

La coppia  $(G, \cdot)$  con  $G$  insieme e  $\cdot : G \times G \rightarrow G$   
 si dice GRUPPO.  $(a, b) \mapsto a \cdot b$

In  $(G, \cdot)$  valgono alcune proprietà:

$$1) (ab)c = a(bc) \quad \forall a, b, c \in G$$

( $\Rightarrow$  la scrittura  $abc$  non è ambigua)

$$2) (\exists! \text{ elemento neutro}):$$

$$\exists! 1 \in G \text{ t.c. } a \cdot 1 = a = 1 \cdot a \quad \forall a \in G$$

$$3) (\exists! \text{ elemento inverso}):$$

$$\forall a \in G \exists! b \in G \text{ t.c. } ab = 1 = ba$$

Dim. ( $\exists!$  dell'elemento neutro):

Sappiamo che  $\exists u \in G$  t.c.  $\forall a \in G \quad au = a = ua$

Sappiamo che  $\exists 1 \in G$  t.c.  $\forall a \in G \quad a \cdot 1 = a = 1 \cdot a$

$$\Rightarrow au = a \Rightarrow \text{scelgo } a = 1 \Rightarrow 1 \cdot u = 1$$

$$\Rightarrow \text{per } a = u \text{ si ha } u = 1u \Rightarrow u = 1$$

q.e.d.

Dim. ( $\exists!$  dell'elemento inverso):

Sappiamo  $a \cdot c = c \cdot a = 1$ . Dimostriamo  $c = b$ :

$$c = c \cdot 1 = c \cdot (a \cdot b) = (c \cdot a) \cdot b = 1 \cdot b = b$$

q.e.d.

$\Rightarrow$  dato l'elemento inverso è unico, lo si denoterà  
 come  $a^{-1}$ . Definiamo quindi, ricorsivamente:

$$a^0 = 1, \quad a^{n+1} = a^n \cdot a \quad (n > 0),$$

$$a^n = (a^{-1})^{-n} \quad (n < 0)$$

### Esercizio:

Dati  $m, n$  interi, dim. che :

$$1) \alpha^{m+n} = \alpha^m \alpha^n$$

$$2) (\alpha^n)^m = \alpha^{nm}$$

Dim.

1) Per induzione

2) Usando la 2<sup>a</sup> def. ( $n < 0$ )

### Gruppi additivi:

L'operazione si denota con  $+$ , quindi si ha:

$$1) (\alpha + b) + c = \alpha + (b + c) \quad \forall \alpha, b, c \in G$$

( $\Rightarrow$  la scrittura  $\alpha + b + c$  non è ambigua)

2) ( $\exists!$  elemento neutro):

$$\exists! 0 \in G \text{ t.c. } \alpha + 0 = \alpha = 0 + \alpha \quad \forall \alpha \in G$$

3) ( $\exists!$  elemento inverso):

$$\forall \alpha \in G \exists! b \in G \text{ t.c. } \alpha + b = 0 = b + \alpha$$

In un gruppo additivo, l'elemento inverso si dice opposto e si indica con  $-\alpha$ , mentre le potenze si definiscono come multipli:

$$0\alpha = 0, \quad (n+1)\alpha = n\alpha + \alpha \quad (n \geq 0),$$

$$n\alpha = (-n)(-\alpha) \quad (n < 0)$$

N.B.

Si tratta solo di una differenza NOTAZIONALE, tutte le proprietà continueranno a valere anche nei gruppi additivi.

Un gruppo dato da un'operazione COMMUTATIVA si dice ABELIANO ( $ab = ba \quad \forall a, b \in G$ )

esempi di gruppi:

1)  $(\mathbb{Z}, +)$ ,  $(\mathbb{Q}, +)$ ,  $(\mathbb{Q} \setminus \{0\}, \cdot)$ ,  $(\mathbb{R}^n, +)$  ecc.

2) Dati  $G_1, G_2$  gruppi si ha che  $G_1 \times G_2$  è un gruppo rispetto a  $(a, b)(c, d) = (ac, bd)$ :

$$\bullet (a, b)^{-1} = (a^{-1}, b^{-1})$$

$$\bullet (1, 1) = 1$$

3) Dato  $A$  insieme qualsiasi, definiamo  $S(A)$  insieme delle applicazioni bigettive da  $A$  in  $A$ . Si ha che  $S(A) \neq \emptyset \quad \forall A$  ( $\text{Id} \in S(A) \quad \forall A$ ). Scelgo come operazione la composizione di applicazioni  $\circ$ : allora  $(S(A), \circ)$  è un gruppo con elemento inverso  $f^{-1}$  ed elemento neutro  $\text{Id}$ .

$\Rightarrow$  Se  $|S(A)| \geq 2$ , il gruppo si dice GRUPPO SIMMETRICO su  $A$

$\Rightarrow$  Se  $A = \{1, 2, \dots, n\}$ ,  $S(A)$  si denota con  $S_n$  e si ha  $|S_n| = n!$  ed è il gruppo delle PERMUTAZIONI su  $A$ .

$\Rightarrow$  si ha che se  $|A| < +\infty$ , allora  $|S(A)| < +\infty$ , mentre se  $A$  è infinito, anche  $S(A)$  è infinito.

---

Studieremo il gruppo  $S_n$  (GRUPPI SIMMETRICI)

$\Rightarrow S_0$  e  $S_1$  sono gruppi banali (contengono solo

l'elemento neutro)

$\Rightarrow S_2$  è abeliano ( $|S_2| = 2 \Rightarrow$  1 dei 2 elementi è l'elemento neutro)

$\Rightarrow$  se  $n \geq 3$ ,  $S_n$  non è abeliano:

si ha  $\tau, \tau \in S_n$  t.c.

$$\tau(x) = \begin{cases} 2 & x=1 \\ 1 & x=2 \\ x & x \geq 3 \end{cases}, \quad \tau(x) = \begin{cases} 2 & x=1 \\ 3 & x=2 \\ 1 & x=3 \\ x & x \geq 3 \end{cases}$$

$$\Rightarrow \tau \circ \tau(1) = \tau(2) = 1 \quad \left. \begin{array}{l} \tau \circ \tau \neq \tau \circ \tau \end{array} \right\}$$

$$\Rightarrow \tau \circ \tau(1) = \tau(2) = 3 \quad \left. \begin{array}{l} \tau \circ \tau \neq \tau \circ \tau \end{array} \right\}$$

$\Rightarrow S_n$  non è abeliano per  $n \geq 3$

cerchiamo una notazione "comoda" per le permutazioni:

es.  $n=3$

$$\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \Rightarrow \begin{array}{l} \tau(1)=2 \\ \tau(2)=1 \\ \tau(3)=3 \end{array}$$

se  $n=9$  consideriamo:

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 1 & 5 & 2 & 8 & 6 & 9 & 7 \end{pmatrix}$$

$\Rightarrow$  "seguiamo" gli elementi:

$$1 \mapsto 3, \quad 3 \mapsto 1$$

$$2 \mapsto 4, \quad 4 \mapsto 5, \quad 5 \mapsto 2$$

$$6 \mapsto 8, \quad 8 \mapsto 3, \quad 3 \mapsto 7, \quad 7 \mapsto 6$$

} sono 3 "cicli"

$\Rightarrow$  denotiamo tali "cicli" come:  
 $(1\ 3), (2\ 4\ 5), (6\ 8\ 9\ 7)$

$\Rightarrow$  dunque quindi  $T = (1\ 3)(2\ 4\ 5)(6\ 8\ 9\ 7)$   
(ma importa l'ordine)

Come costruiamo questi cicli?

dato  $T \in S_n$  prendiamo  $x, T(x), T(T(x)), \dots$

$\Rightarrow$  denotiamo  $T(T(\dots(T(x))\dots))$  con  $T^p(x)$  e ottieniamo  
 $x, T(x), T^2(x), T^3(x), \dots$

$\Rightarrow$  Ad un certo punto DEVE esserci una ripetizione  
(l'insieme A è finito), dimostriamo che tale  
ripetizione è proprio il primo elemento  $x$ :

si  $K > 0$  il 1° esponente t.c.  $T^K(x) = T^\ell(x)$

con  $0 \leq \ell < K$ , mostriamo che deve essere  $\ell = 0$ .

Se  $\ell > 0$  si ha:

$$T(T^{K-1}(x)) = T^K(x) = T^\ell(x) = T(T^{\ell-1}(x))$$

$$\Rightarrow T(T^{K-1}(x)) = T(T^{\ell-1}(x))$$

$\Rightarrow T$  è biettiva per definizione

$$\Rightarrow T^{K-1}(x) = T^{\ell-1}(x) \Leftrightarrow$$

( $K$  non sarebbe il 1° esponente di una ripetizione)

$$\Rightarrow$$
 deve essere  $\ell = 0$

q.e.d.

$\Rightarrow$  Possiamo quindi dare l'algoritmo per i cicli disgiunti.

Dato  $\tau \in S_n$  si procede come segue:

- 1) Se tutti gli elementi di  $\{1, \dots, n\}$  sono stati mensionati da  $\tau$ , fine. Altrimenti (2)
- 2) Si apre una parentesi
- 3) Si scrive il numero più basso  $x$  non ancora mensionato da  $\tau$
- 4) Si pone  $y = \tau(x)$
- 5) Se  $y$  è già stato mensionato, si chiude la parentesi e (1). Altrimenti (6)
- 6) Si pone  $x = y$  e (4)

Esempio:

- $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} \Rightarrow \tau = (1 \ 4 \ 3)(2)$
- $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \Rightarrow \tau = (1 \ 3)(2 \ 4)$
- $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \Rightarrow \tau = (1 \ 2 \ 3 \ 4)$
- $\tau = \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ 2 & 3 & 4 & \dots & n & 1 \end{pmatrix} \Rightarrow \tau = (1 \ 2 \ 3 \ \dots \ n)$

Come sono fatte le permutazioni in  $S_3$ ?

$$S_3 = \{(1)(2)(3), (1 \ 2)(3), (1 \ 3)(2), (1)(2 \ 3), (1 \ 2 \ 3), (1 \ 3 \ 2)\}$$

- $\Rightarrow$  i punti dei cicli di lunghezza 1 si dicono ELEMENTI UNITI ( $\tau(x) = x$ )
- $\Rightarrow$  l'azione della funzione è il suo nome stesso!!!
- $\Rightarrow$  ogni ciclo può essere considerato una permutazione, con la condizione che gli elementi non menzionati siano uniti!!!

es. in  $S_3$   $(245) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 4 & 3 & 5 & 2 & 6 & 7 & 8 & 9 \end{pmatrix}$

- $\Rightarrow$  Allora  $(13)(245)(6837)$  è la composizione delle 3 permutazioni (ed equivale, ovviamente, con la decomposizione in cicli disgiunti vista sopra) ed è commutativa!!!
- $\Rightarrow$  Possiamo quindi calcolare le composizioni tra permutazioni con lo stesso algoritmo visto sopra!

es.:

$$(14)(235) \circ (352)(46) = (146)(235)$$

$\Rightarrow$  da dx verso sx si ha:

$$\begin{array}{l}
 1 \mapsto 1 \mapsto 1 \mapsto 1 \mapsto 4 \\
 4 \mapsto 6 \mapsto 6 \mapsto 6 \mapsto 6 \\
 6 \mapsto 4 \mapsto 4 \mapsto 4 \mapsto 1
 \end{array}
 \quad
 \left. \begin{array}{l}
 2 \mapsto 2 \mapsto 3 \mapsto 5 \mapsto 5 \\
 5 \mapsto 5 \mapsto 2 \mapsto 3 \mapsto 3 \\
 3 \mapsto 3 \mapsto 5 \mapsto 2 \mapsto 2
 \end{array} \right\} 2^{\circ} \text{ ciclo } (235)
 \quad
 \left. \begin{array}{l}
 1^{\circ} \text{ ciclo } (146)
 \end{array} \right\}$$

Come si calcola  $(1\ 2\ 3)^2$ ,  $(1\ 2\ 3\ 4)^2$ ,  $(1\ 2\ 3\ 4)^{-1}$ ?

$$(1\ 2\ 3)^2 = (1\ 2\ 3)(1\ 2\ 3) = (1\ 3\ 2)$$

$$(1\ 2\ 3\ 4)^2 = (1\ 3)(2\ 4)$$

$$(1\ 2\ 3\ 4)^{-1} = (1\ 4\ 3\ 2) = (4\ 3\ 2\ 1)$$

L'identità non ha cicli di lunghezza  $> 1$ , quindi si eleva come  $()$

$$\Rightarrow (1\ 2\ 3\ 4)^4 = () \quad !!!$$

Dato che  $\tau = \tau_1 \tau_2 \dots \tau_k$  con  $\tau_i$  cicli disgiunti di lunghezza  $l_i$ , si ha che  $\tau^l = ()$  con  $l = \text{mcm}\{l_i\}$

$$(1\ 2)(3\ 4\ 5)(6\ 7\ 8\ 9) \Rightarrow [(1\ 2)(3\ 4\ 5)(6\ 7\ 8\ 9)]^{12} = ()$$

$\Rightarrow$  Ogni permutazione  $\tau \in S_3$  soddisfa  $\tau^6 = ()$

Esercizio:

Dim. che data  $\tau \in S_n$ , si ha  $\tau^{n!} = ()$

Siano  $\tau = (1\ 2\ 4)(3\ 5)$ ,  $\tau' = \underbrace{(1\ 4)(2\ 3)}$ , chi è  $\tau \circ \tau' \circ \tau^{-1}$ ?

$$\Rightarrow \tau \circ \tau' \circ \tau^{-1} = (1\ 2)(3)(4\ 5)$$

$$= (1\ 2)(4\ 5)$$

$$= (\tau(1)\ \tau(4))(\tau(2)\ \tau(3))$$

