Cenni di Algebra Astratta

Prof.
Marco
Compagnoni

- Insiemi
- Relazioni
- Funzioni

SEZIONE 2.1

- Operazioni
- Strutture algebriche
- Gruppi
- Campi

SEZIONE 2.2

- Relazione di equivalenza

SEZIONE 2.4

INSIEMI (2.1)

Un insieme è una collezione di oggetti.

$A = \{a_1, \dots, a_n\}$ $\quad |A| = n =$ cardinalità di A

Insiemi di cardinalità infinita:

$\mathbb{N} = \{0, 1, 2, \dots\}$ $\quad \mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$

$\mathbb{Q} = \{q = \frac{m}{n} \mid m, n \in \mathbb{Z},\ n \neq 0\}$ $\quad \mathbb{R} = \{x$ numeri decimali$\}$

$\mathbb{C} = \{z = x + iy \mid x, y \in \mathbb{R},\ i^2 = -1\}$

Operazioni tra sottoinsiemi: $A \cup B$, $A \cap B$, $A \setminus B$.

Prodotto cartesiano: dati $A_1 = \{a_{11}, \dots, a_{1n_1}\}, \dots, A_m = \{a_{m1}, \dots, a_{mn_m}\}$

$$A_1 \times \dots \times A_m = \{\underbrace{(a_{11}, a_{21}, \dots, a_{m1})}_{n\text{-upla di elementi}}, \dots, (a_{1n_1}, a_{2n_2}, \dots, a_{mn_m})\}$$

Relazione: sottoinsieme del prodotto cartesiano $A_1 \times \dots \times A_m$

$A = \{a_1, a_2\}$, $B = \{b_1, b_2\}$ $\Rightarrow$

$A \times B = \{(a_1, b_1), (a_1, b_2), (a_2, b_1), (a_2, b_2)\}$

$R_0 = \emptyset$,

$R_1 = \{(a_1, b_1)\}$, $R_2 = \{(a_1, b_2)\}$, $R_3 = \{(a_2, b_1)\}$, $R_4 = \{(a_2, b_2)\}$,

$R_5 = \{(a_1, b_1), (a_1, b_2)\}$, $R_6 = \{(a_1, b_1), (a_2, b_1)\}$, $R_7 = \{(a_1, b_1), (a_2, b_2)\}$,

$R_8 = \{(a_1, b_2), (a_2, b_1)\}$, $R_9 = \{(a_1, b_2), (a_2, b_2)\}$, $R_{10} = \{(a_2, b_1), (a_2, b_2)\}$,

$R_{11} = \{(a_1, b_1), (a_1, b_2), (a_2, b_1)\}$, $R_{12} = \{(a_1, b_1), (a_1, b_2), (a_2, b_2)\}$,

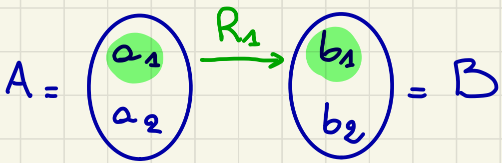
$R_{13} = \{(a_1, b_1), (a_2, b_1), (a_2, b_2)\}$, $R_{14} = \{(a_1, b_2), (a_2, b_1), (a_2, b_2)\}$,

$R_{15} = A \times B$.

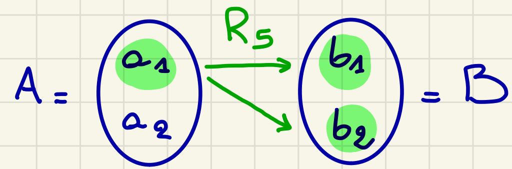
ESISTONO RELAZIONI "SPECIALI":

- funzioni
- operazioni
- relazioni di equivalenza

Funzioni (2.1)

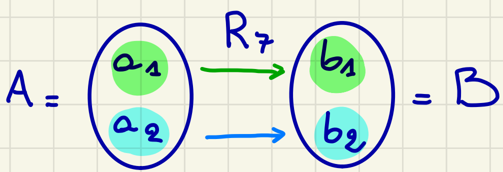


$a_1 \sim_{R_1} b_1$



$a_1 \sim_{R_5} b_1$

$a_1 \sim_{R_5} b_2$



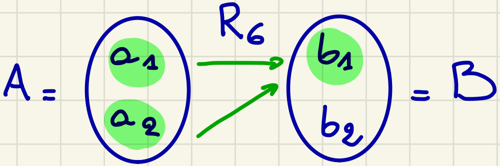
$$R_7 : A \longrightarrow B$$
$$a_1 \longmapsto b_1$$
$$a_2 \longmapsto b_2$$

$R_7(a_1) = b_1$

$R_7(a_2) = b_2$

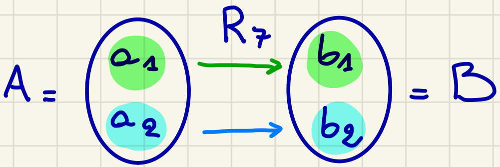
Una funzione $f : A \to B$ è una relazione che associa ad ogni elemento di A un unico elemento di B.

Notazioni:
- A è il dominio, B è il codominio di f
- se $a \in A$, $b = f(a)$ è la sua immagine
- $Im(f) =$ insieme delle immagini di f
- $f^{-1}(b) = \{ a \in A \mid f(a) = b \} =$ controimmagine di b



$$Im(R_6) = \{b_1\}$$

$$R_6^{-1}(b_1) = \{a_1, a_2\} = A \quad , \quad R_6^{-1}(b_2) = \emptyset$$



$$Im(R_7) = \{b_1, b_2\} = B$$

$$R_7^{-1}(b_1) = \{a_1\} \quad , \quad R_7^{-1}(b_2) = \{a_2\}$$

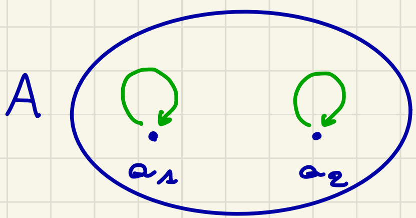
$Im(R_7) = B \implies R_7$ è suriettiva

$|R_7^{-1}(b_1)| = |R_7^{-1}(b_2)| = 1 \implies R_7$ è iniettiva

$\implies R_7$ è biunivoca

$\Delta_A = \{(a,a) \mid a \in A\}$ = insieme diagonale di $A \subseteq A \times A = A^2$

Δ_A è una relazione ed in particolare è una funzione.



$$\Delta_A = Id_A : \begin{array}{l} A \longrightarrow A \\ a \longmapsto a \end{array}$$

Funzione identità

OPERAZIONI (2.2)

Un'operazione n-aria è una funzione

$$* : A_1 \times \dots \times A_n \longrightarrow A_{n+1}$$
$$(a_1, \dots, a_n) \longmapsto *(a_1, \dots, a_n)$$

- $A_1 = \dots = A_n = A_{n+1} \Rightarrow *$ è un'operazione interna
- $n = 2 \Rightarrow *(a_1, a_2) = a_1 * a_2$ è un operazione binaria

$$+ : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N} \qquad \text{operazione binaria interna}$$
$$(n_1, n_2) \longmapsto n_1 + n_2$$

$$- : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{Z} \qquad \text{operazione binaria esterna}$$
$$(n_1, n_2) \longmapsto n_1 - n_2$$

$A = \{a_1, a_2\}$ $\quad * : A \times A \to A$

$*$	a_1	a_2
a_1	$a_1 * a_2$	$a_1 * a_2$
a_2	$a_2 * a_1$	$a_2 * a_2$

$*_1$	a_1	a_2
a_1	a_1	a_1
a_2	a_1	a_1

$*_2$	a_1	a_2
a_1	a_2	a_1
a_2	a_1	a_1

$*_3$	a_1	a_2
a_1	a_1	a_2
a_2	a_1	a_1

$*_4$	a_1	a_2
a_1	a_1	a_1
a_2	a_2	a_1

$*_5$	a_1	a_2
a_1	a_1	a_1
a_2	a_1	a_2

$*_6$	a_1	a_2
a_1	a_2	a_2
a_2	a_1	a_1

$*_7$	a_1	a_2
a_1	a_2	a_1
a_2	a_2	a_1

$*_8$	a_1	a_2
a_1	a_2	a_1
a_2	a_1	a_2

$*_9$	a_1	a_2
a_1	a_1	a_2
a_2	a_2	a_1

$*_{10}$	a_1	a_2
a_1	a_1	a_2
a_2	a_1	a_2

$*_{11}$	a_1	a_2
a_1	a_1	a_1
a_2	a_2	a_2

$*_{12}$	a_1	a_2
a_1	a_2	a_2
a_2	a_2	a_1

$*_{13}$	a_1	a_2
a_1	a_2	a_2
a_2	a_1	a_2

$*_{14}$	a_1	a_2
a_1	a_2	a_1
a_2	a_2	a_2

$*_{15}$	a_1	a_2
a_1	a_1	a_2
a_2	a_2	a_2

$*_{16}$	a_1	a_2
a_1	a_2	a_2
a_2	a_2	a_2

$(A, *_8)$ è un gruppo abeliano con $e = a_2$ ed $a_1^{-1} = a_1$.

$(A, *_9)$ è un gruppo abeliano con $e = a_1$ ed $a_2^{-1} = a_2$.

Sono lo stesso gruppo.

$(\mathbb{Z}_2, +)$: $\mathbb{Z}_2 = \{0, 1\}$,

$+$	0	1
0	0	1
1	1	0

STRUTTURA ALGEBRICA (DEFINIZIONE 2.13)

- $A_1, \dots, A_m$ insiemi (supporto della struttura);
- $*_1, \dots, *_n$ operazioni.

$(A_1, \dots, A_m, *_1, \dots, *_n)$ é detta struttura algebrica

GRUPPO $(G, *)$ (DEFINIZIONE 2.14)

Siano $a, b, c \in G$. $* : G \times G \to G$ é un' operazione interna che soddisfa tre proprietà:

i) esistenza elemento neutro e tale che $e * a = a * e = a$;

ii) esistenza inverso a^{-1} tale che $a^{-1} * a = a * a^{-1} = e$;

iii) associatività $a * (b * c) = (a * b) * c$.

Se inoltre vale $a * b = b * a$ per ogni a, b allora $(G, *)$ si dice gruppo commutativo o abeliano.

Esempi

$(\mathbb{N}, +)$: elemento neutro 0, associativo, commutativo, no inverso.

$(\mathbb{N}\setminus\{0\}, \cdot)$: elemento neutro 1, associativo, commutativo, no inverso.

$(\mathbb{Z}, +)$: gruppo abeliano, $-n$ è l'inverso di n.

$(\mathbb{Z}\setminus\{0\}, \cdot)$: elemento neutro 1, associativo, commutativo, no inverso.

$(\mathbb{Q}, +)$: gruppo abeliano.

$(\mathbb{Q}\setminus\{0\}, \cdot)$: gruppo abeliano, q/p è l'inverso di p/q.

$(\mathbb{R}, +)$, $(\mathbb{R}\setminus\{0\}, \cdot)$, $(\mathbb{C}, +)$, $(\mathbb{C}\setminus\{0\}, \cdot)$ sono gruppi abeliani.

$$(\cancel{3750} + 1125) - \cancel{3750} = (1125 + 3750) - 3750 =$$

$$= 1125 + (3750 - 3750) = 1125 + 0 = 1125$$

CAMPO $(\mathbb{K}, *, \circ)$ (DEFINIZIONE 2.19)

i) $(\mathbb{K}, \overset{+}{*})$ gruppo abeliano con elemento neutro e;

ii) dato $\mathbb{K}^* = \mathbb{K} \setminus \{e\}$, $(\mathbb{K}^*, \overset{\cdot}{\circ})$ gruppo abeliano;

iii) distributività $a \circ (b * c) = (a \circ b) * (a \circ c)$.

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

ESEMPI

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

$(\mathbb{Z}_2, +, \cdot)$

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

Campo finito

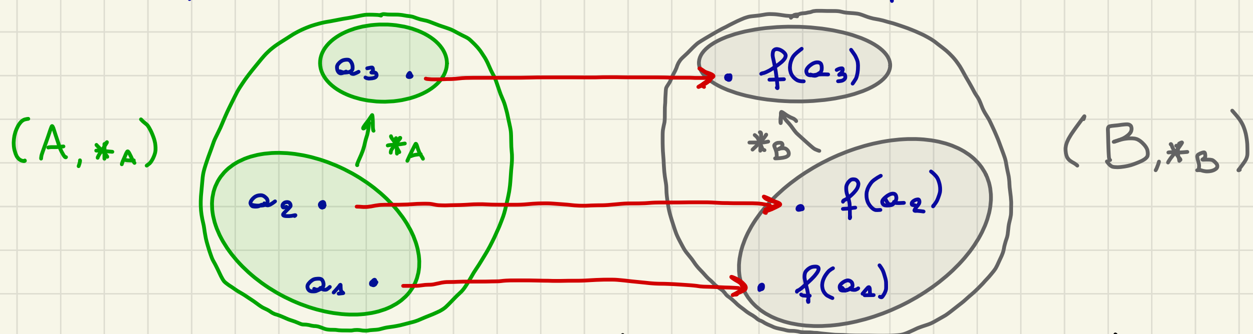
Esercizio: verificare che $\mathbb{Z}_2$ è un campo.

Omomorfismo (Definizione 2.13)

Funzione f tra due strutture algebriche che commuta con le operazioni.
Se f è invertibile con f^{-1} omomorfismo, allora f si dice isomorfismo e le strutture si dicono isomorfe.

Omomorfismo di Gruppi (Definizione 2.14)

$(A, *_A), (B, *_B)$ $\quad f: A \to B \quad f(a_1 *_A a_2) = f(a_1) *_B f(a_2)$.



Omomorfismo di Campi (Definizione 2.21)

$(A, *_A, \circ_A), (B, *_B, \circ_B)$ $\quad f: A \to B$

- $f(a_1 *_A a_2) = f(a_1) *_B f(a_2)$;
- $f(a_1 \circ_A a_2) = f(a_1) \circ_B f(a_2)$.

ESEMPI

- $f_a : \mathbb{K} \to \mathbb{K}$ $\qquad f_a(x+y) = a(x+y) = (ax) + (ay) = f_a(x) + f_a(y)$

  $\quad x \mapsto ax$ $\qquad f_a(xy) = a(xy) \neq (ax)(ay) = f_a(x) f_a(y)$

$\Rightarrow$ f_a è un isomorfismo di gruppi da $(\mathbb{K}, +)$ in $(\mathbb{K}, +)$, ma non da $(\mathbb{K}^*, \cdot)$ in $(\mathbb{K}^*, \cdot)$, a meno che $a = 0, 1$.

- f_0, detta funzione nulla, è un omomorfismo di campi;
- $f_1 = Id_{\mathbb{K}}$ è un omomorfismo di campi.

- $f : \mathbb{R} \to \mathbb{R}$ $\qquad f(x+y) = e^{x+y} = e^x e^y = f(x) f(y)$

  $\quad x \mapsto e^x$

$\Rightarrow$ f è un omomorfismo di gruppi da $(\mathbb{R}, +)$ in $(\mathbb{R}^*, \cdot)$.

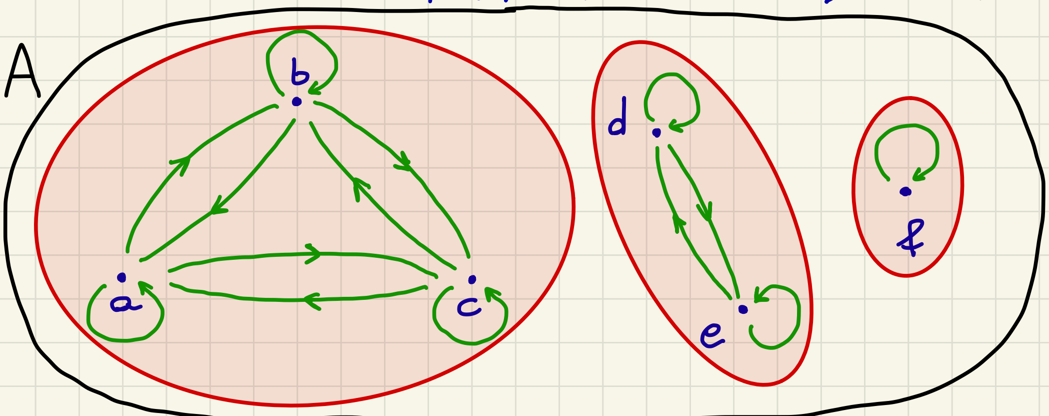
Relazioni di Equivalenza (Definizione 2.35)

$R \subseteq A \times A$ è di equivalenza se è:

i) riflessiva $(a,a) \in R$; $\quad a \sim_R a$

ii) simmetrica $(a,b) \in R \Rightarrow (b,a) \in R$; $\quad a \sim_R b \Rightarrow b \sim_R a$

iii) transitiva $(a,b),(b,c) \in R \Rightarrow (a,c) \in R$. $\quad a \sim_R b,\ b \sim_R c \Rightarrow a \sim_R c$



$[a] = [b] = [c] = \{a,b,c\}$

$[d] = [e] = \{d,e\}$

$[f] = \{f\}$

$A = [a] \cup [d] \cup [f]$

Classe di Equivalenza (Definizione 2.37)

$R \subseteq A \times A$ di equivalenza, $a \in A$.

$[a]_R = \{b \in A \mid b \sim_R a\}$ = classe di equivalenza di a.

$A = \{a_1, a_2\}$

$A \times A = \{(a_1,a_1), (a_1,a_2), (a_2,a_1), (a_2,a_2)\}$

$R_0 = \emptyset,$

$R_1 = \{(a_1,a_1)\}$, $R_2 = \{(a_1,a_2)\}$, $R_3 = \{(a_2,a_1)\}$, $R_4 = \{(a_2,a_2)\}$,

$R_5 = \{(a_1,a_1),(a_1,a_2)\}$, $R_6 = \{(a_1,a_1),(a_2,a_1)\}$, $R_7 = \{(a_1,a_1),(a_2,a_2)\}$,

$R_8 = \{(a_1,a_2),(a_2,a_1)\}$, $R_9 = \{(a_1,a_2),(a_2,a_2)\}$, $R_{10} = \{(a_2,a_1),(a_2,a_2)\}$,

$R_{11} = \{(a_1,a_1),(a_1,a_2),(a_2,a_1)\}$, $R_{12} = \{(a_1,a_1),(a_1,a_2),(a_2,a_2)\}$,

$R_{13} = \{(a_1,a_1),(a_2,a_1),(a_2,a_2)\}$, $R_{14} = \{(a_1,a_2),(a_2,a_1),(a_2,a_2)\}$,

$R_{15} = A^2$.

$R_7 = \Delta_A$ e $R_{15} = A^2$ sono le uniche relazioni di equivalenza.

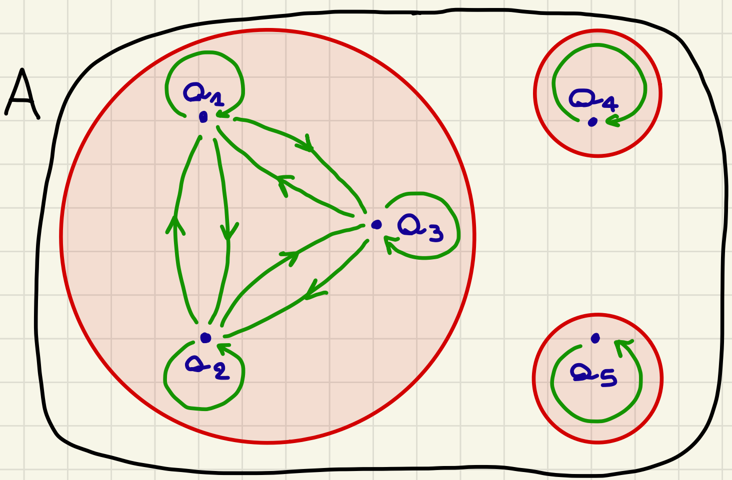
$[a_1]_{R_7} = \{a_1\}$, $[a_2]_{R_7} = \{a_2\}$, $[a_1]_{R_{15}} = \{a_1, a_2\} = [a_2]_{R_{15}}$.

TEOREMA 2.38

Ogni insieme è l'unione disgiunta delle classi di equivalenza.

INSIEME QUOZIENTE (DEFINIZIONE 2.39)

$$A/R = \{ [a]_R \mid a \in A \}.$$



$[a_1] = [a_2] = [a_3] = \{a_1, a_2, a_3\}$,

$[a_4] = \{a_4\}$, $[a_5] = \{a_5\}$.

$[a_1] \cap [a_4] = [a_1] \cap [a_5] =$

$[a_4] \cap [a_5] = \emptyset$,

$[a_1] \cup [a_4] \cup [a_5] = A$.

$$A/R = \{ [a_1], [a_4], [a_5] \}.$$