$S(X) := \{ f : X \to X \mid f \text{ biiettiva} \}$.

$(S(X), \circ)$ è un gruppo

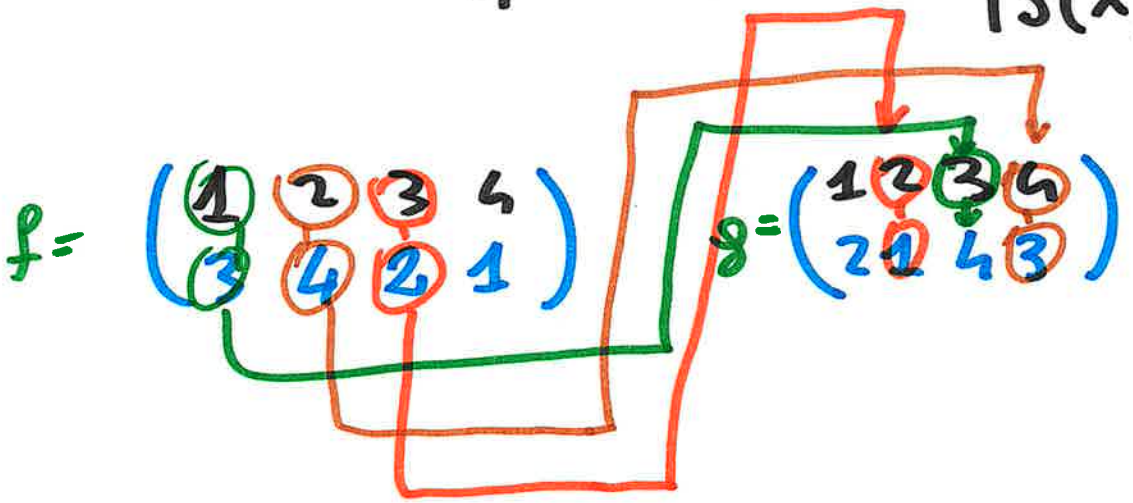
$\mathrm{id}_X : \begin{cases} X \to X \\ x \to x \end{cases}$ è l'identità

$f : X \to X$ biiettiva

$f^{-1} : X \to X$

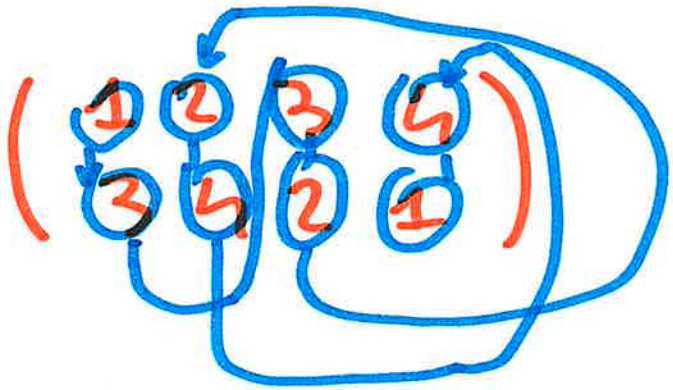
$|X| < \infty$ $\quad X = \{1, 2, 3, 4\}$ $\quad |X| = 4$

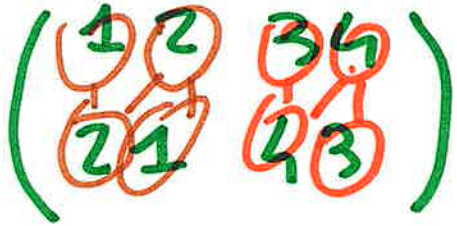
$|S(X)| = 4!$



$g \circ f$

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



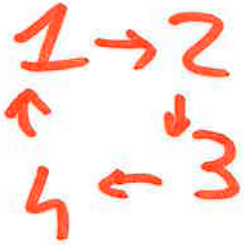


$(1\,3\,2\,4) = (3\,2\,4\,1) = (2\,4\,1\,3)$

$(12)(34)$

↑ ↑

2 scambi

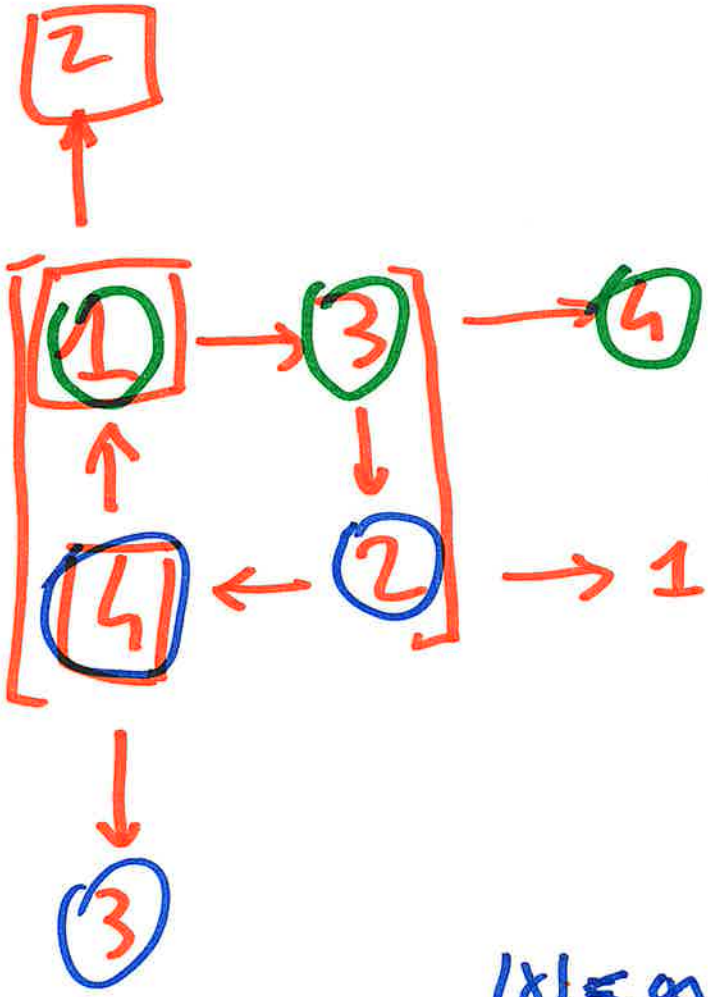


(1234)

$gof = (12)(34)(1324) =$

$= (1423)$

$(12)\cdot(12) =$



(1423)

$|X| < \infty$

OSS: 1) OGNI PERMUTAZIONE SI PUÓ SCRIVERE COME PRODOTTO DI CICLI DISGIUNTI

2) OGNI CICLO È PRODOTTO DI SCAMBI.

$f: X \mapsto X$ $\qquad |X| < \omega$

$(13)(12) = (123)$

$(a_1 a_2 \dots a_n) = (a_1 a_n)(a_1 a_{n-1}) \dots (a_1 a_2)$

$(1234) = (14)(13)(12)$

$(G, \circ)$

$f: G \to H$

$(\mathbb{Z}, +)$

$(\mathbb{Q}, +)$

$(\mathbb{R}, +)$

$(\mathbb{C}, +)$

gruppi abeliani

X

$S(X)$

$(\mathbb{Q}^* , \cdot)$

$(\mathbb{R}^* , \cdot)$

$(\mathbb{C}^* , \cdot)$

gruppi abeliani

$(\{0,1\}, \cdot)$

$(\{0,1\}, +)$

$+$	0	1
0	0	1
1	1	0

$(\mathbb{Z}, -)$ non è un gruppo

$a - b := a + (-b)$ in $(\mathbb{Z}, +)$

$(\mathbb{Z}, +, \cdot)$ → [$(\mathbb{Z}, +)$ è un gruppo commutativo

$(\mathbb{Z}, \cdot)$ soddisfa

0) $\forall a, b \in \mathbb{Z}: ab = b \cdot a$

1) $\exists\, 1 \in \mathbb{Z}: \forall a \in \mathbb{Z}\ \ 1 \cdot a = a \cdot 1 = a$

[2) $\forall a, b, c \in \mathbb{Z}: a \cdot (b \cdot c) = (a \cdot b) \cdot c$

[$\forall a, b, c \in \mathbb{Z}: \quad a \cdot (b + c) = ab + ac$

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

$(A, +, \cdot)$ è detto **ANELLO** se

1) $(A, +)$ è un gruppo abeliano
2) $(A, \cdot)$ è associativo
3) valgono le prop. distributive

$\forall a, b, c \in A$: $a(b+c) = ab + ac$
$(a+b)\cdot c = ac + bc$

è detto **commutativo** se $\forall a, b \in A: a \cdot b = b \cdot a$

con **unità** se $\exists 1 \in A: a \cdot 1 = 1 \cdot a = a \ \forall a \in A$

campo se $(A \setminus \{0\}, \cdot)$ è un gruppo abeliano

cioè A è commutativo, con unità ed $\forall a \in A \setminus \{0\}: \exists a^{-1} \in A: a^{-1} \cdot a = a \cdot a^{-1} = 1$

Campo = field.

corpo = ANELLO CON UNITÁ TALE CHE $(A\setminus\{0\}, \cdot)$ è un gruppo [non necessariamente abeliano]

↳ DIVISION RING

SKEWFIELD = corpo in cui $(A\setminus\{0\}, \cdot)$ non è abeliano.

$(A, +, \cdot)$ anello

$+$ $(A \setminus \{0\}, \cdot)$ gruppo

<u>OSS</u>: In un anello A $\forall a \in A$: $a \cdot 0 = 0 \cdot a = 0$

$A = \{0\}$ con $0 + 0 = 0$, $0 \cdot 0 = 0$ è un anello

$\mathbb{F}_1$ NON è UN CAMPO perché in UN CAMPO $A \setminus \{0\}$ deve essere un gruppo e qui $A \setminus \{0\} = \emptyset$.

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

$$0 = (-a \cdot 0) + a \cdot 0 = (-a \cdot 0) + (a \cdot 0 + a \cdot 0) =$$

$$= ((-a \cdot 0) + a \cdot 0) + a \cdot 0 =$$

$$0 + a \cdot 0 = a \cdot 0 \qquad \square$$

$(\mathbb{Z}_4, +, \cdot)$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$(a+b) \% 4$

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$(a \cdot b) \% 4$

$2 \cdot 2 = 0$

NON VALE LA LEGGE DI ANNULLAMENTO DEL PRODOTTO!

In $(\mathbb{Z}, +, \cdot)$ vale la legge di annullamento del prodotto.

$(\mathbb{Z}, +, \cdot)$ $\forall a, b \in \mathbb{Z} : a \cdot b = 0 \Rightarrow a = 0$ oppure $b = 0$

DOMINIO DI INTEGRITÀ

oss: Se $(\mathbb{K}, +, \cdot)$ campo $\Rightarrow$ $\mathbb{K}$ dominio di integrità:

Se $(\mathbb{K}, +, \cdot)$ campo $\Rightarrow$ $(\mathbb{K}^*, \cdot)$ con $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$.

gruppo $\Rightarrow$ $\forall a, b \in \mathbb{K}^* : a \cdot b \in \mathbb{K}^* \Rightarrow$

$\Rightarrow a \cdot b \neq 0$.

$\Rightarrow a \cdot b = 0 \Rightarrow a \in \mathbb{K}^* \setminus \mathbb{K}$ oppure $b \in \mathbb{K}^* \setminus \mathbb{K}$

"$\{0\}$

oss: $(\mathbb{Z}, +, \cdot)$ è un dominio euclideo

si può fare la divisione con resto.

$\forall a, b \in \mathbb{Z}$ $\exists\, q \in \mathbb{Z}$ tale che

$a = qb$

oppure $\exists\, r$ con $1 \leq r < |b|$ $\exists q$:

tale che $a = qb + r$

Esempi $(\mathbb{Z}, +, \cdot)$ anello → DOM. EUCLIDEO

$(\mathbb{Q}, +, \cdot)$

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

$(\mathbb{C}, +, \cdot)$

] campi

$(\mathbb{Z}[x], +, \cdot)$ DOMINIO DI INTEGRITÀ.

$$\mathbb{Z}[x] = \left\{ \sum_{i=0}^{n} a_i x^i \mid a_i \in \mathbb{Z},\ n \in \mathbb{N} \right\}.$$

$$f(x) = \sum f_i x^i \qquad g(x) = \sum g_i x^i$$

$$\Rightarrow \quad (f+g)(x) = \sum (f_i + g_i) x^i$$

$$(f \cdot g)(x) = f(x) \cdot g(x) = \sum_i \sum_{e+m=i} (f_e \cdot g_m) x^i =$$

$$= \sum_i f_i \sum_j g_j x^{i+j}$$

In $(\mathbb{Z}[x], +, \cdot)$ non è possibile fare "divisione con resto" di polinomi $2x+1$ e $3x$

$\deg f(x) := \max\{i : f_i \neq 0\}$

oppure -1 se $f(x) = 0$

Def $(A, +, \cdot)$ DOMINIO EUCLIDEO se $\exists\, \partial : A \setminus \{0\} \to \mathbb{N}$ tale che $\forall\, a, b \in A$ vale

$\exists\, q \in A$: $a = qb$ oppure $\exists\, q \in A, r \in A$:

$a = qb + r$ e $\partial(r) < \partial(b)$.

$(\mathbb{K}[x], +, \cdot)$ è un dominio euclideo.

con $\mathbb{K}$ campo.

$\mathbb{R}[x]$
$\mathbb{Q}[x]$
$\mathbb{C}[x]$

} polinomi in x a coeff. in $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$.

$$2x+1 \;:\; 3x \;\Rightarrow$$

$$2x+1 = \frac{2}{3}\cdot(3x) + 1$$

$$q = \frac{2}{3} \qquad r = 1 \qquad \partial(r) = 0 < \partial(3x) = 1$$

$\mathbb{K}$ campo

in $\mathbb{K}$ si può studiare l'equazione

$$\boxed{ax+b=0}$$

In $\mathbb{Z}$ $\quad ax+b=0$

$\rightarrow \quad ax=-b$

quando è risolubile?

se $a=0$ e $b=0 \Rightarrow \forall x \in \mathbb{Z}$

se $a\neq 0$ e $b=0 \Rightarrow x=0$

$a=0$ e $b\neq 0 \Rightarrow \nexists$ sol.

$a\neq 0$ $b\neq 0 \iff a|b \iff \exists q:$ $b=aq$

In $\mathbb{K}$ con $\mathbb{K}$ campo

$$ax + b = 0$$

$$ax = -b$$

$a \neq 0$ $\exists!$ sol.

$a = 0$ $\begin{cases} \forall x \in \mathbb{K} \\ \nexists x \in \mathbb{K}. \end{cases}$

- $a = 0, \ b = 0 \Rightarrow \forall x \in \mathbb{K}$
- $a \neq 0, \ b = 0 \Rightarrow \exists! x \in \mathbb{K} \quad x = 0$
- $a = 0, \ b \neq 0 \Rightarrow \nexists$ sol.
- $a \neq 0, \ b \neq 0 \Rightarrow \exists a^{-1} \in \mathbb{K} \Rightarrow$

$$(a^{-1}a)x = a^{-1}(-b)$$

$$x = a^{-1}(-b)$$

$\exists! x \in \mathbb{K}.$

In $\mathbb{Z}_4$: NON È UN DOMINIO DI INTEGRITÀ.

$2x = 0$ ha soluzioni $\{0, 2\}$.

$3x = 1$ ha sol. $x = 3$

$3x = 2$ ha sol. $x = 2$

$2x = 3$ non ha soluzioni

$0 \cdot x = 0$ ha sol. $\{0, 1, 2, 3\}$.

$\mathbb{F}_2 = \{0, 1\}$

$\| $

$\mathbb{Z}_2$

+	0	1
0	0	1
1	1	0

XOR

·	0	1
0	0	0
1	0	1

AND

$\mathbb{Z}_3 = \mathbb{F}_3$

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$\mathbb{Z}_4$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

NON È CAMPO.

$\mathbb{F}_4$

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

È UN CAMPO

Se p = primo $\Rightarrow \mathbb{Z}_p = \mathbb{F}_p$ è un campo

ALTRIMENTI $\forall$ p primo, $n \geq 1$ intero

$\exists$ un campo $\mathbb{F}_q$ di ordine $q = p^n$

NON ESISTONO CAMPI CON UN NUMERO DI ELEMENTI CHE NON È POTENZA DI PRIMO

provate a scrivere le tabelle di $\mathbb{Z}_5 = \mathbb{F}_5$ e di $\mathbb{Z}_6$