

$f: \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$ bijective permutazione su n oggetti.
 L'insieme delle permutazioni su n oggetti si indica con S_n .

Se $f \in S_n$

$$f = \begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix} = \begin{pmatrix} n & n-1 & \dots & 2 & 1 \\ f(n) & f(n-1) & \dots & f(2) & f(1) \end{pmatrix}$$

Def. Una permutazione di tipo

$$f = \begin{pmatrix} c_1 & c_2 & \dots & c_{h-1} & c_h & c_{h+1} & \dots & c_n \\ c_2 & c_3 & & c_h & c_1 & c_{h+1} & \dots & c_n \end{pmatrix} = (c_1 \xrightarrow{} c_2 \xrightarrow{} \dots \xrightarrow{} c_n)$$

$$= (c_2 \xrightarrow{} c_3 \xrightarrow{} \dots \xrightarrow{} c_{h-1} \xrightarrow{} c_h \xrightarrow{} c_1) = (c_3 c_4 \dots c_h c_1 c_2) = \dots$$

si dice ciclo di lunghezza h .

Esempio:

$$1. f = (1 \ 3 \ 7) \in S_8$$

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

2, 4, 5, 6, 8 fissati; 1, 3, 7 mossi.

$$2. g = (5 \xrightarrow{} 6 \xrightarrow{} 7 \xrightarrow{} 8) \in S_8$$

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 6 & 7 & 8 & 5 \end{pmatrix} = (5 \ 6 \ 7 \ 8)$$

1, 2, 3, 4 fissati;
 5, 6, 7, 8 mossi

Def. Si dice che un elemento $a \in \{1, \dots, n\}$ viene mosso dalla permutazione f se $f(a) \neq a$. Si dice che a è fissato da f se $f(a) = a$

Def. Sono $f, g \in S_n$ due permutazioni. Si dice che $f \circ g$ sono disgiunte se gli elementi mossi da f sono fissati da g (e viceversa)

Esempio: $f \circ g$ degli esempi precedenti non sono disgiunte perché 7 è mosso sia da f che da g .

Esempio

$$h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & \cancel{8} & \cancel{9} \\ 4 & 3 & 2 & 1 & 5 & 6 & 7 & \cancel{8} & \cancel{9} \end{pmatrix} = \underbrace{(14)}_{(14)} \circ \underbrace{(23)}_{(23)}$$

$$k = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & \cancel{8} & \cancel{9} \\ 1 & 2 & 3 & 4 & 5 & 7 & 9 & \cancel{8} & \cancel{6} \end{pmatrix} = (679)$$

$h \circ k$ sono disgiunte

h move 1, 2, 3, 4 che sono fissati da k
 $(k$ move 6, 7, 9 che sono fissati da h)

Prop. Se $f, g \in S_n$, $f \circ g$ disgiunte allora $g \circ f = f \circ g$.

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

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

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

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

Teorema. Una permutazione di S_n o è un ciclo o si può scrivere come prodotto di cicli disgiunti in modo unico a meno dell'ordine.

Esempio'

$$(a) f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 3 & 2 & 5 & 1 & 6 & 10 & 8 & 7 & 9 \end{pmatrix} = (1 \ 4 \ 5) \circ (2 \ 3) \circ (7 \ 10 \ 9) =$$

$$\sigma_1 = (1 \ 4 \ 5)$$

$$\sigma_2 = (2 \ 3)$$

$$\sigma_3 = (7 \ 10 \ 9)$$

$$= (2 \ 3) \circ (1 \ 4 \ 5) \circ (7 \ 10 \ 9)$$

$$(b) h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 2 & 4 & 5 & 3 & 1 \end{pmatrix} = (1\ 6) \circ (3\ 4\ 5)$$

Def. Un ciclo di lunghezza 2 si dice scambio.

Osserv. Sia $(c_1 \dots c_n)$ un ciclo di lunghezza h .

Allora

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

Esempio $(2\ 3\ 4\ 6\ 9) \in S_9$

$$(2\ 3\ 4\ 6\ 9) = (2\ 9) \circ (2\ 6) \circ (2\ 4) \circ (2\ 3)$$

$$= \cancel{(1\ 5)} \circ \cancel{(1\ 5)} \circ (2\ 9) \circ (2\ 6) \circ (2\ 4) \circ (2\ 3) \circ \cancel{(5\ 7)} \circ \cancel{(5\ 7)}$$

ciclo di lunghezza 5
che classe di
permutazione per.

$(1\ 2\ 4\ 5) \in S_5$
ciclo di lunghezza 4
classe di permutazione di posizioni

$$(1\ 2\ 4\ 5) = \cancel{(1\ 5)} \circ (1\ 4) \circ (1\ 2) = (1\ 5) \circ (1\ 4) \circ (1\ 2) \circ \cancel{(2\ 5)} \circ \cancel{(2\ 5)}$$

Infatti:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 3 & 4 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 1 & 5 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix}.$$

Un ciclo di lunghezza h può essere sempre scritto come prodotto di $h-1$ scambi non disgiunti.

Osserv. Ogni permutazione può essere scritta come prodotto di scambi (non disgiunti in generale) non in un unico modo.

Osserv. Sia $\sigma = (\alpha_1 \alpha_2)$ uno scambio, allora

$$\delta \circ \sigma = (\alpha_1 \alpha_2) \circ (\alpha_1 \alpha_2) = id_{S_n}$$

$$\begin{aligned} \text{Esempio } (14)(14) &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix} = \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = id_{S_4} \end{aligned}$$

Teorema. Se una permutazione f si scrive in due modi come prodotto di scambi, allora essi contengono entrambi un numero pari o un numero dispari di scambi.

Def. Una permutazione di S_n si dice di classe pari se una sua scomposizione in scambi contiene un numero pari di scambi, si dice di classe dispari se una sua scomposizione in scambi contiene un numero dispari di scambi.

Osserv. Un ciclo di lunghezza h si scrive come prodotto di $h-1$ scambi e quindi un ciclo di lunghezza dispari ha classe di permutazione pari, un di lunghezza pari ha classe di permutazione dispari.

Esercizio Sia $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 1 & 3 & 6 & 5 & 4 & 8 & 7 & 2 \end{pmatrix} \in S_9$

scrivere f come prodotto di cicli disgiunti e calcolare le classi di permutazione di f .

$$f = \overbrace{(1\ 9\ 2)}^{\text{pari}} \circ \overbrace{(4\ 6)}^{\text{dispari}} \circ \overbrace{(7\ 8)}^{\text{dispari}} = (1\ 2) \circ (1\ 9) \circ (4\ 6) \circ (7\ 8)$$

f ha classe di permutazione pari

NUMERI INTERI

\mathbb{Z} = insieme dei numeri interi = $\{-3, -2, -1, 0, 1, 2, 3, \dots\}$

Teorema (divisione fra numeri interi).

Siano $a, b \in \mathbb{Z}$ $b \neq 0$. Allora esistono e sono unici $q, r \in \mathbb{Z}$ tali che

$$a = b \cdot q + r \quad 0 \leq r < |b|.$$

Osserv. L'unicità è assicurata dalle condizioni $0 \leq r < |b|$.

$$a = 27 \quad b = 4 \quad |b| = 4$$

$$\boxed{27 = 4 \cdot 6 + 3} = 5 \cdot 4 - 3 = 3 \cdot 4 + 3$$

$0 \leq 3 < 4$

Def. Se $a, b \in \mathbb{Z}$ $\underbrace{b \neq 0}$ e $a = b \cdot q + r \quad 0 \leq r < |b|$

allora q si dice quoziente, r si dice resto della divisione di a per b .

Osserv. Se $a \in \mathbb{N}$ $a < b$, allora si può scrivere

$$a = b \cdot 0 + a \quad 0 \leq a < b = |b|$$

$$a = 7$$

$$b = 8$$

$$q = 8 \cdot 0 + 7$$

division de
7 par 8.

Esempio. $a = 27$

$$b = 4$$

$$\begin{array}{c} 27 = 4 \cdot 6 + 3 \\ \hline a = -27 \quad b = 4 \end{array} \quad q = 6 \quad r = 3$$

$$-27 = -(4 \cdot 6 + 3) = 4 \cdot (-6) \underline{-3} =$$

$$= 4 \cdot (-6) - 4 + \underline{4 - 3} =$$

$$= \cancel{4} \cdot (-6) + \cancel{4} \cdot (-1) + 1 =$$

$$= 4(-6-1) \cancel{+1} = \underbrace{4 \cdot (-7)}_{-28} + 1$$

$$q = -7$$

$$r = 1$$

$$a = 27$$

$$b = -4$$

$$27 = 4 \cdot 6 + 3 = (-4)(-6) + 3$$

$$0 \leq 3 < |-4| = 4$$

$$\begin{array}{l} q = -6 \\ r = 3 \end{array}$$

$$a = -27 \quad b = -4$$

$$\begin{aligned}-27 &= - (4 \cdot 6 + 3) = (-4) \cdot 6 - 3 = \\&= (-4) \cdot 6 - 4 + \underbrace{4 - 3}_{=} = \\&= \cancel{(-4)} \cdot 6 + \cancel{(-4)} \cdot 1 - 1 \\&= -4 \cdot 7 + 1\end{aligned}$$

Osserv. Siano $a, b \in \mathbb{Z}$ $b \neq 0$. Allora

$b | a \Leftrightarrow$ il resto della divisione di a per b è 0.

Def. Siano $a, b \in \mathbb{Z}$ non entrambi nulli
si dice che un numero intero $d \in \mathbb{Z}$ è un
massimo comune divisore tra a e b se

1. $d | a \wedge d | b$

2. Se $d' \in \mathbb{Z}$ tale che $d' | a \wedge d' | b$, allora $d' | d$.

Osserv. Siano $a, b \in \mathbb{Z}$, non entrambi nulli.

Se $d \in \mathbb{Z}$ è un massimo comune divisore fra a e b , allora d è anche un massimo comune divisore

tra $\frac{-a}{d} e \frac{b}{d}$, tra $a e -b$, tra $-a e b$

verifichi: d è massimo comune divisore fra $\frac{-a}{d} e \frac{b}{d}$

1. $d | a \wedge d | b \Rightarrow d | -a \wedge d | b$

2. se $d' \in \mathbb{Z}$ tale che $d' | -a \wedge d' | b$ allora

$$d' | a \wedge d' | b \text{ e quindi } d | d'.$$

Osserv. Siano $a, b \in \mathbb{Z}$, $b \neq 0$. Se $d \in \mathbb{Z}$

è un massimo comune divisore fra a e b ,

allora anche $-d$ è un massimo comune divisore
fra a e b .

Dim

1. $d | a \wedge d | b \Rightarrow -d | a \wedge -d | b$

2. $d' \in \mathbb{Z}$ tale che $d' | a \wedge d' | b$, allora

$$d' | d \text{ e quindi } d' | -d.$$

Esempio $a=6$, $b=15$

3 è un massimo comune divisore fra 6 e 15
ma anche -3 è un massimo comune divisore
fra 6 e 15.

Osserv. Se $a=0$ e $b \neq 0$, allora b è un
massimo comune divisore fra a e b .

1. $b|0 \wedge b|b$

2. Se $d' \in \mathbb{Z}$ tale che $d'|0 \wedge d'|b \Rightarrow d'|b$.

Eg. 7 è massimo comune divisore fra 0 e 7.

Teorema. Siano $a, b \in \mathbb{Z}$ non entrambi nulli.
Allora esiste un massimo comune divisore d fra
 a e b ; inoltre l'unico altro massimo comune divisore
fra a e b è $-d$. Infine esistono $x_0, y_0 \in \mathbb{Z}$
tali che

$$d = ax_0 + by_0, \quad \text{identità di Bezout.}$$

Come di dimostrazione: algoritmo delle divisioni successive.

$$b \neq 0$$

$$\underline{a} = \underline{b} q_1 + \underline{r}_1$$

$$0 \leq r_1 < |b|$$

$$\underline{b} = \underline{r}_1 q_2 + \underline{r}_2$$

$$0 \leq r_2 < r_1$$

$$r_1 = r_2 q_3 + r_3$$

$$0 \leq r_3 < r_2$$

⋮
⋮
⋮

$$r_{m-3} = r_{m-2} q_{m-1} + \underline{r_{m-1}}$$

$$0 \leq r_{m-2} < r_{m-1}$$

$$r_{m-2} = r_{m-1} \underline{q_m}$$

$$\underline{r_m = 0}$$

→ un massimo comune divisore

Osserv. Siano $a, b \in \mathbb{Z}$ non entrambi nulli. Allora se d è un massimo comune divisore fra a e b , l'unico altro massimo comune divisore fra a e b è $-d$. L'unico massimo comune divisore positivo fra a e b si indica col simbolo

$$\text{M.C.D.}(a, b).$$

$$\text{Esunpi. } a = 18 \quad b = 5$$

$$\begin{array}{l}
 18 = 5 \cdot 3 + 3 \\
 5 = 3 \cdot 1 + 2 \\
 3 = 2 \cdot 1 + 1 \\
 2 = 2 \cdot 1 + 0
 \end{array}
 \qquad
 \begin{array}{l}
 r_1 = 3 \\
 r_2 = 2 \\
 r_3 = 1 \\
 r_4 = 0
 \end{array}
 \qquad
 \begin{array}{l}
 \Rightarrow 3 = 18 + 5(-3) \\
 \Rightarrow 2 = 5 + 3(-1) \\
 \Rightarrow 1 = 3 + 2(-1)
 \end{array}$$

$$\text{M.C.D.}(18, 5) = 1.$$

Vogliamo scrivere l'identità del Bezout per $a = 18$ e $b = 5$

$$1 = a \cdot x_0 + b y_0 \quad x_0, y_0 \in \mathbb{Z} \text{ opportuni.}$$

$$\begin{aligned}
 1 &= 3 + 2(-1) = 3 + (5 + 3(-1))(-1) = 3 + 5 \cdot (-1) + 3 \cdot 1 = \\
 &= 3 \cdot \cancel{\frac{1}{2}} + 5 \cdot \cancel{\frac{1}{2}} + 3 \cdot \cancel{\frac{1}{2}} = 3 \cdot 2 + 5 \cdot (-1) = (18 + 5(-3)) \cdot 2 + 5(-1) \\
 &= 18 \cdot \underbrace{2}_{36} + 5 \cdot (-6) + 5 \cdot (-1) = 18 \cdot 2 + 5 \cdot (-7) \\
 &\qquad\qquad\qquad - 35
 \end{aligned}$$

$$\exists x_0 = 2 \quad y_0 = -7 \quad \text{tali che} \quad 1 = 18 \cdot x_0 + 5 y_0$$

$$1 = 18 \cdot 2 + 5 \cdot (-7)$$

Identità del Bezout.