

Sottostrutture algebriche (di st. con 1 op. binaria) (155)

Consideriamo una struttura algebrica $(X, *)$ e un sottoinsieme $A \neq \emptyset$ di X . Se $(A, *)$ ha la stessa struttura algebrica di $(X, *)$ dico che

$(A, *)$ è una sottostruttura algebrica di $(X, *)$

Che cosa significa?

Vediamolo sulle principali str. alg.

1) $(X, *)$ semigruppo : $(A, *)$ sarà sottosemigruppo di $(X, *)$ se

- $\forall a_1, a_2 \in A$ si ha $a_1 * a_2 \in A$
- $*$ è associativa: questa proprietà vale certamente poiché se $\forall x_1, x_2, x_3 \in X$ si ha $(x_1 * x_2) * x_3 = x_1 * (x_2 * x_3)$ lo stesso vale in particolare per ogni terza di elem. di $A \subseteq X$

2) $(X, *)$ monoido : $(A, *)$ sarà sottomonoido di $(X, *)$ se

- $(A, *)$ sottosemigruppo di $(X, *)$ (vedi 1)
- l'elemento neutro n di X appartiene ad A .

Attenzione: NON BASTA CHE A abbia "un elemento neutro". Deve essere lo stesso di X .

Ad es. se $S = \{1, 2\}$ e $(X, *) = (S^S, o)$ (vedi p. 151) il sottoinsieme $A = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} \right\}$ è tale che $\begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$ e quindi in A l'elemento $\begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$ funziona da neutro. Ma (A, o) NON è un sottomonoido di (S^S, o) pur essendone sottosemigruppo.

3) $(X, *)$ gruppo : $(A, *)$ sarà sottogruppo di $(X, *)$ se

- $(A, *)$ sottomonoido di $(X, *)$ (vedi 2)
- $\forall a \in A$ l'inverso a^{-1} in X rispetto a $*$ appartiene ad A .

La condizione data sull'inverso equivale a chiedere

che ogni $a \in A$ sia dotato di inverso $\bar{a} \in A$ rispetto a $*$.

- E' ovvio che, se $\forall a \in A$ l'inverso in X di a sta in A si ha

$$a * a^{-1} = a^{-1} * a = u \quad (\text{neutro sia di } X \text{ che di } A \text{ per (2)})$$

- Viceversa se $\forall a$ esiste $\bar{a} \in A$ t.c.

$$a * \bar{a} = \bar{a} * a = u$$

si ha

$$a^{-1} * (a * \bar{a}) = \dots = a^{-1} * u$$

$$\text{pr. ass. } \Downarrow (a^{-1} * a) * \bar{a} = \dots = a^{-1} * u$$

$$a^{-1} \text{ inverso in } X \Downarrow u * \bar{a} = \dots = a^{-1} * u$$

$$\text{neutro ds. sim. } \Downarrow \bar{a} = a^{-1}$$

4) $(X, *)$ semireticolo : $(A, *)$ sarà sottosemireticolo di $(X, *)$ se

- $(A, *)$ sottosemigruppo di $(X, *)$
- $*$ è commutativa: certo vero poiché lo è più in generale in $(X, *)$
- ogni elem. di A è idempotente : certo vero come sopra.

Si vede quindi che per verificare che un sottoinsieme A di $(X, *)$ ne sia una sottostruzione basta:

- 1) se $(X, *)$ è semigruppo : verificare che A non sia \emptyset e che l'operazione $*$ sia INTERNA ad A .
- 2) se $(X, *)$ è monoidale : verificare che il neutro di X sta in A ($\Rightarrow A \neq \emptyset$) e che $*$ sia INTERNA ad A .
- 3) se $(X, *)$ è un gruppo : verificare come in (2) e che $\forall a \in A$ anche $a^{-1} \in A$ (a^{-1} inverso in X di A)
- 4) se $(X, *)$ è reticolo : verificare che A non sia \emptyset e che l'operazione $*$ sia interna ad A .

ESEMPI.

1) L'insieme dei numeri interi dispari D è un sottosemigruppo di

• $(\mathbb{Z}, +)$? 1) $D \neq \emptyset$ ad es. $D \ni 1$

2) $\forall 2h+1, 2k+1, h, k \in \mathbb{Z} : (2h+1)+(2k+1) \in D$?

NO: \Rightarrow non commutativa.

• (\mathbb{Z}, \circ) ? 1) $D \neq \emptyset$ 2) $\forall 2h+1, 2k+1 \dots (2h+1)(2k+1) \in D$?

SI: sottosemigruppo,

ma è un sottomonoido? SI: $1 \in D$

2) L'insieme $2\mathbb{Z}$ dei numeri interi pari è un sottosemigruppo di

• $(\mathbb{Z}, +)$: 1) $2\mathbb{Z} \neq \emptyset$ 2) $2h+2k, h, k \in \mathbb{Z}$ è pari
sottosemigruppo

ma è un sottomonoido? $0 \in 2\mathbb{Z}$ SI

ma è un sottogruppo? $ta = 2h - a \in 2\mathbb{Z} : \text{SI}$
 $t \in \mathbb{Z}$

• (\mathbb{Z}, \circ) 1) $2\mathbb{Z} \neq \emptyset$
2) $(2h)(2k) \in 2\mathbb{Z}$ (sottosemigruppo): SI

ma è un sottomonoido? $1 \notin 2\mathbb{Z}$: NO

3) L'insieme $SL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2x2}(\mathbb{R}) \mid ad-bc=1 \right\}$

i) è un sottomonoido di $M_{2x2}(\mathbb{R})$ con prodotto righe x col?

ii) è un sottogruppo di $GL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2x2}(\mathbb{R}) \mid ad-bc \neq 0 \right\}$
con prodotto righe per colonne?

i) $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in SL_2(\mathbb{R})$: SI $1 \cdot 1 - 0 \cdot 0 = 1$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix} \Rightarrow$$

$$(aa' + bc')(cb' + dd') - (ab' + bd')(ca' + dc') =$$

$$= ad(a'd' - b'c') - (ad)b'c' + bc(a'd') =$$

$$= ad(a'd' - b'c') + bc(b'c' - a'd') =$$

$$= (ad - bc)(a'd' - b'c') = 1 \cdot 1$$

e quindi $SL_2(\mathbb{R})$ è un sottomonoide di $M_2(\mathbb{R})$. (158)

ii) immaisi tutto: è vero che $SL_2(\mathbb{R}) \subseteq GL_2(\mathbb{R})$?

Cioè le matrici di $SL_2(\mathbb{R})$ sono invertibili? Sia $a \neq 0$

$$\left(\begin{array}{cc|cc} a & b & 1 & 0 \\ c & d & 0 & 1 \end{array} \right) \leftarrow \text{Matrice che traduce il sistema} \\ \underbrace{\text{matr.}}_{\text{dei coeff.}} \quad \overbrace{\text{T.N.}}^{\text{T.N.}} \quad \left(\begin{array}{cc} a & b \\ c & d \end{array} \right) \left(\begin{array}{cc} x & y \\ z & w \end{array} \right) = \left(\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right) \dots \text{Perché?}$$

moltiplico la I riga per $\frac{1}{a}$:

$$\left(\begin{array}{cc|cc} 1 & b/a & 1/a & 0 \\ c & d & 0 & 1 \end{array} \right) \text{ sottraggo } c \text{ volte la I riga alla II:}$$

$$\left(\begin{array}{cc|cc} 1 & b/a & 1/a & 0 \\ 0 & d - \frac{bc}{a} & -c/a & 1 \end{array} \right) \quad d - \frac{bc}{a} = \frac{ad - bc}{a} = \frac{1}{a} \quad \begin{matrix} \text{poiché} \\ \text{così} \\ \text{def. } SL_2(\mathbb{R}) \end{matrix}$$

$$\left(\begin{array}{cc|cc} 1 & b/a & 1/a & 0 \\ 0 & 1/a & -c/a & 1 \end{array} \right) \text{ sottraggo } b \text{ volte la II riga alla I:}$$

$$\left(\begin{array}{cc|cc} 1 & 0 & 1/a + bc/a & -b \\ 0 & 1/a & -c/a & 1 \end{array} \right) \text{ moltiplico per a la II riga:}$$

$$\left(\begin{array}{cc|cc} 1 & 0 & 1/a + bc/a & -b \\ 0 & 1 & -c & a \end{array} \right) \quad \text{se } ad - bc = 1, \quad \frac{1+bc}{a} = d$$

$\left(\begin{array}{cc|cc} 1 & 0 & d & -b \\ 0 & 1 & -c & a \end{array} \right)$ - Se $a \neq 0$ la stessa matrice $\left(\begin{array}{cc} d & -b \\ -c & a \end{array} \right)$ funziona da inversa e quindi
cioè se $a \neq 0$ e $ad - bc = 1$, la matrice $\left(\begin{array}{cc} a & b \\ c & d \end{array} \right)$
ha inversa (\Rightarrow sta in $GL_2(\mathbb{R})$) e tale
inversa ha la forma $\left(\begin{array}{cc} d & -b \\ -c & a \end{array} \right)$. vale

Secondo fatto: $SL_2(\mathbb{R})$ è chiuso rispetto a prodotto
e contiene il neutro di $GL_2(\mathbb{R})$: $\left(\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right)$ (VEDI i))

Treda verifica: l'inversa di una matrice $\left(\begin{array}{cc} a & b \\ c & d \end{array} \right) \in SL_2(\mathbb{R})$
sta in $SL_2(\mathbb{R})$?

$$\left(\begin{array}{cc} a & b \\ c & d \end{array} \right)^{-1} = \left(\begin{array}{cc} d & -b \\ -c & a \end{array} \right) \quad e \quad da - (-b)(-c) = ad - bc = 1$$

Quindi $SL_2(\mathbb{R})$ è sottogruppo di $GL_2(\mathbb{R})$.

Quel che andiamo a fare ora (determinare un criterio per stabilire se un sottoinsieme di un gruppo $(X, *)$ è un sottogruppo) somiglia a una cosa ben nota a proposito di spazi e sottospazi vettoriali.

Per stabilire se un sottoinsieme U di uno spazio vett. V (con operazione interne: + e operazione esterna: prodotto per scalare $\in \mathbb{R}$) è un sottospazio vettoriale posso agire in 2 modi equivalenti:

- A) mostro che:
 ① $\forall \underline{u}_1, \underline{u}_2 \in U$ si ha $\underline{u}_1 + \underline{u}_2 \in U$
 ② $\forall \underline{u} \in U, \forall a \in \mathbb{R}$ si ha $a\underline{u} \in U$

B) mostro che: $\forall a, b \in \mathbb{R}$ e $\forall \underline{u}_1, \underline{u}_2 \in U$ si ha $a\underline{u}_1 + b\underline{u}_2 \in U$.

A) \Rightarrow B) poiché se vale ② $\forall a, b \in \mathbb{R}$ e $\forall \underline{u}_1, \underline{u}_2 \in U$ si ha $a\underline{u}_1 \in U$ e $b\underline{u}_2 \in U$ e quindi se vale ①: $a\underline{u}_1 + b\underline{u}_2 \in U$.

B) \Rightarrow A) poiché, (prendendo $a=b=0$) si vede che $0 = 0\underline{u}_1 + 0\underline{u}_2 \in U$
 (prendendo $a=b=1$) si ha $\underline{u}_1 + \underline{u}_2 \in U$
 (prendendo $a=1, b=0$) si ha $a\underline{u}_1 \in U$
 e questo $\forall \underline{u}_1, \underline{u}_2 \in U$ e per ogni $a \in \mathbb{R}$.

Si usa più facilmente B) se si immagina che U sia un sottospazio di V mentre si usa (uno solo possibilmente dei punti (0), (1), (2) di) A se si vuol provare che U non è un sottospazio vettoriale.

ESA) L'insieme U dei polinomi reali di grado esattamente 1 non è un sottospazio vettoriale dello sp. vett. (su \mathbb{R}) $\mathbb{R}[x]$ poiché $0 \notin U$.

ESB) L'insieme U dei polinomi $p(x) \in \mathbb{R}[x]$ che valgono 0 in $x=1$ è un sottosp. vett. di $\mathbb{R}[x]$ poiché $\forall p, q \in \mathbb{R}[x]$ tali che $p(1)=0=q(1)$ e $\forall a, b \in \mathbb{R}$ si ha $(ap(x)+bq(x))_{x=1} = a p(1) + b q(1) = a \cdot 0 + b \cdot 0 = 0 \Rightarrow ap+bq \in U$.

Se $(X, *)$ è un gruppo c'è un modo talora più veloce di stabilire se $(A, *)$ è un suo sottogruppo (159)

PROP. Se $(X, *)$ è un gruppo e $A \subseteq X$, allora $(A, *)$ è sottogruppo di $(X, *)$ se e solo se $\forall a, b \in A$ si ha $a * b^{-1} \in A$.

Dim. Se $(A, *)$ è sottogruppo di $(X, *)$ allora

$$1) b \in A \Rightarrow b^{-1} \in A$$

2) $a, b^{-1} \in A \Rightarrow a * b^{-1} \in A$ e quindi è fondata la seconda implicazione.

Viceversa, se $\forall a, b \in A$ si ha $a * b^{-1} \in A$:

$$1) u = a * a^{-1} \in A$$

$$2) u * a^{-1} = a^{-1} \in A$$

3) $\forall a, b \in A, b^{-1} \in A$ e quindi $a * (b^{-1})^{-1} \in A$
cioè $a * b \in A$.

Ricordiamo che se $(X, *)$ è un gruppo, $*$ è associativa e quindi sono definite le potenze intere di ogni elemento $a \in X$:

$$\text{se } n=1 \quad a^n = a$$

$$\text{se } n \geq 1 \quad a^n = a * a^{n-1}$$

$$\text{se } n=0 \quad a^0 = u \quad \text{per def}$$

$$\text{se } n=-1 \quad a^{-1} \text{ è l'inverso di } a$$

$$\text{se } n < -1 \quad a^n = (a^{-1})^{-n}$$

vedi 159bis

ES. 1. È vero che $\forall a \in (X, *)$ gruppo

$$A = \{a^n, n \in \mathbb{Z}\}$$

è un sottogruppo di $(X, *)$?

Provo che \forall coppia di el. in A : a^m, a^n con $m, n \in \mathbb{Z}$ (event. coincidenti) si ha $a^m * (a^n)^{-1} \in A$

A proposito di potenze:

(159
bis)

$$(a^m)^{-1} \stackrel{\text{①}}{=} a^{-m} \stackrel{\text{②}}{=} (a^{-1})^m \quad \forall m \text{ intero}$$

Dimo. per INDUZ.

- Se $m=0$: $(a^0)^{-1} = a^{-0} = a^0 = a$, $(a^{-1})^0 = a$

- sia vero per m . Allora

$$\begin{aligned} (a^{m+1})^{-1} &= (a^m * a)^{-1} = a^{-1} * (a^m)^{-1} \stackrel{\text{IP. IND.}}{=} a^{-1} * a^{-m} \\ &= a^{-1} * (a^{-1})^m = (a^{-1})^{m+1} = a^{-(m+1)} \end{aligned}$$

DF potenza con exp < 0

quindi per induzione è vero $\forall m \geq 0$.

- Sia $m < 0$

$$(a^m)^{-1} \stackrel{\text{DF potenza con exp < 0}}{=} ((a^{-1})^{-m})^{-1} = \text{poiché } -m > 0 \text{ applico ①}$$

$$= (a^{-1})^{-(-m)} = (a^{-1})^m \quad \text{per l'algebra in } \mathbb{Z}$$

applico ②

all'elem.:

a^{-1} ed

exp: $-m$

$$((a^{-1})^{-1})^{-m} = a^{-m}$$



(160)

A proposito di intersezioni di infiniti sottogruppi

Considero i sottogruppi di $(\mathbb{Z}, +)$ delle forme

$$2k\mathbb{Z} = \{2kh \mid h \in \mathbb{Z}\} \text{ con } k \text{ intero qualsiasi}$$

Chi è $\bigcap_{k \in \mathbb{Z}} 2k\mathbb{Z}$? È l'insieme dei numeri

interi divisibili per ogni numero pari ... e quindi

è il sottogruppo formato dal solo elem. neutro:

(0) poiché non esistono interi divisibili per un numero infinito di numeri interi (e quindi di primi loro fattori).

Tuttavia se nel gruppo $(\mathbb{R}[x], +)$ considero i sottogruppi $(\mathbb{R}_n[x], +)$ con $n \geq 0$, $\bigcap_{n \in \mathbb{N}} \mathbb{R}_n[x] = \mathbb{R}_0[x]$ cioè è "all'incirca" (vedi isomorfismi) il gruppo $(\mathbb{R}, +)$.

$$\begin{aligned}
 a^n * (a^m)^{-1} &= a^n * a^{-m} = a^n * (a^{-1})^m = \\
 &= a^{n-1} * \underbrace{a * a^{-1}}_{=} * (a^{-1})^{m-1} = a^{n-1} * (a^{-1})^{m-1} = \dots \\
 &= a^{n-m} \in A \Rightarrow \text{gruppo.}
 \end{aligned} \tag{160}$$

ES. 2 Sia $(X, *)$ un gruppo abeliano. Allora l'insieme

$$A = \{a \in X \mid a^n = u \text{ per un certo } n \in \mathbb{N}^*\}$$

è un sottogruppo di $(X, *)$?

L'insieme A non è vuoto poiché contiene almeno u . Adesso:
Siano $a, b \in A$ t.c. $a^n = u, b^m = u$

$$\begin{aligned}
 a * b^{-1} \in A ? \quad (a * b^{-1})^n &= (\underbrace{a * b^{-1}}_{\substack{\text{poiché } * \text{ è comm.} \\ \text{e assoc.}}} * \underbrace{a * b^{-1} * \dots * a * b^{-1}}_{\substack{n \text{ volte}}} * \dots * \underbrace{a * b^{-1}}_{\substack{n \text{ volte}}} = \\
 &= \underbrace{a * a * \dots * a}_{\substack{n \text{ volte}}} * \underbrace{b^{-1} * b^{-1} * \dots * b^{-1}}_{\substack{n \text{ volte}}} = \\
 &= a^n * (b^{-1})^n = a^n * b^m = a^n * (b^m)^{-1} = u * u^{-1} = u
 \end{aligned}$$

ES. 3 Sia $(X, *)$ un gruppo e siano $(A, *)$ e $(B, *)$ due suoi sottogruppi.

L'insieme $A \cap B$ è un sottogruppo rispetto a $*$?

E se prendo $n > 2$ sottogruppi $(A_i, *)$ cosa posso dire di $A_1 \cap A_2 \cap \dots \cap A_n$?

E se i sottogruppi $(A_i, *)$ fossero infiniti?

L'insieme $A \cap B$ contiene almeno l'elemento neutro.

$\forall a, b \in A \Rightarrow a * b^{-1} \in A$ poiché $(A, *)$ è gruppo

$\forall a, b \in B \Rightarrow a * b^{-1} \in B$ "

quindi $\forall a, b \in A \cap B \Rightarrow a * b^{-1} \in A \cap B$

$\rightarrow A \cap B$ è sottogruppo

analog. se si ristretta su numero finito di sottogruppi di $(X, *)$.

Anche se sono infiniti sgr. di $\bigcap_{i \in I} A_i \supseteq A$
e quindi $\bigcap_{i \in I} A_i$ non è vuota e l'ultimo dice che è un sottogruppo

4) $\text{gr} (S_3, \circ)$ i sottogruppi

$$A = \{ \text{id}, (12) \}$$

$$B = \{ \text{id}, (12), (13) \}$$

$$C = \{ \text{id}, (123), (132) \}$$

$$D = \{ (12), (23) \}$$

Sono sottogruppi? Se non lo sono, quale è il più piccolo sottogruppo di S_3 che li contiene?

$$A \ni \text{id}, (12)^{-1} = (12) \in A \quad (12) \circ (12) = \text{id} \\ \text{id}^{-1} = \text{id} \in A \quad (12) \circ \text{id} = (12) \quad \left. \begin{array}{l} \text{id} \circ (12) = (12) \\ \text{id} \circ \text{id} = \text{id} \end{array} \right\} \Rightarrow \text{chiuso} \\ \text{risp. o}$$

$\Rightarrow A$ è un sottogruppo di S_3

C'è un sottogruppo di S_3 ?

$$(123), (123)^2 = (132), (123)^3 = \text{id}$$

$C = \{ (123)^n, n \in \mathbb{Z} \}$ è sottogruppo.

D: è un sottogruppo di S_3 ?

no poiché non contiene id che è l'elemento neutro

$$B: (12)(13) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (132) \notin B$$

\Rightarrow operazione non interna, quindi B non sgr

$$B = \frac{A}{\text{sgr}} \cup \underbrace{\{ \text{id}, (13) \}}_{\text{sgr}} \quad \text{ma non è sgr.}$$

posso fare l'unione gruppale di A e $\{ \text{id}, (13) \}$ cioè cercare il più piccolo sgr. di S_3 che contiene l'unione B , che è S_3 poiché un tale sgr. deve contenere $(132), (123), (23) = (123) \circ (13)$

5) in $(\mathbb{Z}, +)$ l'insieme $3\mathbb{Z}$ dei multipli di 3 e l'insieme $4\mathbb{Z}$ dei multipli di 4 sono sottogruppi? E $3\mathbb{Z} \cup 4\mathbb{Z}$? Se non lo sono qual è il più piccolo sottogruppo che li contiene? (162)

$$3\mathbb{Z} = \{3n, n \in \mathbb{Z}\} \text{ sgr.}$$

$$4\mathbb{Z} = \{4n, n \in \mathbb{Z}\} \text{ sgr.}$$

$3\mathbb{Z} \cup 4\mathbb{Z} = \{3n, 4n | n, n \in \mathbb{Z}\}$ non è un sgr. perché all'unione non appartiene sempre $4n - 3n$, ad es. non appartiene $4 - 3 = 1$

unione
gruppale
 $3\mathbb{Z} \oplus 4\mathbb{Z} = \mathbb{Z}$ poiché deve contenere $1 = 4 - 3$ e quindi ogni numero $1 \cdot n$ con $n \in \mathbb{Z}$

6) lo stesso con $6\mathbb{Z}$ e $4\mathbb{Z}$. S'inferisce una regola generale. ($\dots a\mathbb{Z} \oplus b\mathbb{Z} = \text{M.C.D}(a,b)\mathbb{Z}$)

$A = 6\mathbb{Z} \cup 4\mathbb{Z}$ non è un sgr poiché $6 - 4 = 2 \notin A$

$6\mathbb{Z} \oplus 4\mathbb{Z} = ?$ $6\mathbb{Z} \oplus 4\mathbb{Z} \supseteq 2\mathbb{Z}$ poiché contiene 2

è vero che $6\mathbb{Z} \oplus 4\mathbb{Z} \subseteq 2\mathbb{Z}$?

ogni suo el.: $6h - 4k = 2(3h - 2k) \in 2\mathbb{Z}$) si

N.B. Fare l'unione gruppale di un certo numero di sottogruppi di un gruppo $(X, *)$ significa trovare il più piccolo sottogruppo di $(X, *)$ che contiene ciascuno di tali sottogruppi, cioè fare l'intersezione di tutti i sottogruppi che ne contengono l'unione minimistica.