ARITMETICA 6 NOV 2017

Note Title 11/6/2017

Gruppi

Definizione Un gruppo è un insieme G dotato di un'operazione (binaria) $* : G \times G \to G$ con le seguenti proprietà:

- l'operazione è associativa
  $(a*b)*c = a*(b*c) \quad \forall a, b, c \in G$

- esiste un elemento neutro $e \in G$, cioè
  $e * x = x * e = x \quad \forall x \in G$

- ogni elemento ha un inverso, cioè
  $\forall x \in G \ \exists y \in G$ tale che
  $x * y = y * x = e$

La proprietà commutativa è FACOLTATIVA.

Esempi $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/m\mathbb{Z}$ $+$

moltiplicazione $\mathbb{Z}^* = \{\pm 1\}, \mathbb{Q}^* = \mathbb{Q} - \{0\}, \mathbb{R}^*, \mathbb{C}^*, (\mathbb{Z}/m\mathbb{Z})^*$

Isometrie del piano. Operazione: composizione.

S_n = gruppo di permutazioni su n elementi. (composizione)

Matrici

$m \times n$ con $+$

$n \times n$, con $\det \neq 0$, con $\cdot$

Gli ultimi esempi sono non commutativi

Es. S_n $n \geq 3$ non è commutativo.

$n = 3$

σ	τ
$1 \to 2$	$1 \to 2$
$2 \to 1$	$2 \to 3$
$3 \to 3$	$3 \to 1$

$\sigma \circ \tau$	$\tau \circ \sigma$
$1 \to 1$	$1 \to 3$
$2 \to 3$	$2 \to 2$
$3 \to 2$	$3 \to 1$

Notazione L'operazione $*$ si denota spesso con $\cdot$ (moltiplicazione)

Regole di calcolo

Cancellazione:

$$ac = bc \Rightarrow a = b$$

($ac = bc \Rightarrow acc^{-1} = bcc^{-1} \Rightarrow ae = be \Rightarrow a = b$)

(c^{-1} è l'inverso)

Vale anche $ca = cb \Rightarrow a = b$

Inverso del prodotto:

$$\boxed{(ab)^{-1} = b^{-1}a^{-1}}$$

$$ab \cdot b^{-1}a^{-1} = a e a^{-1} = a a^{-1} = e$$

Analogamente $b^{-1}a^{-1}ab = e$.

In un gruppo si risolvono le equazioni del tipo

$$ax = b \qquad xa = b$$

Se $ax = b$, allora

$$x = ex = a^{-1}ax = a^{-1}b$$

D'altra parte, se $x = a^{-1}b$, allora

$$ax = a a^{-1}b = eb = b$$

Una e una sola soluzione

Tabella di moltiplicazione

Es $G = (\mathbb{Z}/5\mathbb{Z})^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

In ogni riga ed in ogni colonna tutti gli elementi compaiono una e una sola volta

Riga corrispondente all'elemento $a \in G$ contiene gli elementi ax per tutti gli $x \in G$

$$x \to ax$$

è una funzione bigettiva

Questo corrisponde all'esistenza e unicità della soluzione dell'equazione

$$ax = b$$

Surgettività $\forall b \in G \ \exists$ una soluzione

Iniettività unicità della soluzione

SOTTOGRUPPI

Def. Un sottoinsieme NON VUOTO H di un gruppo G si dice un SOTTOGRUPPO di G se è esso stesso un gruppo con l'operazione INDOTTA da G.

INDOTTA: Faccio l'operazione che c'è in G, ma restringendomi ai soli elementi di H.

Notazione: $H < G$ $(H \leq G)$ vuol dire H è un sottogruppo di G.

Esempi $m\mathbb{Z} < \mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$

$\downarrow$

multipli di m

Rotazioni con centro O < Isometrie

Matrici di $\det = 1$ < Matrici invertibili

Regola per la verifica che un sottoinsieme H di G è in realtà un sottogruppo di G

Si devono fare le seguenti verifiche:

1. $e \in H$
2. $x \in H, y \in H \Rightarrow xy \in H$
3. $x \in H \Rightarrow x^{-1} \in H$.

Oss L'identità è unica

Supponiamo che e_1, e_2 siano due elementi neutri. Allora

$e_2 = e_1 e_2 = e_1$ $\quad e_2$ è neut.

$\downarrow$

e_1 è neutro

L'associatività è ovvia.

La proprietà 2 ci dice che in H è un'operazione (associativa)

La proprietà 1 ci dice che c'è l'el. neutro.

La proprietà 3 ci dice che ogni elemento ha un inverso.

Oss. Si possono combinare (2) e (3) in

$x \in H, y \in H \Rightarrow x y^{-1} \in H$

Proposizione I sottogruppi di $\mathbb{Z}$ sono tutti e soli quelli della forma
$m\mathbb{Z}$ con $m \geq 0$.

Dim. Intanto controlliamo che questi siano sottogruppi:

① - $0 \in m\mathbb{Z}$ $\quad 0 = m \cdot 0$
② - $x, y \in m\mathbb{Z} \Rightarrow x+y \in m\mathbb{Z}$
③ - $x \in m\mathbb{Z} \Rightarrow -x \in m\mathbb{Z}$

② $x = mh \quad y = mk \quad x+y = mh+mk = m(h+k)$

③ $x = mh \quad -x = -mh = m(-h)$

Ora dimostriamo che non ce ne sono altri.
Sia $H < \mathbb{Z}$.
Certamente $0 \in H$
Se $H = \{0\}$ FUNZIONA e $H = 0 \cdot \mathbb{Z}$
Se $H \neq \{0\}$ $H \ni$ elemento $x \neq 0$
Se $x < 0$ so che $H \ni -x > 0$.
In ogni caso H contiene un elemento positivo.
$S = \{x \in H, x > 0\}$. $S \neq \emptyset$.
$S \subseteq \mathbb{N}$

$\Rightarrow S$ ha un elemento minimo m.
Voglio dimostrare che $H = m\mathbb{Z}$

- $H \supseteq m\mathbb{Z}$

$m \in H \qquad m+m = 2m \in H$

Per induzione $\quad km \in H \quad \forall k > 0$.

$(km + m = (k+1)m)$

$m \cdot 0$ è OK

Se $k > 0$ e $h = -k$

$mh = m(-k) = -mk$ è l'opposto di mk

- $H \subseteq m\mathbb{Z}$

Sia $x \in H$

Divisione euclidea:

$$x = qm + r \qquad 0 \leq r < m$$

$$r = x - qm = x + (-qm) \in H$$

$\in H$ (sotto qm)

$x \in H$, $-qm \in H$, $x \in H$, $-qm \in H$

r non può essere positivo (altrimenti sarebbe minore del minimo di S).

$\Rightarrow r = 0$

e dunque $x = qm \in m\mathbb{Z}$

$H, K < G$

$H \cup K < G$?

$H \cap K < G$?

Intersezione è OK. $\quad H \cap K < G$

Infatti:

$e \in H$, $e \in K \Rightarrow e \in H \cap K$

se $x \in H \cap K$, $y \in H \cap K$ allora

$x \in H$, $y \in H$ $\quad$ $x \in K$, $y \in K$

$xy \in H$ $\quad$ $xy \in K$

$xy \in H \cap K$

se $x \in H \cap K$ allora $x \in H$ $x \in K$

quindi $x^{-1} \in H$ $x^{-1} \in K$ $\Rightarrow x^{-1} \in H \cap K$.

L'unione no, a meno dei casi particolari

$H \subseteq K$ $\quad$ $K \subseteq H$. (casi ovvi)

Supponiamo di non essere in questi casi particolari

$H \not\subseteq K$ $\quad$ $K \not\subseteq H$

$\exists x \in H, x \notin K$ $\quad$ $\exists y \in K, y \notin H$

Se $xy \in H \cup K$ avrei

- $xy = h \in H$ $\quad$ $y = x^{-1}h$ $\quad$ $y \in H$ $\quad$ contraddizione
- $xy = k \in K$ $\quad$ $y \in K$

.