GRUPPI (I PARTE)

Def: Sia $(A,*)$ una coppia formata da un insieme A e da un'operazione:

$$* : A \times A \longrightarrow A \qquad \text{(operazione \underline{binaria} su } A)$$
$$(a_1, a_2) \longmapsto a_1 * a_2$$

1) Se l'operazione $*$ è associativa, $(A,*)$ si dice <u>semigruppo</u>
2) Se l'operazione $*$ è associativa ed esiste un elemento neutro $e \in A$ rispetto a $*$, allora $(A,*,e)$ si dice <u>monoide</u>.
3) Se $(A,*,e)$ è un monoide e $\forall a \in A \ \exists b \in A$ tale che $a * b = e = b * a$, cioè se esiste l'inverso di ogni elemento, allora $(A,*,e)$ si dice <u>gruppo</u>.
4) Se $(A,*,e)$ è un gruppo e l'operazione $*$ è commutativa, allora $(A,*,e)$ si dice <u>gruppo abeliano</u>.

Esempi:

1) $(\mathbb{N},+)$ l'operazione $+$ è associativa
esiste l'elemento neutro: 0 } $\Rightarrow$ $(\mathbb{N},+,0)$ è un monoide
(+ è commutativa) monoide commutativo

però, a parte 0, nessun numero naturale ha "inverso" rispetto all'addizione ....
dato $n\in\mathbb{N}$, il suo "inverso" m dovrebbe essere t.c. $m+n=0 \Rightarrow m=-n$ opposto
ma questo non sta in $\mathbb{N}$.

$(\mathbb{N},+,0)$ non è un gruppo.

2) $(\mathbb{Z},+)$ l'operazione $+$ è associativa
esiste l'el. neutro: 0
(commutativa)
$\forall x\in\mathbb{Z}\ \exists(-x)\in\mathbb{Z}$ t.c. $x+(-x)=0$
} $(\mathbb{Z},+,0)$ è un gruppo abeliano

3) $(\mathbb{Q},+,0)$, $(\mathbb{R},+,0)$ sono gruppi abeliani.

4) $(\mathbb{N}\setminus\{0\},+)$ è un semigruppo (+ è associativa, ma manca l'el. neutro).

5) Sia X un insieme.

$(\mathcal{P}(X), \cap)$

$\left.\begin{array}{l} \cap \text{ è associativa? Sì} \\ X \text{ è el. neutro: } \forall S \subseteq X,\ S \cap X = S \\ \cap \text{ è commutativa} \end{array}\right\}$ è un monoide commutativo

Non esiste, in generale l'inverso di un elemento: dato $S \subseteq X$, dovremmo trovare $T \subseteq X$ tale che $S \cap T = X$. Succede solo se $S = T = X$.

$(\mathcal{P}(X), \cap, X)$ non è un gruppo.

6) Sia X un insieme. Consideriamo $\mathcal{F}_X = \{ f \mid f : X \longrightarrow X \text{ è una funzione} \}$

$(\mathcal{F}_X, \circ)$

composizione di funzioni

$\left.\begin{array}{l} \circ \text{ è associativa} \\ \text{esiste l'el. neutro: } id_X : X \longrightarrow X \end{array}\right\}$ $(\mathcal{F}_X, \circ, id_X)$ è un monoide.

($\circ$ non è commutativa)

Non è un gruppo: $f \in \mathcal{F}_X$ ha inverso $\Leftrightarrow \exists g \in \mathcal{F}_X$ t.c. $\begin{cases} g \circ f = id_X \\ f \circ g = id_X \end{cases}$ ma questo succede solo per le funzioni biettive.

Mentre sappiamo che esistono funzioni non biettive (se $|X| \geq 2$)

7) Se restringiamo l'esempio precedente a $\mathcal{B}_X = \{ f \mid f : X \to X \text{ funzione biettiva} \}$

$(\mathcal{B}_X, \circ, id_X)$ è un gruppo (non abeliano)

Bisogna osservare che:
- la composizione di funzioni biettive è biettiva (quindi $\circ$ si restringe)
- $id_X \in \mathcal{B}_X$ (e l'operazione resta associativa)
- sappiamo che se f è biettiva $\Rightarrow \exists f^{-1} \in \mathcal{B}_X$ t.c. $f \circ f^{-1} = f^{-1} \circ f = id_X$

8) Se in particolare scegliamo $X = I_n = \{1, 2, 3, \dots, n\}$ allora

$\mathcal{B}_X = S_n$ insieme delle permutazioni.

$(S_n, \circ, id_{I_n})$ è un gruppo (non abeliano)

abbiamo visto esempi in cui $\sigma \circ \tau \neq \tau \circ \sigma$

9) Dato un insieme X finito. Consideriamo l'insieme $P_X = \{\text{parole sull'alfabeto } X\}$

un elemento di P_X è una stringa finita $x_n x_{n-1} \dots x_2 x_1 x_0$ con $x_i \in X$.

Come operazione consideriamo la "concatenazione": $(x_n \dots x_1 x_0) \cdot (y_m \dots y_1 y_0) = x_n \dots x_1 x_0 y_m \dots y_1 y_0$

$(P_X, \cdot, \{\})$ è un monoide

stringa vuota

10) Sia $N \in \mathbb{N}$, $N \geq 2$, consideriamo $(\mathbb{Z}_N, +)$.

Abbiamo visto che $+$ è associativa, commutativa, ha el. neutro, inoltre $\forall \bar{x} \in \mathbb{Z}_N$ $\exists \overline{-x}$ t.c. $\bar{x} + \overline{-x} = \bar{0}$, quindi $(\mathbb{Z}_N, +, \bar{0})$ è un gruppo abeliano.

Consideriamo ora le strutture moltiplicative degli insiemi numerici:

11) $(\mathbb{N}, \cdot, 1)$ è un monoide.

12) $(\mathbb{Z}, \cdot, 1)$ è un monoide.

$\}$ non sono gruppi (in generale gli inversi non esistono)

13) $(\mathbb{Q}, \cdot, 1)$ è un monoide, ma non è un gruppo perché 0 non ha inverso.

Il problema si risolve restringendo a $\mathbb{Q}^{\times} = \mathbb{Q} \setminus \{0\}$

$(\mathbb{Q}^{\times}, \cdot, 1)$ è un gruppo abeliano, infatti $\cdot$ è associativa e commutativa e

$$\forall x \in \mathbb{Q} \setminus \{0\} \quad \exists \frac{1}{x} \in \mathbb{Q} \setminus \{0\} \text{ t.c. } x \cdot \frac{1}{x} = 1.$$

Allo stesso modo $(\mathbb{R}^{\times}, \cdot, 1)$ è un gruppo abeliano. $(\mathbb{R}^{\times} = \mathbb{R} \setminus \{0\})$

Se consideriamo $\mathbb{Z}^{\times} = \{\pm 1\}$, $(\mathbb{Z}^{\times}, \cdot, 1)$ è un gruppo abeliano.

14) Consideriamo $(\mathbb{Z}_N, \cdot, \overline{1})$ $(N \geq 2)$ è un <u>monoide</u>.

In generale non è un gruppo, nemmeno togliendo lo $\overline{0}$, perché potrebbero esserci dei divisori di $\overline{0}$ (che non sono invertibili).

Se p è primo, allora $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{\overline{0}\}$ e $(\mathbb{Z}_p^\times, \cdot, \overline{1})$ è un <u>gruppo abeliano</u>

<u>Es.</u> $p=5$ $\mathbb{Z}_5^\times = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ $\overline{2} \cdot \overline{3} = \overline{1}$, $\overline{4} \cdot \overline{4} = \overline{1}$

Se N non è primo, occorre restringere di più: $\mathbb{Z}_N^\times \subsetneq \mathbb{Z}_N \setminus \{\overline{0}\}$, ma ancora $(\mathbb{Z}_N^\times, \cdot, \overline{1})$ è un gruppo abeliano.

<u>Es.</u> $N=12$ $\mathbb{Z}_{12}^\times = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$ $\overline{5} \cdot \overline{5} = \overline{1}$, $\overline{7} \cdot \overline{7} = \overline{1}$, $\overline{11} \cdot \overline{11} = \overline{1}$

15) Dati due gruppi $(G, *, e)$ e $(H, \square, i)$ allora

$G \times H$ ha una struttura di gruppo

$$(G \times H) \times (G \times H) \longrightarrow G \times H$$
$$((g_1, h_1), (g_2, h_2)) \longmapsto (g_1 * g_2, h_1 \square h_2)$$

elemento neutro: (e, i)

Inverso: $(g, h)^{-1} = (g^{-1}, h^{-1})$