Def di Gruppo

Struttura algebrica $(A, *)$ con A insieme

$* : A \times A \longrightarrow A$ operazione binaria

tale che

1) $\exists e \in A : \forall a \in A : \quad a * e = e * a = a$ (el. neutro).
2) $\forall a \in A \ \exists a' \in A \quad a * a' = a' * a = e$ (esistenza degli inversi)
3) $\forall a, b, c \in A : \quad (a * b) * c = a * (b * c)$ (prop. associativa).

Esempi $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$ $(\mathbb{C}, +)$

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

$\mathbb{K}^* = \mathbb{K} \setminus \{0\}$

Un gruppo è detto commutativo o abeliano se

$\forall a, b \in A \quad a * b = b * a$

Sia $(\mathbb{K}, +, \cdot)$ un campo $\Rightarrow GL(n, \mathbb{K}) = \{ M : \text{matrici } n \times n \text{ ad entrate in } \mathbb{K} \text{ con } \det(M) \neq 0 \}$

$GL(n, \mathbb{K})$ è un gruppo non commutativo

$SL(n, \mathbb{K}) = \{ M \in GL(n, \mathbb{K}) \mid \det(M) = 1 \}$

Ricordiamoci che un anello è una struttura algebrica $(A, +, \cdot)$ ove

1) $(A,+)$ gruppo commutativo

2) $(A,\cdot)$ è associativa

3) valgono le prop. distributive
$\forall a,b,c \in A \quad (a+b)\cdot c = ac+bc$
$a(b+c) = ab+ac$

Es. $(\mathbb{Z},+,\cdot)$

- Un anello è detto con unità se $\exists\, 1 \in A$ elemento neutro per il prodotto
- Un anello è detto commutativo se l'operazione $\cdot$ è commutativa
- Un anello (commutativo e con unità) è detto campo se $(A\setminus\{0\},\cdot)$ è un gruppo commutativo.

~~$(\mathbb{Q},+,\cdot)$ $(\mathbb{R},+,\cdot)$ $(\mathbb{C},+,\cdot)$~~

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

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

$(\mathbb{F}_2,+,\cdot)$ è un campo.

Gruppi Ciclici

Un gruppo $(G,+)$ è detto ciclico se $\exists\, g \in G$ tale che $\forall h \in G \ \exists i$ con $h = \underbrace{g+g+\dots+g}_{i \text{ volte}}$

o $h = \underbrace{-(g+g+\dots+g)}_{i \text{ volte}}$.

g è detto generatore di G

$G = \langle g \rangle$

$(\mathbb{Z}, +)$ $\quad \mathbb{Z} = \langle 1 \rangle$

In generale se $(G', \cdot)$ $\quad G' = \langle g' \rangle$

$(G, +)$ sono gruppi ciclici $\quad G = \langle g \rangle$

scriveremo $h' \in G'$ come $h' = g'^{i} \quad i \in \mathbb{Z}$

$h \in G$ come $h = i \cdot g \quad i \in \mathbb{Z}$

(i: numero; g: elemento del gruppo)

Sia $n > 0$ un intero. Definisco su $\mathbb{Z}$ la relazione di equivalenza $a \equiv b \pmod n$

se $n \mid (a-b)$ cioè se $\exists k \in \mathbb{Z}$ tale che $(a-b) = kn$.

(n divide)

"essere congruenti modulo n"

RIFLESSIVA $(a-a) = 0 = 0n \qquad a \equiv a \bmod n$

SIMMETRICA $(a-b) = kn \Rightarrow (b-a) = -kn = (-k)n \qquad a \equiv b \bmod n \Rightarrow b \equiv a \bmod n$

TRANSITIVA $a \equiv b \bmod n \rightarrow (a-b) = kn$

$b \equiv c \bmod n \quad (b-c) = hn$

$\Rightarrow (a-c) = kn + hn = (k+h)n$

$\Rightarrow a \equiv c \bmod n$

come sono fatte le classi di equivalenza?

$$[a]_n := \{ b \in \mathbb{Z} \mid a \equiv b \bmod n \} =$$

$$= \{ b \in \mathbb{Z} \mid (a-b) = kn \} = \{ b \in \mathbb{Z} \mid a = kn + b \} =$$

simm. $$= \{ b \in \mathbb{Z} \mid (b-a) = kn \} = \{ b \in \mathbb{Z} \mid b = kn + a \} =$$

$$= \{ kn + a \mid k \in \mathbb{Z} \} = \boxed{a + n\mathbb{Z}}$$

ove $n\mathbb{Z} := \{ kn \mid k \in \mathbb{Z} \}$.

$$\{ a + x \mid x \in n\mathbb{Z} \}.$$

oss 1) Le classi di equivalenza di $a \equiv b \bmod n$ sono in corrispondenza 1 ad 1 con i possibili resti della divisione per n.

Supponiamo infatti $a = \alpha n + r_1$

$b = \beta n + r_2$

$$\Rightarrow (a-b) = (\alpha - \beta)n + (r_1 - r_2)$$

$$a \equiv b \bmod n \iff r_1 = r_2$$

Le classi di equivalenza mod n sono n

Scriviamo l'insieme di queste classi come

$$\boxed{\mathbb{Z}_n := \frac{\mathbb{Z}}{n\mathbb{Z}}}$$

$a \equiv b \mod n \iff (a-b) = kn \iff (a-b) \in n\mathbb{Z}$

$\mathbb{Z}_n$ può essere dotato della struttura di gruppo ciclico.

$(\mathbb{Z}_n, \oplus)$

$$(a + n\mathbb{Z}) \oplus (b + n\mathbb{Z}) := (a+b) + n\mathbb{Z}$$

$n = 10$

$$[3] \oplus [11] = [11+3] = [14]$$

$$[14] = [14 \,\%\, 10] = [4]$$

<u>oss</u> 1) $[0]$ è elemento neutro

2) $[a] \oplus [-a] = [a-a] = [0]$

3) $[a] \oplus [b] = [a+b] = [b+a] =$

$$= [b] \oplus [a]$$

4) $([a] \oplus [b]) \oplus [c] = [(a+b)+c] =$

$$= [a+(b+c)] =$$

$$= [a] \oplus ([b] \oplus [c]).$$

<u>N.B</u> dovremmo verificare che $\oplus$ è ben posta

$\forall \alpha \in [a] \; \forall \beta \in [b]$ si ha $\alpha + \beta \in [a+b]$

$a \in [a] \iff a = a + kn$

$\beta \in [b] \iff \beta = b + hn$ $\Rightarrow$ $\alpha+\beta = (a+b) + (k+h)n \in [a+b]$

$(\mathbb{Z}_n, +)$ è un gruppo commutativo finito con n elementi

oss II: in $(\mathbb{Z}_n, +)$ ogni classe si scrive come $[a]$ con $a \in \{0, 1, \dots, n-1\}$.

inoltre $[a+1] = [a] + [1]$

$$[a] = a\,[1]$$

$$\uparrow$$

$$\underbrace{[1]+[1]+\dots+[1]}_{a \text{ volte}}$$

$\Rightarrow$ $(\mathbb{Z}_n, +)$ è un gruppo ciclico con n elementi generato da $[1]$

$n=5$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

↑ chiavi

← messaggi

ogni riga contiene tutti gli elementi

$\cdot$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

NON È UN GRUPPO

OSS: Se $(G, \cdot)$ è un gruppo allora

$\forall g \in G$ la funzione $t_g : \begin{cases} G \to G \\ h \to h \cdot g \end{cases}$

è una bijezione. $t_{g^{-1}}$

Similmente $\tau_g : \begin{cases} G \to G \\ h \to g \cdot h \end{cases}$

0 1 2 3 ——— 25

A B C D ——— Z

C D

2 3 ——— B

$a \to a + 2 \bmod 26$

$\mathbb{Z}_{26}$

$\mathbb{Z}_{26}$ $\quad E(k, d) := d + k \bmod 26$

$m = (d_1 d_2 \dots d_n)$ messaggio di n caratteri

ECB

$(E(k, d_1), E(k, d_2) \dots E(k, d_n))$

(Electronic) Codebook Mode

oss 1) possiamo forzare la codifica di Cesare per forza bruta testando 26 chiavi

2) Si può fare di meglio?

Def Gruppo simmetrico: Sia X un insieme

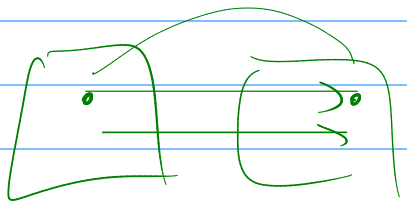
consideriamo $S(X)$ il gruppo i cui elementi sono le biiezioni $f: X \to X$ rispetto l'op. di composizione di funzioni

A) $i: \begin{cases} X \to X \\ x \to x \end{cases}$ è l'identità infatti

$$(f \circ i)(x) = f(i(x)) = f(x)$$
$$(i \circ f)(x) = i(f(x)) = f(x).$$

B) $\forall f \in S(X)$ poniamo $f^{-1}(x) :=$ elemento $y \in X$ con $f(y) = x$

$$f \circ f^{-1} = \iota$$
$$f^{-1} \circ f = \iota$$



C) Vale la prop. associativa

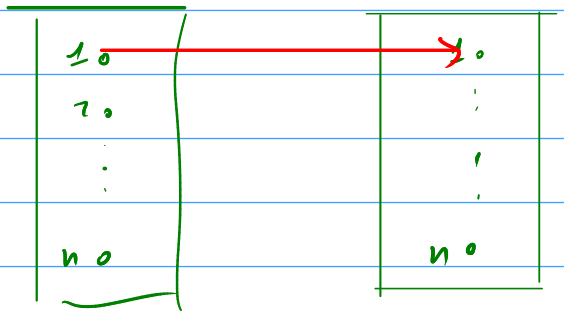
$$(f \circ g) \circ h = f \circ (g \circ h)$$

Massimo $S(X)$ come spazio delle chiavi
X come alfabeto.

$$E(\sigma, x) := \sigma(x)$$

Quanti elementi ci sono in $S(X)$?

se $|X| = n$



$f(1)$ ci sono n possibilità

$f(2)$ n n $n-1$ n

$\vdots$

$f(n-1)$ n n 2 possibilità

$f(n)$ 1 possibilità

$n \cdot (n-1) \cdot (n-2) \cdots \cdot 1 = n!$

$S_n := S(X)$ con $X = \mathbb{Z}_n$ ha $n!$ elementi