  è divisore dello zero

$$[2]_8 \cdot [4]_8 = [0]_8$$

Prop.  $(\mathbb{Z}_n, +, \cdot)$ .     $[a]_n \in \mathbb{Z}_n$      $[a]_n$  è divisore dello zero se e solo se M.C.D.  $(a, n) \neq 1$ .

Per esempio  $[1]_8, [3]_8, [5]_8, [7]_8$  non sono divisori dello zero.

$$[2]_8, [4]_8, [6]_8 \quad [4]_8 \cdot [6]_8 = [24]_8 = [0]_8.$$

$$[3]_8 \cdot [3]_8 = [1]_8 \Rightarrow [3]_8^{-1} = [3]_8$$

$$[5]_8 \cdot [5]_8 = [1]_8 \Rightarrow [5]_8^{-1} = [5]_8$$

$$[7]_8 \cdot [7]_8 = [1]_8 \Rightarrow [7]_8^{-1} = [7]_8.$$

Def. Sia  $(A, +, \cdot)$  un anello e sia  $a \in A$ . Si dice che  $a$  è un elemento unitario di  $(A, +, \cdot)$  se è invertibile rispetto a  $\cdot$ .

Prop. Sia  $(A, +, \cdot)$  un anello. Se  $a \in A$ ,  $a$  unitario allora  $a$  non può essere un divisore dello zero  
Dim.  $0_A$  non può essere unitario perché

$$\forall a \in A \quad 0_A \cdot a = 0_A \neq 1_A \quad \text{ar} \cdot 0_A = 0_A \neq 1_A$$

$(0_A \neq 1_A \quad \text{a meno che } A = \{a\})$

Sia  $a \in A$ ,  $a$  unitario: e quindi ammette inverso  $\bar{a}^{-1} \neq 0_A$

Se  $a$  fosse divisore dello zero, esisterebbe  $b \in A \quad b \neq 0$   
tale che  $a \cdot b = 0_A$ . Moltiplichiamo per  $\bar{a}^{-1}$ :

$$\bar{a}^{-1} \cdot (a \cdot b) = \bar{a}^{-1} 0_A$$

$$(\underbrace{\bar{a}^{-1} \cdot a}_{1_A}) \cdot b = 0_A$$

$$b = 0_A \quad \text{contraddizione.}$$

Prop. Sia  $(A, +, \cdot)$  un anello. Se  $a \in A$ ,  $a$  divisore  
dello zero, allora  $a$  non può essere unitario.

Dim.  $a \neq 0$  ed  $\exists b \in A \quad b \neq 0$  tale che

$$a \cdot b = 0_A -$$

se fosse  $a$  invertibile, esisterebbe  $\bar{a}^{-1} \neq 0_A$  e quindi,  
moltiplicando per  $\bar{a}^{-1}$  avremmo:

$$\bar{a}^{-1} (a \cdot b) = \bar{a}^{-1} 0_A$$

$$(\bar{a}^t a) b = 0_A$$

$$b = 0_A \quad \text{contro addizionali}$$

In  $(\mathbb{Z}, +, \cdot)$  nessun elemento è divisore dello zero e gli unici elementi unitari sono  $1, -1$ .

Sia  $(A, +, \cdot)$  un anello finito. Se  $a \in A$ ,  $a \neq 0_A$  allora  $a$  è unitario oppure  $a$  è divisore dello zero.

In  $(\mathbb{Z}_8, +, \cdot)$  sono unitari:  $[1]_8, [3]_8, [5]_8, [7]_8$   
sono divisori dello zero:  $[2]_8, [4]_8, [6]_8$

Teorema. Sia  $[a]_n \in \mathbb{Z}_n$ . Allora  $[a]_n$  è unitario se e solo se  $\text{M.C.D.}(a, n) = 1$ .

Dim.  $[a]_n \in \mathbb{Z}_n$  è invertibile per  $\cdot$  se e solo se  $\text{M.C.D.}(a, n) = 1$  (dimostrato stamattina).

Sia  $p \in \mathbb{N}^*$ ,  $p$  primo. Tutti gli elementi non nulli di  $\mathbb{Z}_p$  sono unitari nell'anello  $(\mathbb{Z}_p, +, \cdot)$ .

$$\forall [a]_p \in \mathbb{Z}_p^* \quad \text{M.C.D.}(a, p) = 1.$$

Dif. Sia  $(A, +, \cdot)$  un anello. Si dice che  $(A, +, \cdot)$  è un corpo se ogni elemento non nullo di  $A$  è unitario; si dice che  $(A, +, \cdot)$  è un campo se  $(A, +, \cdot)$  è un corpo commutativo.

Sono campi  $(\mathbb{Q}, +, \cdot)$ ,  $(\mathbb{R}, +, \cdot)$ ,  $(\mathbb{Z}_p, +, \cdot)$  per  $p$  primo.

$\forall q \in \mathbb{Q}^*$  esiste l'inverso rispetto a  $\cdot$  che è  $\frac{1}{q} = q^{-1}$   
lo stesso per  $(\mathbb{R}, +, \cdot)$ .

Osserv.  $(\mathbb{Z}_n, +, \cdot)$  ha esattamente  $\varphi(n)$  elementi unitari  
cioè  $[a]_n$  tali che  $\text{M.C.D.}(a, n) = 1$ .

Esempio:  $(\mathbb{Z}_{15}, +, \cdot)$  determinare gli elementi unitari  
e i divisori dello zero.

$[0]_{15}$  non è unitario e nemmeno divisore dello zero

Sono unitari divisori dello zero  $[1]_{15}, [2]_{15}, [4]_{15}, [7]_{15}, [8]_{15}, [11]_{15}, [13]_{15}, [14]_{15}$   
 $[3]_{15}, [5]_{15}, [6]_{15}, [9]_{15}, [10]_{15}, [12]_{15}$

$$[1]_{15}^{-1} = [1]_{15} \quad [2]_{15}^{-1} = [8]_{15} \quad [2]_{15} \cdot [8]_{15} = [16]_{15} = [1]_{15}$$

$$[4]_{15}^{-1} = [4]_{15}$$

$$[7]_{15}^{-1} = [13]_{15} \quad \text{per chi} \quad [7]_{15} \cdot [13]_{15} = [91]_{15} = [1]_{15}$$

$$[11]_{15}^{-1} = [1]_{15} \quad \text{per chi} \quad [1]_{15} \cdot [11]_{15} = [121]_{15} = [1]_{15}$$

$$[14]_{15}^{-1} = [14]_{15}$$

---

$$[3]_{15} \cdot \underline{[5]}_{15} = [15]_{15} = [0]_{15}$$

$$[3]_{15} \cdot \underline{[10]}_{15} = [30]_{15} = [0]_{15}$$