

e . e . e . e . e . e .

Definiamo delle operazioni su \mathbb{Z}_n

$$Z_n = \frac{Z}{\sqrt{n}} = \frac{Z}{\sqrt{(n)}} : \{[0], [1], \dots, [n-1]\} = \frac{Z}{\sqrt{n}}$$

$$a \sim b \iff a - b \equiv 0 \pmod{n}$$

Visione anche $\bar{a} = [a]$ per denotare la classe di a .

Definitions line

$$+: \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n$$

$$(\bar{a}, \bar{b}) \mapsto +(\bar{a}, \bar{b}) = \bar{a} + \bar{b} = \overline{a+b}$$

Siccome + è definita su un proiettante \mathbb{Z}_n , devo verificare che + non dipende dalla scelta dei rappresentanti (a, b)

$$\bar{a}, \bar{b}, \bar{c}, \bar{d} \in \mathbb{Z}_n \text{ t.c.}$$

$$(\bar{a}, \bar{b}) = (\bar{c}, \bar{d}) \quad \text{TBW: } \overline{a+b} = \overline{c+d}$$

$$\left\{ \begin{array}{l} \bar{a} = \bar{c} \\ b = d \end{array} \right. \iff \left\{ \begin{array}{l} a - c = k \cdot n \\ b - d = h \cdot n \end{array} \right. \quad k, h \in \mathbb{Z}$$

$$(a-c) + (b-d) = kn + ln = \underbrace{(k+l)n}_{\frac{1}{2}} \longrightarrow \overline{a+b} = \overline{c+d}$$

grindoli + e' una funzione BEN DEFINITA

$$\text{Ex } Z_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\} \quad \bar{1} + \bar{3} = \bar{4} \quad \begin{matrix} \curvearrowleft \\ \bar{0} \end{matrix} \quad \bar{1} + \bar{3} = \bar{5} = \bar{0} \quad , \quad \bar{3} + \bar{4} = \bar{7} = \bar{2}$$

corrisponde a:
1: prendo el. t.c. blz. per \rightarrow lec R=2
2: " " " S R=2
3: " " " S R=2
4: " " " S R=2

$+ : \mathbb{R}_n \times \mathbb{R}_n \rightarrow \mathbb{R}$ OPERAZIONE

$$+ \text{ associative: } (\bar{a} + \bar{b}) + \bar{c} = (\bar{a} + \bar{b}) + \bar{c} = \overline{(\bar{a} + \bar{b}) + \bar{c}} = \overline{\bar{a} + (\bar{b} + \bar{c})}$$

+ associative in Z

$$+ \text{ commutative: } \bar{a} + \bar{b} = \overline{a+b} = \overline{b+a} = \bar{b} + \bar{a}$$

$$\bar{0} \text{ e' l'elemento neutro} \quad \bar{0} + \bar{a} = \overline{0+a} = \bar{a} \quad \forall a \in \mathbb{Z}$$

ogni elemento di \mathbb{Z}_n è invertibile, $-\bar{q} + \bar{q} = -\bar{q+q} = \bar{0}$

$(\mathbb{Z}_n, +, \bar{0})$ groups abeliens : $-[\alpha] = [-\alpha]$ $\alpha + (-\alpha) = 0 \text{ mod } n$

DEFINICIÓN UN PRODUCTO TTO : $\mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n$

$$(\bar{a}, \bar{b}) \mapsto \bar{a} \cdot \bar{b} = \overline{a \cdot b} \Rightarrow \text{in } \mathbb{Z}$$

- x ben definito ($\&$ esercizio) (presi c, d come primi, for $\overline{a \cdot b} = \overline{c \cdot d}$ in \mathbb{Z}_n)

$$[x] - [y] = [x - y]$$

$$(a, b) \in \mathbb{Z}^2 \text{ s.t. } ([a], [b]) = ([x], [y]) \quad \text{also} \quad [x+y] = [ab]$$

$$\begin{array}{l} \uparrow \\ s = nk + x \quad n, k \in \mathbb{Z} \\ b = nk + y \end{array}$$

$$x \cdot b = \frac{u^2 u \cdot h}{0} + \frac{u \cdot h y}{0} + \frac{u \cdot h x}{0} + x y \rightarrow [x \cdot b] = [x \cdot y]$$

- * è un'operazione su \mathbb{Z}_n

- è un'operazione su \mathbb{Z}_n
- è associativa $(\bar{a} \cdot \bar{b}) \cdot \bar{c} = (\bar{a} \cdot \bar{b}) \circ \bar{c} = \bar{a} \cdot (\bar{b} \cdot \bar{c}) = \bar{a} \cdot (\bar{b} \cdot \bar{c})$
- è commutativa $\bar{a} \cdot \bar{b} = \bar{b} \cdot \bar{a} = \bar{b} \circ \bar{a} = \bar{a} \circ \bar{b}$
- ha elemento neutro $\bar{1}$ $\bar{a} \cdot \bar{1} = \bar{a} \cdot 1 = \bar{a}$
- ha sempre inverso? $(\mathbb{Z}_n, \cdot, \bar{1})$ è un monoido

$\bar{1} e \bar{-1}$ hanno sempre inverso

Esempio \mathbb{Z}_5 $\bar{2} \cdot \bar{3} = \bar{6} = \bar{1}$ $\bar{2} e \bar{3}$ sono invertibili (sono $\bar{6}$ le \bar{e}^{-1})

$$\begin{array}{lll} \mathbb{Z}_4 & \bar{2} \text{ e invertibile?} & \bar{2} \cdot \bar{5} = \bar{0} \neq \bar{1} \\ & \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\} & \bar{2} \cdot \bar{1} = \bar{2} \neq \bar{1} \quad \bar{2} \text{ non e' invertibile} \\ & & \bar{2} \cdot \bar{3} = \bar{6} \neq \bar{1} \\ & & \bar{2} \cdot \bar{2} = \bar{4} \neq \bar{1} \end{array}$$

$\bar{3}$ ha inverso in \mathbb{Z}_4 ?

$$\begin{array}{ll} \bar{3} \cdot \bar{5} = \bar{0} \neq \bar{1} & \bar{3} \text{ non e' invertibile} \\ \bar{3} \cdot \bar{1} = \bar{3} \neq \bar{1} & \\ \bar{3} \cdot \bar{2} = \bar{6} \neq \bar{1} & \\ \bar{3} \cdot \bar{3} = \bar{9} = \bar{1} \neq \bar{1} & \end{array}$$

Teorema $[x] \in \mathbb{Z}_n$. Allora $[x]$ è invertibile (rispetto al prodotto) $\iff \text{gcd}(x, n) = 1$

ovvero x è coprimo con n

infatti in \mathbb{Z}_n x non è invertibile: $\text{gcd}(x, n) = 2 \neq 1$

Oss la condizione " $\text{gcd}(x, n) = 1$ " non dipende dalla scelta del rappresentante $x \in [x]$.

$$\exists y \in [x] \text{ allora } \text{gcd}(x, n) = 1 \iff \text{gcd}(y, n) = 1 \quad \text{cioè è vero per tutti} \\ y = x + nk, \quad k \in \mathbb{Z}$$

Dimostrazione " \Rightarrow $[x]$ invertibile in $\mathbb{Z}_n \rightarrow \exists [y] \in \mathbb{Z}_n$ t.c. $[x] \cdot [y] = [1]$

$$\begin{aligned} \rightarrow x \cdot y = 1 + nk, \quad \exists k \in \mathbb{Z} \quad \rightarrow \cancel{x}y - \cancel{nk} = 1 \quad \text{eq. diagonale lineare.} \\ \rightarrow \text{gcd}(x, n) = 1 \quad \text{per avere soluzione} \\ \text{all'eq.} \end{aligned}$$

$$\begin{aligned} \leftarrow \quad \text{Supponiamo che } \text{gcd}(x, n) = 1 \stackrel{\text{def}}{\rightarrow} \exists y, k \in \mathbb{Z} \quad \text{t.c. } x \cdot y - nk = 1 \\ \rightarrow xy = 1 + nk \quad \rightarrow [x][y] = [1] \quad \text{in } \mathbb{Z}_n \quad \square \end{aligned}$$

$$M(\mathbb{Z}_n) = \{[x] \in \mathbb{Z}_n \mid \text{gcd}(x, n) = 1\} \quad \text{INVERTIBILI DI } \mathbb{Z}_n \quad \begin{array}{l} \text{(si intende per convenzione} \\ \text{rispetto a mod } n = \end{array} \quad \begin{array}{l} \text{intere coprime minori di } n \\ \text{rispetto al prodotto} \end{array}$$

Esempio Se $n = p$ primo allora $\mathbb{Z}_n < p$, $m \in \mathbb{Z}_+$ $\text{gcd}(m, p) = 1$

Quindi tutti gli $[x] \neq [0]$ sono invertibili in \mathbb{Z}_p per intere coprime minori di p

$$M(\mathbb{Z}_p) = \{[1], [2], [3], \dots, [p]\} \quad M(\mathbb{Z}_4) = \{[1], [3]\} \quad \begin{array}{l} \text{(eventualmente)} \\ \text{per i primi scelti.} \\ \text{se } \text{gcd}(n, p) \neq 1 \end{array}$$

Def (funzione di Eulero) $n \in \mathbb{Z}_+, n \geq 2$ $\varphi(n) := \#\{x \in \mathbb{Z} \mid 1 \leq x \leq n \text{ e } \text{gcd}(x, n) = 1\}$ o numeri minori di n coprimi con n

$$\varphi(2) = 1 \quad \varphi(3) = 2 \quad \varphi(4) = 2 \quad \varphi(5) = 4 \quad \varphi(6) = 2$$

$\text{MCD}(x, n) = 1$

overo i numeri minori di n coprimenti di n

$$\varphi(2) = 1 \quad \varphi(3) = 2 \quad \varphi(4) = 2 \quad \varphi(5) = 4 \quad \varphi(6) = 2 \dots$$

↳ vediamo x divisori di $M(\mathbb{Z}_n)$

- se p primo $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$, se $\alpha = 1 \rightarrow \varphi(p) = p - 1$
- $a, b \in \mathbb{Z}_+$, $\text{MCD}(a, b) = 1$ allora $\varphi(ab) = \varphi(a)\varphi(b)$ si dice φ moltiplicativa
 - $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ p_i primi, $\alpha_i \in \mathbb{Z}_+$
- $$\rightarrow \varphi(n) = n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_s}\right)$$
- Es. $\varphi: \mathbb{N} \rightarrow \mathbb{N}$
se x è un numero naturale
 si vole tale proprietà

TEOREMA DI FERMAT

num coprimenti
 $n > 1, n \in \mathbb{N}, x \in \mathbb{Z}, \text{MCD}(x, n) = 1$. Allora $x^{\varphi(n)} \equiv 1 \pmod{n}$

(overo $[x]^{\varphi(n)} = [1]$ in \mathbb{Z}_n)

D El teorema dice come trovare l'inverso di $[x]$ in \mathbb{Z}_n :

$$[x] \cdot [x]^{\varphi(n)-1} = [x]^{\varphi(n)} = [1]$$

$\underbrace{_{\substack{[x]^{-1}}}}$

COROLARIO (Piccolo teorema di Fermat)

p primo, $x \in \mathbb{Z}, \text{MCD}(x, p) = 1 \rightarrow x^{p-1} \equiv 1 \pmod{p}$

Dim (cor) $n = p$ nel teorema, $\varphi(p) = p - 1$ \square

Es \mathbb{Z}_5 $[2]^{p-1} = [2]^4 = [16] = \overbrace{[1]}^{\substack{\text{perché siamo in } \mathbb{Z}_5 \text{ (}16/5 = \text{resto } 1\text{)}}}$
 $[2]^{p-2} = [2]^3 = 8 = [3] \text{ e l'inverso di } [2] \text{ in } \mathbb{Z}_5$

Es \mathbb{Z}_6 l'inverso di $[5]$? $[5]^{\varphi(6)-1} = [5]^{2-1} = [5]$
 $\varphi(6) = 2$
n coprimi con 6 interi < 6

infatti $[5] \cdot [5] = [-1] \cdot [-1] = [1]$

Es Qual è l'inverso di $[3]$ in \mathbb{Z}_7 ?

$\text{MCD}(3, 7) = 1 \rightarrow [3]$ è invertibile

$$[3]^{p-1} = [1] \text{ quindi } [3]^{p-2} = [3]^{6-2} = [3]^5$$

$$[3]^5 = [3]^2 \cdot [3]^2 \cdot [3] = [2] \cdot [2] \cdot [3] = [4] \cdot [3] = [12] = [5]$$

$$[3]^2 = [5] = [2] \quad \text{Quindi } [3]^{-1} = [5]$$

Es Qual è l'inverso di $[2]$ in \mathbb{Z}_9 ?

$$\varphi(3) = 3^2 - 3 = 6$$

$\text{MCD}(2, 3) = 1 \rightarrow [2]$ è invertibile in \mathbb{Z}_9

$$[2]^{p-1} = [2]^{\varphi(9)-1} = [2]^5 = [32] = [5]$$

$$32 = 3 \cdot 3 + 5$$

$$\text{e dunque } [2] \cdot [5] = [10] = [1]$$

Dim (teorema di Euler)

$$M(\mathbb{Z}_n) = \{[x] \mid 1 \leq x < n, \text{MCD}(x, n) = 1\} = \{[x_1], [x_2], \dots, [x_{\varphi(n)}]\}$$

Dimo (teorema di Euler)

$$M(\mathbb{Z}_n) = \{[a] \mid 1 \leq a < n, \text{mcd}(a, n) = 1\} = \{[a_1], [a_2], \dots, [a_{\varphi(n)}]\}$$

$$\varphi(n) = \#\ M(\mathbb{Z}_n) \quad [a_i] \neq [a_j] \quad \text{se } i \neq j$$

$$\text{Se } x \in \mathbb{Z}, \text{mcd}(x, n) = 1$$

$$\text{tao } [x]^{e(n)} = [1]$$

$$\text{mcd}(x, n) = 1$$

$$\text{mcd}(a_i, n) = 1 \quad \forall i = 1, \dots, \varphi(n) \quad \parallel \rightarrow \text{mcd}(a_i \cdot x, n) = 1$$

$$\rightarrow [a_i \cdot x] \in M(\mathbb{Z}_n) \rightarrow [a_i \cdot x] = [a_j] \quad \text{per un qualche } j \in \{1, \dots, \varphi(n)\}$$

$$\text{Se } [a_k] \neq [a_i] \quad \text{allora} \quad [a_k \cdot x] \neq [a_i \cdot x] \quad (\text{se fosse } [a_k \cdot x] = [a_i \cdot x])$$

$$\text{allora moltiplicando per } [x]^{-1} \text{ ottengo } [a_k \cdot x][x]^{-1} = [a_i \cdot x][x]^{-1} \rightarrow [a_k] = [a_i] \text{ falso}$$

perciò invertibili

moltiplico entrambi i membri per $[a_1]^{-1} \dots [a_{\varphi(n)}]^{-1}$, ottengo:

$$[1] = [1] \cdot [x]^{\varphi(n)} \rightarrow [1] = [x]^{\varphi(n)} \quad \square$$

$$\text{Ese } \mathbb{Z}_8 \quad \varphi(8) = \frac{8^2 - 8^1}{2} = 8 - 4 = 4$$

$$8 = 2^3$$

$$M(\mathbb{Z}_8) = \{[1], [3], [5], [7]\}$$

$$[1]^4 = [1], \quad [3]^4 = [81] = [1], \quad [5]^4 = [25] = [-1], \quad [7]^4 = [-1] = [1]$$

$$\varphi_8 = 1$$

Definizioni ulteriori sui monoidi

lunedì 30 novembre 2020 14:55

e . e . e . e - e

Def (prodotto di monoidi / gruppi) $(M, \star, \lambda), (L, \circ, \eta)$

$$(\star \times \circ): (M \times L) \times (M \times L) \rightarrow (M \times L)$$

$$((x, y), (z, t)) \rightarrow (x \star z, y \circ t)$$

OPERAZIONE BINARIA
su $M \times L$

Queste operazioni rendono $M \times L$ un monoido: $(M \times L, \star \times \circ, (\lambda, \eta))$ elemento neutro

il nuovo monoido è detto **prodotto diretto** di M e L (dei monoidi)

$$\text{E' vero che } M(M \times L) = M(M) \times M(L)$$

Quindi se M e L sono gruppi, anche $M \times L$ è un gruppo.

Ese $(\mathbb{Z}_7, \cdot, 1) \times (\mathbb{Z}_3, \cdot, 1)$ monoidi prodotto

$$(\bar{2}, \bar{5}) \in \mathbb{Z}_7 \times \mathbb{Z}_3$$

$$(\bar{3}, \bar{6}) \in \mathbb{Z}_7 \times \mathbb{Z}_3$$

monoidi prodotto

$$\begin{matrix} \bar{2} & \bar{5} \\ \bar{3} & \bar{6} \end{matrix}$$

$$(\bar{2}, \bar{5}) \cdot (\bar{3}, \bar{6}) = (\bar{2} \cdot \bar{3}, \bar{5} \cdot \bar{6}) = (\bar{6}, \bar{3}) = (\bar{6}, \bar{3}) = (-\bar{1}, \bar{3})$$

$$(\bar{3}, \bar{6}) \text{ e invertibile in } \mathbb{Z}_7 \times \mathbb{Z}_3? \iff (\bar{3} \text{ e invertibile in } \mathbb{Z}_7) \wedge (\bar{6} \text{ e invertibile in } \mathbb{Z}_3)$$

✗

$$(3, 2) \text{ e invertibile in } \mathbb{Z}_7 \times \mathbb{Z}_3 \text{ e l'inverso e' } (\bar{5}, \bar{5})$$

Sottomonoidi e sottogruppi

Def (M, \star, λ) monoido, $L \subseteq M$ è detto **sottomonodo** (di M) se:

$$1) \lambda \in L$$

$$2) \forall a, b \in L \rightarrow a \star b \in L \quad (L \text{ e chiuso } \xrightarrow{\text{se (multiplicativamente) due el. e L rimangono in L}} \text{rispetto a } \star)$$

L'operazione $\star: M \times M \rightarrow M$ si restringe a $\star: L \times L \rightarrow L$, quindi (L, \star, λ) è un monoido.

Ese $(\mathbb{Z}, +, 0) \supseteq (\mathbb{N}, +, 0)$ sottomonodo

$$\{ \text{numeri pari} \} \subseteq (\mathbb{Z}, +, 0)$$

\nwarrow \nearrow

\mathbb{Z}

$$\{ \text{numeri dispari} \} \subseteq (\mathbb{Z}, +, 0) \text{ non e' un sottomonodo} \quad 0 \notin \{ \text{dispari} \}$$

Ese $(M, \star, \lambda) \supseteq \{ \lambda \}$ sottomonodo $\lambda \star \lambda = \lambda$ (el. neutro)

Ese $(R, \circ, 1) \supseteq \{ R, \circ, 1 \}$ sottomonodo

Ese $(\mathbb{C}, \cdot, 1)$ catena di sottomonodi $\xrightarrow{\text{f. bijective (invertibili)}}$

$$\mathbb{C} \supseteq \mathbb{R} \supseteq \mathbb{C}^* \supseteq \mathbb{R}^* \supseteq \mathbb{C}^{**} \supseteq \mathbb{R}^{**} \supseteq \dots$$

$(\mathbb{C}, \cdot, 1)$ catena di sottomonoidi \rightarrow gruppi (invertibili)

Ese X insieme, $(X^*, \circ, \text{Id}_x) \supseteq (\text{Big}(x), \circ, \text{Id}_x)$ sottomonodo

Ese $(\mathbb{N}, *, \lambda) \supseteq (\mathbb{M}(\mathbb{N}), *, \lambda)$ sottomonodo che è anche un gruppo (^{tutti gli elementi hanno un inverso})

Ese $(\mathbb{Z}_8, \cdot, \bar{1}) \quad \mathbb{M}(\mathbb{Z}_8) = \{[1], [3], [5], [7]\}$

$(\mathbb{M}(\mathbb{Z}_8), \cdot, \bar{1})$ è un gruppo (gruppo relativistico mod 8)

Def $(G, *, \lambda)$ monodo, $H \subseteq G$ è detto **sottogruppo** (di G) se:

1) $\lambda \in H$

2) $\forall a, b \in H \rightarrow a * b \in H \quad (H \text{ è chiuso rispetto a } *)$

3) $\forall a \in H \rightarrow a^{-1} \in H$

Ese $(\mathbb{Z}, +, 0) \supseteq n\mathbb{Z}$ sottogruppo (anche i loro opposti sono pari)

" $\supseteq \mathbb{N}$ non è un sottogruppo (ok 1+2 ma no 3))

l'inverso di 2 ($\text{cioè } -2$) non sta in \mathbb{N})

Ese $(\mathbb{R}^*, \cdot, 1) \supseteq (\mathbb{R}^*, \cdot, 1)$ sottogruppo

AI

$(\mathbb{C}^*, \cdot, 1)$

Ese $(\mathbb{Z}, -, 0)$ in \mathbb{Z} , dato $n \in \mathbb{Z}$, c'è un sottogruppo $n\mathbb{Z} = \{kn \mid k \in \mathbb{Z}\}$

1) $0 \in n\mathbb{Z}$

2) $a, b \in n\mathbb{Z} \rightarrow a = kn \rightarrow a + b = (k+n)n \in n\mathbb{Z}$
 $b = hn$

3) $a \in n\mathbb{Z} \rightarrow a = kn \rightarrow -a = (-k) \cdot n \in n\mathbb{Z}$
l'inverso è rispetto alla somma

Non ce ne sono altri!

Prop Se H è un sottogruppo di $(\mathbb{Z}, +, 0)$ allora $\exists n \in \mathbb{Z}$ t.c. $H = n\mathbb{Z}$

Dmo Non è banale $H = \{14a + 21b \mid a, b \in \mathbb{Z}\}$ è un sottogruppo

$$\begin{array}{c} 14a + 21b \\ 14c + 21d \\ \hline 14(a+c) + 21(b+d) \end{array} \rightarrow (14a + 21b) + (14c + 21d) = 14(a+c) + 21(b+d)$$

Dmo H sottogruppo di $(\mathbb{Z}, +, 0)$.

• se $H = \{0\}$ allora scalo $n=0$, $0 \cdot \mathbb{Z} = \{0 \cdot k \mid k \in \mathbb{Z}\} = \{0\} = H$

- se $H \neq \{0\}$ sia $n > 0$ il minimo intero positivo che appartiene ad H

(\exists minimo perché N è bene ordinato) Tesi: $H = n\mathbb{Z}$

$$\text{"2" } n \in H \xrightarrow{H \text{ sottogruppo}} n+n \in H \quad \begin{matrix} \text{anche } n+n \text{ (diviso rispetto alle somme)} : \\ \text{con } n+\dots+n \in H \end{matrix} \quad \rightarrow kn \in H \text{ con } k \in \mathbb{Z} \quad \text{quindi } n\mathbb{Z} \subseteq H$$

$$-n \in H$$

E' Sia $t \in H$ $\frac{t}{n} = q_n + r$ $r, q \in \mathbb{Z}$, $0 \leq r < n$ divisione euclidea
 H per tp

$\rightarrow r = t - q_n n \in H$ perché H è un sottogruppo
 siamo in un sottogruppo, quindi le differenze rimangono in esso.

$n > 0$ è il più piccolo intero > 0 in H $\rightarrow r = 0$

allora $t = q_n n \rightarrow t \in n\mathbb{Z} \quad \square$

Esempio $H = \{14a + 21b \mid a, b \in \mathbb{Z}\}$ sottogruppo di $(\mathbb{Z}, +, 0)$

cerchiamo il più piccolo intero $n > 0$ in H , questo è $\gamma = \text{MCD}(14, 21)$

Quindi $H = \gamma\mathbb{Z}$ (multipli di γ)

\uparrow
 (è sempre il MCD per i numeri
 scritti in questa forma
 (e.g. olio d'oliva), gli u.c.m.d.
 sono tali che u.c.m.d. $\leq n$)

\downarrow
 D'ep. non ha
 soluzione (no int.)
 è sottogruppo di $(\mathbb{Z}, +, 0)$

$\text{e} \cdot \text{e} = \text{e} = \text{e} \cdot \text{e}$

$$\text{Ese} \quad X = \{x_1, x_2, x_3\} \quad G = \{f: X \rightarrow X \text{ bijective}\} \subseteq X^X$$

G è l'insieme delle permutazioni di un insieme con 3 elementi, si denota con $S_3 = G$

$$|G| = 3! = 3 \cdot 2 \cdot 1 = 6 \text{ elementi}$$

(G, \circ, Id_X) è un gruppo (sottogruppo del monoido (X^X, \circ, Id))

elementi invertibili

Determiniamo i suoi elementi:

$$\bullet \text{ Id}_X \quad \text{Id}: X \rightarrow X \\ x_i \mapsto x_i$$

$$\bullet \varphi: \begin{array}{l} x_1 \mapsto x_2 \\ x_2 \mapsto x_1 \\ x_3 \mapsto x_3 \end{array}$$

$$\bullet \psi: \begin{array}{l} x_1 \mapsto x_2 \\ x_2 \mapsto x_3 \\ x_3 \mapsto x_1 \end{array}$$

φ è detta trasposizione
($1 \leftrightarrow 2$, scambia)

ψ 3-ciclo $\underbrace{1-2-3}$

$$\varphi, \psi: X \rightarrow X \text{ bijective} \quad \varphi, \psi \in G$$

$$\varphi^2 = \varphi \circ \varphi = \text{Id}_{(2-\text{ciclo})}, \quad \psi^3 = \psi \circ \psi \circ \psi = \text{Id}_{(3-\text{ciclo})} \rightarrow \psi^2 \circ \psi = \text{Id} \rightarrow \psi^{-1} = \psi^2$$

$$\hookrightarrow \varphi^{-1} = \varphi \quad \text{per la definizione di inverso} \quad (\text{ottenuto Id dall'operazione } \varphi)$$

$$\psi^2: \begin{array}{l} x_1 \mapsto x_3 \\ x_2 \mapsto x_1 \\ x_3 \mapsto x_2 \end{array}$$

applico prima φ poi ψ ($x_1 \xrightarrow{\varphi} x_2 \xrightarrow{\psi} x_3$)

$$\bullet \psi \circ \varphi: \begin{array}{l} x_1 \mapsto x_3 \\ x_2 \mapsto x_2 \\ x_3 \mapsto x_1 \end{array}$$

$$\bullet \varphi \circ \psi: \begin{array}{l} x_1 \mapsto x_1 \\ x_2 \mapsto x_3 \\ x_3 \mapsto x_2 \end{array}$$

$$\psi \circ \varphi, \varphi \circ \psi \in G$$

$\psi \circ \varphi \neq \varphi \circ \psi \rightarrow G$ non è abeliano (operazione non elettrone)

$$\text{Id}_X, \varphi, \psi, \varphi \circ \psi, \psi \circ \varphi, \psi^2 \in G \quad \text{e sono 2 a 2 distinti}$$

$$|G| = 6 \rightarrow G = \{\text{Id}_X, \varphi, \psi, \varphi \circ \psi, \psi \circ \varphi, \psi^2\}$$

! Tutte le altre possibili composizioni ricadono necessariamente in questi elementi

$$\text{Ad esempio: } (\varphi \circ \psi) \circ (\psi \circ \varphi) = \varphi \circ \psi^2 \circ \varphi: \begin{array}{l} x_1 \xrightarrow{\varphi} x_2 \xrightarrow{\psi^2} x_1 \xrightarrow{\varphi} x_2 \\ \xrightarrow{\psi} x_2 \xrightarrow{\varphi} x_1 \xrightarrow{\psi} x_3 \xrightarrow{\varphi} x_3 \\ \xrightarrow{\psi} x_3 \xrightarrow{\varphi} x_1 \end{array}$$

ψ

Sottogruppi di G

$$H = \{\text{Id}, \psi\} \quad \text{sottogruppo}$$

o.c. neutro (non ha cambiato valore)

$$1) \text{Id} \in H \quad \checkmark$$

$$2) \forall a, b \in H \rightarrow a \circ b \in H \quad \checkmark \quad a \circ b = \text{Id} \in H$$

$$3) \forall a \in H \rightarrow a^{-1} \in H \quad \checkmark \quad a^{-1} = a \in H$$

↪ inverso di $\text{Id} \in H$

$$T = \{\text{Id}, \varphi, \psi, \varphi \circ \psi\} \quad \text{non è un sottogruppo} \quad \psi^{-1} = \psi^2 \notin T$$

$$N = \{\text{Id}, \psi, \psi^2\} \quad \text{sottogruppo}$$

Monoidi e gruppo sottostante

Def (M, \star, λ) monoidi (rispettivamente gruppo), \sim una relazione di equivalenza su M .

Diciamo che \sim è compatibile rispetto a \star se:

$$\forall a, b, c, d \in M \quad (a \sim b) \wedge (c \sim d) \rightarrow (a \star c) \sim (b \star d)$$

In questo caso possiamo definire un'operazione sul quoziente M/n

$$[x] \star [y] := [x+y] \quad \forall x, y \in M \quad \text{non dipende dalla scelta di rappresentanti}$$

$(M/n, [\star], [\lambda])$ è un monoido (con gruppo)
↳ l'inverso della classe è uguale alla classe dell'inverso

Esempio $(\mathbb{Z}, +, \sim)$ gruppo $x \sim y \iff x-y \equiv 0 \pmod{n}$ (aritmetica modulare)

$$\begin{array}{l} a \equiv b \pmod{n} \\ c \equiv d \pmod{n} \end{array} \quad \begin{array}{l} \mapsto a+c \equiv b+d \pmod{n} \\ \text{operazione} \end{array}$$

\sim è compatibile con $+$, il quoziente \mathbb{Z}/\sim eredita la struttura di gruppo
" \mathbb{Z}_n

$(\mathbb{Z}_n, +, \bar{0})$ gruppo

Esempio $(\mathbb{Z}, \circ, 1)$ monoido (solo 1 è invertibile) $x \sim y \iff x-y \equiv 0 \pmod{n}$

\sim è compatibile con $\circ \rightarrow (\mathbb{Z}_n, \circ, \bar{1})$

$$\begin{array}{l} a \equiv b \pmod{n} \\ c \equiv d \pmod{n} \end{array} \quad \begin{array}{l} \mapsto a \cdot c \equiv b \cdot d \pmod{n} \\ \text{operazione} \end{array}$$

Esempio $(\mathbb{Z}, \circ, 1)$ monoido $a \sim b \iff \exists n, m \in \mathbb{N} \text{ s.t. } z^n a = z^m b$

Provare che \sim è compatibile con \circ

$$a \sim b \quad z^n a = z^m b \quad \exists n, m \in \mathbb{N}$$

$$c \sim d \quad z^n c = z^m d \quad \exists n, m \in \mathbb{N}$$

$$\exists k, j \in \mathbb{N} \quad k=z^n \text{ e } j=z^m$$

$$z^n a \cdot z^m c = z^m b \cdot z^n d$$

$$z^{n+m} a c = z^{m+n} b d \rightarrow z^{n+m} a c = z^{n+m} b d$$

$$\text{pensi } z, t \in \mathbb{Z} \text{ s.t. } z = a c \text{ e } t = b d$$

RELAZIONE DI EQUIVALENZA INDOTTA DA UN SOTTOGRUPPO

(G, \star, λ) gruppo, $H \subseteq G$ sottogruppo, H induce la relazione:

$$g, g' \in G \quad g \sim g' \iff g^{-1} \circ g' \in H \quad \text{simmetria}$$

\sim è relazione di equivalenza.

1) riflessiva: $\forall g \in G \quad g \sim g \iff \underbrace{g^{-1} \circ g}_{(g^{-1} \star g) = \lambda} \in H \quad \text{vero, } \lambda \in H \text{ perché } H \text{ è sottogruppo}$

2) simmetrica: $g, g' \in G \quad g \sim g' \rightarrow g' \sim g$

$$\begin{array}{l} g \sim g' \rightarrow g^{-1} \star g' \in H \xrightarrow{\text{sottogruppo}} (g^{-1} \star g')^{-1} \in H \xrightarrow{\text{composto}} (g^{-1} \star g') \star (g')^{-1} \star g \\ g' \sim g \iff (g')^{-1} \star g \in H \quad (g')^{-1} \star g \xrightarrow{\text{composto}} = g^{-1} \star g \star (g')^{-1} \star g \\ = g^{-1} \star g = \lambda \end{array}$$

3) transitiva: $g \sim g', g' \sim g'' \quad \text{resta } g \sim g''$

$$\text{allora } g^{-1} \star g' \in H, (g')^{-1} \star g'' \in H \quad \rightarrow g^{-1} \star g'' \in H$$

$$\begin{array}{l} g^{-1} \star g'' = (g^{-1} \star g') \star (g')^{-1} \star g'' \in H \rightarrow g \sim g'' \\ \text{per } \star \text{ si intende} \quad \text{inserendo le parentesi} \\ \text{per l'associatività di } \star \end{array}$$

(G, \star, λ) , $H \subseteq G$ sottogruppo

$$g \sim g' \iff g^{-1} \star g' \in H$$

$g \in G$, la classe di equivalenza di g

$$[g] = \{x \in G \mid x \sim g\}$$

$$x \sim g \iff x^{-1} \star g \in H \iff \exists h \in H \text{ t.c. } x^{-1} \star g = h$$

$$\iff \exists h \in H \text{ t.c. } \underbrace{x + x^{-1} \star g}_{\lambda} = x \star h \iff \exists h \in H \text{ t.c. } g = x \star h$$

$$\text{Se } h = x^{-1} \iff \exists h \in H \quad g \star h = x \star x^{-1} \star h = x$$

cioè perdo nei gruppi esistono gli inversi

$$[g] = \{x \in G \mid \exists h \in H \quad x = g \star h\} = g \star H$$

classe laterale di G modulo H

moltiplicando $g = x \star h \in H$ ottengo ulteriori elementi (esso perde \sim_S)

(se \star non commutativa, $\sim_S \neq \sim_D$)

$$G_{\sim_S} = \{g \star H \mid g \in G\} =: G/H$$

$$[G : H] := \#(G/H) \text{ INDICE DI } H \text{ in } G \text{ (cardinalità del quoziente)}$$

Analogamente $g \sim_D g' \iff g + (g')^{-1} \in H$

\sim_D è relazione di equivalenza

$$g \in G, \text{ la classe } [g] = \{x \in G \mid x \sim_D g\} = \{x = h + g \mid h \in H\} = H + g$$

classe laterale destra di G modulo H

$$G_{\sim_D} = \{H + g \mid g \in G\} =: H \backslash G \quad (\text{uguale a } G/H)$$

I due insiemi G_{\sim_S} e G_{\sim_D} sono equipotenti, ma in generale sono diversi

Esempio $G = S_3 = \{\bar{e}_d, \varphi, \psi, \varphi \circ \psi, \psi \circ \varphi, \psi^2\}$

$$H = \{\bar{e}_d, \varphi\} \text{ sottogruppo} \quad \varphi^2 = \bar{e}_d$$

classi laterali sinistre $g \star H$ al variare di $g \in G$

$$g = \bar{e}_d \quad \{ \bar{e}_d, \varphi \}$$

$\bar{e}_d \circ \bar{e}_d = \bar{e}_d \circ \varphi \rightarrow$ compare a dx con gli el. di H

in effetti sono

$$g = \varphi \quad \{ \varphi, \bar{e}_d \}$$

anche classi di equivalenza
(hanno stessi elementi)

$$g = \psi \quad \{ \psi, \varphi \circ \psi \}$$

$$g = \psi \circ \varphi \quad \overrightarrow{\psi \circ \varphi}$$

ho 3 classi laterali sinistre

$$g = \varphi \circ \psi \quad \{ \varphi \circ \psi, \varphi \circ \psi \circ \varphi \}$$

$$H = \{\bar{e}_d, \varphi\}$$

$$\psi \circ H = \{ \psi, \psi \circ \varphi \}$$

$$g = \varphi \circ \psi \quad \{ \varphi \circ \psi, \varphi \circ \psi^2 \}$$

$$g = \psi^2 \quad \rightarrow$$

$$H = \{ \text{Id}, \psi \}$$

$$\psi \circ H = \{ \psi, \psi \circ \psi \}$$

$$\psi^2 \circ H = \{ \psi, \psi \circ \psi \}$$

CLASSI LATENTI DESTRE $H \circ g$ al variare di $g \in G$

$$g = \text{Id} \quad \{ \text{Id}, \psi \} = H$$

$$g = \varphi \quad \rightarrow$$

$$g = \psi \quad \{ \psi, \psi \circ \psi \} = H \circ \psi$$

$$g = \psi^2 \quad \rightarrow$$

$$g = \psi^2 \quad \{ \psi^2, \psi \circ \psi^2 = \psi \circ \psi \} = H \circ \psi^2 \quad (\text{poss. scegliere anche } H \circ (\psi \circ \psi) \text{ come rappresentante})$$

$$g = \psi \circ \varphi \quad \rightarrow$$

$H \circ g$ classi latenti destre

Sono diverse dalle precedenti;

in particolare $\psi \circ H \neq H \circ \psi$

(osserva gli elementi)

Ese Classi latenti \Rightarrow classi di G modulo $N = \{ \text{Id}, \psi, \psi^2 \}$ (so non s'intesa, per funzioni è 0 (composizioni))

$$G = S_3 = \{ \text{Id}, \varphi, \psi, \varphi \circ \psi, \psi \circ \varphi, \psi^2 \}$$

$N = \{ \text{Id}, \psi, \psi^2 \}$ sottogruppo

• CLASSI LAT:

$$g = \text{Id} \quad \{ \text{Id}, \psi, \psi^2 \} = N \quad \text{ho 2 classi lat. sx}$$

$$g = \psi \quad \{ \psi, \psi^2, \text{Id} \} =$$

$$g = \varphi \quad \{ \varphi, \varphi \circ \psi, \varphi \circ \psi^2 \} = \varphi \circ N$$

$$g = \psi \circ \varphi \quad \{ \psi \circ \varphi, \psi \circ \varphi \circ \psi, \psi \circ \varphi \circ \psi^2 \} =$$

ho 2 classi lat. sx

verso alle precedenti,

(in particolare $N = N$ e $\varphi \circ N = N \circ \varphi$ quando i due elementi)

• CLASS. LAT. DEX:

$$g = \text{Id} \quad \{ \text{Id}, \psi, \psi^2 \} = N$$

$$g = \psi^2 \quad \{ \psi^2, \psi \} = N$$

$$g = \psi \quad \{ \psi, \psi \circ \varphi, \psi^2 \circ \varphi \} = \psi \circ N = N \circ \varphi$$

$$g = \psi \circ \varphi \quad \{ \psi \circ \varphi, \psi \circ \varphi \circ \psi, \psi \circ \varphi \circ \psi^2 \} =$$

verso alle precedenti,

(in particolare $N = N$ e $\varphi \circ N = N \circ \varphi$ quando i due elementi)

Oss G commutativo allora $g \sim g' \iff g \sim g'$ le due relazioni coincidono

$$e \quad g + H = H + g$$

Altamente in generale $g + H \neq H + g$

Def G gruppo, $H \subseteq G$ sottogruppo, H si dice **normale** se $\forall g \in G \quad g + H = H + g$ (classi lat. = classi lat.)
(se G commutativo, allora tutti i sottogruppi sono normali)

$$\stackrel{?}{\circ} g + H = H + g \iff \exists h \in H \quad \exists h' \in H \text{ d.c.} \quad \begin{matrix} g + h = h' + g \\ g + h = h + g \end{matrix}$$

Se H è un sottogruppo normale di G , allora la relazione \sim_H (che è uguale a \sim_D) è compatibile con $*$, quindi possiamo definire un'operazione su G/H ($= H \setminus G$)

$$[g] *_{\sim_H} [g'] = [g * g'] \quad \forall g, g' \in G$$

Vediamo che $*_{\sim_H}$ è ben definita:

$$\begin{array}{lll} g \sim g' & g \sim g' \rightarrow g' = g * u \quad u \in H \\ K \sim K' & K \sim K' \rightarrow K' = K * v \quad v \in H \end{array}$$

TB: $g * u \sim g' * u'$
(non dipende dalla scelta
di rappres. di \sim)

$$H \text{ sottogruppo normale} \rightarrow \exists u' \in H \text{ s.t. } u * K = K * u'$$

$\cancel{H * K = K * H}$

$$g' * u' = g + u * K * v = g + K + \underbrace{u' * v}_{\in H} \rightarrow g' * u' \sim g * u$$

$G/H = G/\sim$ eredita una struttura di gruppo \rightarrow gruppo quoziente di G
modulo H
 $(G/H, *_{\sim_H}, [1])$ vale $[g]^{-1} = [g^{-1}]$

Rs $(\mathbb{Z}, +, \circ)$ gruppo, i sottogruppi sono della forma $n\mathbb{Z} = \{nK \mid K \in \mathbb{Z}\}$

$$\begin{array}{ll} \rightarrow n\mathbb{Z} \text{ normale} & \mathbb{Z}_{n\mathbb{Z}} \\ a \sim_S b \iff -a + b \in n\mathbb{Z} & \xrightarrow{\text{espl. l'opposto}} a' + b \in n\mathbb{Z} \\ \text{(o inverso di +)} & (g \sim g' \iff g' * g \in H) \\ a \sim_D b \iff a - b \in n\mathbb{Z} & \xrightarrow{\text{espl. la somma}} a - b \in n\mathbb{Z} \\ \text{(o inverso di -)} & (g \sim g' \iff g * (g')^{-1} \in H) \end{array}$$

Quindi $\mathbb{Z}_{n\mathbb{Z}} = \mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \bar{n-1}\}$