Algebra

Riccardo Cara

2023/2024

Contents

requisiti per questo corso sarà necessario avere esperienza con la teoria degli insiemi e le sue proprietà:

- intersezione
- unione
- sottoinsieme
- insieme complementare
- proprietà associativa
- proprietà distributiva
- De Morgan

1 Relazioni

Per capire le relazioni, occorre prima introdurre il prodotto cartesiano, ossia una tupla in cui ogni elemento $a \in A$ è associato ad un elemento $b \in B$ ovvero $A \times B = (a, b)|a \in A, b \in B$ ad esempio: se $A = \{1, 2, 3, 4\}$ e $B = \{a, b, c, d\}$ il prodotto cartesiano $A \times B = \{(1, a), (2, b), (3, c), (4, d)\}$. Una relazione (ρ) non è altro che il sottoinsieme del prodotto cartesiano ovvero $\rho \subseteq A \times B$, se $(a, b) \in \rho$ si scrive $a\rho b$. Se una relazione è definita su A ossia $a\rho a'|a \in A, a' \in A$ prende nome di **relazione di identità**. essendo la relazione un insieme, allora su essa valgono le proprietà degli insiemi. il dominio della relazione è:

$\mathcal{D} = a \in A|\exists b \in B|a\rho b$

l'immagine della relazione è:

$\mathcal{I} = b \in B|\exists a \in A|a\rho b$

Se $\forall a \in A$ esiste un solo $b \in B|a\rho b$ allora ρ è una funzione, ma non è detto che il suo inverso (ρ^{-1}) lo sia. ci sono 2 differenti modi di rappresentare graficamente le relazioni,

d	0	0	0	0
c	0	1	1	0
b	1	0	0	1
a	0	0	1	0
	a	b	c	d

rappresentazione tabellare diagramma 2rappresentazione con nodi e frecce.

1.1 Relazioni di equivalenza

Una relazione $\rho \in AxA$ è una *relazione di equivalenza* se:

- **riflessiva**:$a\rho a \forall a \in A$
- **simmetrica**: se $a\rho a'$ allora esiste anche $a'\rho a$
- **transitiva**: se $a\rho a'$ e $a'\rho a''$ allora $a\rho a''$

con Le relazioni di equivalenza introduciamo anche *le classi di equivalenza* scritte come $[a] = b \in A | a\rho b$ ovvero $[a]$ è l'insieme contenente tutti gli elementi in relazione con a (sono equivalenti ad a), avendo 2 classi di equivalenza $[a], [b] \in A$ se le due hanno almeno un elemento c in comune allora $[a] = [b]$ poichè, se $c \in [a]$ significa che ogni elemento in $[a]$ è per definizione equivalente a c, stessa cosa per $[b]$, quindi $[a]$ e $[b]$ sono equivalenti.
L'insieme delle classi di equivalenza in un insieme A viene detto *insieme quoziente* e viene scritto come $A/a = [a] \forall [a] \in A$.

1.2 Partizioni

le partizioni(A_α) di un insieme (A) sono collezioni **diverse** di elementi dello stesso insieme tali che l'unione di essi risulti essere tutto l'insieme ($A_\alpha \cup A_\beta = A$) immaginare un diagramma a torta o semplicemente le partizioni di un HDD. le classi di equivalenza sono partizioni di A essendo che le classi di equivalenza o sono congiunte (sono congiunte le classi $[a] = [b]$, nel diagramma a torta le classi [a]=[b] sono lo stesso spicchio) o disgiunte (spicchi diversi)

1.3 Relazioni di ordine parziale

una relazione è di ordine parziale quando è:

- **riflessiva** $a\rho a \forall a \in A$
- **antisimmetrica** dato $a\rho a'$ non si ha $a'\rho a$
- **Transitiva** se $a\rho a'$ e $a'\rho a''$ allora $a\rho a''$

un esempio di facile comprensione è la relazione tra sottoinsiemi, avendo $\mathcal{P}(X)$ ovvero un insieme composto da tutti i possibili sottoinsiemi di X parti, definiamo la relazione $A\rho B | A \subseteq B$ abbiamo tutte le condizioni rispettate, infatti per ogni sottoinsieme di $\mathcal{P}(X)$ vale $A\rho A = A \subseteq A$, vale anche la seconda condizione, ovvero se $A\rho B$ e $B\rho C$ allora $A\rho C$ poichè se $A \subseteq B$ e $B \subseteq C$ allora $A \subseteq C$, è vera anche l'ultima condizione poichè $A \subseteq B$ implica che $B \nsubseteq A$

2 insiemi e strutture algebriche

2.1 numeri naturali

introduciamo un'astrazione dei numeri naturali ovvero la terna di Peano $(\mathbb{N}, \sigma, 0)$ e segue questi assiomi:

- esiste un numero $0 \in \mathbb{N}$
- σ è una funzione $\sigma : \mathbb{N} \to \mathbb{N}$ chiamata successore
- $x \neq y$ implica $\sigma(x) \neq \sigma(y)$

- $\sigma(x) \neq 0 \forall x \in \mathbb{N}$
- se $U \subseteq \mathbb{N}$, $0 \in U$, $x \in U$ e $\sigma(x) \in U$ allora $U = \mathbb{N}$ ovvero, ogni sottoinsieme di $\mathbb{N}$ che contiene lo 0, e il successore di ogni numero nel sottoinsieme, coincide con $\mathbb{N}$

una volta definiti gli assiomi di Peano, possiamo definire delle operazioni elementari:

- **somma** definiamo la somma come un'operazione $\mathbb{N}\times\mathbb{N} \to \mathbb{N}$ ossia un'operazione che associa una oppia di elementi appartenenti all'insieme $\mathbb{N}$ ad un elemento dell'insieme $\mathbb{N}$, presi degli elementi $n, n', n'' \in \mathbb{N}$ allora $n \times n' \to n'' \equiv n + n' = n''$.

  possiamo notare nella somma che:

  - $\sigma(n) + n' = \sigma(n + n')$
  - $0 + n = n$ poichè 0 nella somma è un *elemento neutro*[1]

- **prodotto**: definiamo il prodotto come l'operazione $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$, presi gli elementi $n, n', n'' \in \mathbb{N}$ allora $n \times n' \to n'' \equiv n \cdot n' = n''$

  possiamo notare nel prodotto che:

  - $0 \cdot n = 0 \forall n \in \mathbb{N}$
  - $1 \cdot n = n$ nell'operazione prodotto, 1 è un elemento neutro
  - $\sigma(n) \cdot n' = n \cdot n' + n''$

2.2 numeri interi

Una volta definiti i numeri naturali, visti il dominio e l'immagine, notiamo che non è possibile risolvere un'equazione come $x + 1 = 0$, questo perchè il risultato non appartiene ai numeri naturali, bensì ai numeri interi $\mathbb{Z}$. È possibile definire i numeri interi partendo dai numeri naturali utilizzando l'insieme quoziente $\mathbb{Z} = \mathbb{N} \times \mathbb{N}/\sim$, definiamo con $n, m \in \mathbb{N}$ la relazione:

$$(n, m) \sim (n', m') \iff n + m' = m + n' \tag{1}$$

ora prendiamo le coppie $(a, 0), (0, a)$, $(a, 0)$ è in relazione con tutte le coppie $n, m | n - m = a$ e $(0, a)$ è in relazione con tutte le coppie $n, m | n - m = -a$, per rendere la situazione più familiare, si possono associare i numeri che vengono in mente quando si pensa all'insieme dei numeri interi, come $-\infty..., -2, -1, 0, 1, 2, ...\infty$ alle coppie di valori $(a, 0), (0, a)$. Associamo alla coppia $(a, 0)$ i valori $a \in \mathbb{Z} | a \geq 0$ e associamo alla coppia$(0, a)$ i valori $a \in \mathbb{Z} | a \leq 0$. Prima si è definito $\mathbb{Z}$ come un insieme quoziente, un insieme quoziente è l'insieme delle classi di equivalenza di un insieme e le classi di equivalenza dell'insieme che stiamo analizzando sono $[(n, m)]$. Definiamo le operazioni:

[1] *elemento neutro:* un elemento che non modifica nulla in un'operazione

- **somma**: $[(n,m)] + [(n',m')] = [(n+n', m+m')]$ ad esempio, la somma $[(0,2)] + [(5,0)] = [(5,2)] = [(3,0)] = 3$, un modo di facile e veloce di trovare la classe di equivalenza in formato $[(a,0)]$ o $[(0,a)]$ è semplicemente, sostituire il valore più piccolo della coppia (min) con 0 e sostituire il valore più grande della coppia (MAX) con $MAX - min$
- **prodotto**:$[(n,m)] \cdot [(n',m')] = [(n \cdot n' + m \cdot m', m \cdot n' + n \cdot m')]$, ad esempio, il prodotto $[(0,2)] \cdot [(5,0)] = [(0 \cdot 5 + 2 \cdot 0, 2 \cdot 5 + 0 \cdot 0)] = [(0,10)] = -10$

2.3 Divisibilità in $\mathbb{Z}$

presi 2 numeri $a, b \in \mathbb{Z}$ con $b \neq 0$esistono solo due numeri unici $q, r \in \mathbb{Z}$ tali che:

$$a = bq + r, 0 \leq r \leq |b| \tag{2}$$

diciamo che:

- $a|b$ si dice a divide b se $\exists c \in \mathbb{Z} : b = ac$
- $a|0 \forall a \in \mathbb{Z}$
- ogni $a \in \mathbb{Z}$ ha divisori $\pm 1, \pm a$
- $0|a \iff a = 0$
- $a|1 \iff a = \pm 1$
- se $a|b$ e $a|c$ allora $a|bx + cy, \forall x, \forall y$ e viceversa

2.4 MCD

siano $a, b \in \mathbb{Z}$, $d \geq 1$ si dice MCD se $d|a$ e $d|b$ per calcolare il MCD si utilizza l'algoritmo Euclideo:

1. si divide a per b, si ottengono q_1 e r_1, se $r_1 \neq 0$ si continua
2. si divide b per r_1, si ottengono q_2 e r_2, se $r_2 \neq 0$ si continua
3. si divide r_1 per r_2, si ottengono q_3 e r_3, se $r_3 \neq 0$ si continua

n. si divide r_{n-2} per r_{n-1}, si ottengono q_n e r_n, se $r_n \neq 0$ si continua

n+1. si divide r_{n-1} per r_n, si ottengono q_{n+1} e r_{n+1}, a questo punto, $r_{n+1} = 0$ e l'$MCD(a,b) = r_n$ ovvero l'ultimo $r \neq 0$

2.5 Equazioni diofantee

2.6 minimo comune multiplo

il minimo comune multiplo, indicato come mcm(a,b) è il valore $k \geq 0 : a|h, b|h$. se $a, b \neq 0$ e $a, b \notin \mathbb{Z}$ allora $|ab| = MCD(a,b) \cdot mcm(a,b)$, ne ricaviamo $mcm = \frac{|ab|}{MCD(a,b)}$

2.7 Numeri primi

i numeri primi sono numeri natruali maggiori di 1 divisibili solo da 1 e da se stessi, dato un numero naturale maggiore di 1, si scrivono tutti i sottomultipli (o divisori) $D(5) = \{1, 5\}$, $D(4) = \{1, 2, 4\}$, $D(15) = \{1, 3, 5, 15\}$, $D(13) = \{1, 13\}$ si può constatare che 5 e 13 sono numeri primi p

2.8 Teorema fondamentale dell'aritmentica

il teorema fondamentale del'aritmetica afferma che un numero $n \geq 2 \in \mathbb{N}$ è un numero primo o si può scrivere come prodotto di numeri primi. Il numero n è un numero composto dal prodotto:

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot ... \cdot p_n^{e_n}, p_n \geq 1, e_n \geq 1 \tag{3}$$

p_1, p_2, p_3 sono numeri primi diversi (2,3,5,7,9,...), ad esempio $28 = 2 * 2 * 7 = 2^2 * 7^1$

3 Strutture algebriche notevoli

enunciamo una definizione necessaria per la comprensione dei prossimi argomenti. Sia X un insieme, è possibile definire su esso un'operazione binaria $X \times X \to X$ chiamata applicazione. l'insieme $(\mathbb{Z}, +)$ è un insieme composto da numeri interi con l'operazione binaria "+" definita su esso.

3.1 Semigruppo

un semigruppo è un insieme S dotato di un'operazione binaria $*$ con le seguenti proprietà:

- $*$ è associativa, $(s * s') * s'' = s * s' * s''$
- $\exists e \in S | s * e = s = e * s \forall s \in S$, ovvero e è un elemento nullo, l'elemento nullo è unico

esiste anche il semigruppo commutativo, ovvero un semigruppo in cui oltre alle proprietà elencate, si ha che $s * s' = s' * s \forall s \in S$.

3.2 Gruppo

un gruppo è un insieme G dotato di un operazione binaria $*$ con le seguenti proprietà:

- $*$ è associativa, $(g * g') * g'' = g * g' * g''$
- $\exists e \in G | g * e = g = e * g \forall g \in G$, ovvero è un elemento nullo, l'elemento nullo è unico

- $\forall g \in G \exists g' | g * g' = e = g' * g$, ovvero per ogni elemento s, vi è il suo inverso, se moltiplicati tra loro viene restituito l'elemento nullo.

un esempio di gruppo è $(\mathbb{Z}, +)$ poichè $\forall z \in \mathbb{Z} \exists -z | z + (-z) = 0$

3.3 Anello

Un anello $(A, \odot, *)$ è un insieme avente 2 operazioni binarie aventi le seguenti proprietà:

- $(A, \odot)$ è un gruppo commutativo, l'elemento neutro è O_A
- $*$ è associativa, ossia $(a * a') * a'' = a * a' * a''$
- vale la proprietà distributiva: $(a \odot a') * a'' = (a * a'') \odot (a' * a'')$

si dice anello commutativo un anello in cui anche l'operazione $*$ è commutativa. si dice anello unitario, un anello che ha un elemento neutro anche sull'operazione $*$, ossia $\exists u \in A | a * u = a = u * a \forall a \in A$, u è un unità. Se un anello commutativo è unitario ed è privo di divisori dello zero (ovvero $a * b = O_a \Rightarrow a = O_a \vee b = O_A$) viene detto dominio di integrità, l'insieme dei numeri interi $(\mathbb{Z}, +, \cdot, 0)$ è un dominio di integrità. **proprietà**

- $\forall a \in A, a * 0 = 0$
- $a * (-a') = (-aa') = (-a) * a'$
- $(-a) * (-a') = aa'$

3.4 campo

Un campo è un Anello commutativo unitario in cui $\forall k \neq 0 \in \mathbb{K}$ ha il proprio inverso.

3.5 anello $\mathbb{Z}_n$

l'anello $\mathbb{Z}_n \equiv \mathbb{Z}/_{\sim_n}$(insieme quoziente) è l'anello commutativo unitario con divisori dello zero (quindi non è un dominio di integrità). Definiamo $\sim_n$ come la relazione

$$a \sim_n b \Leftrightarrow a - b \text{ è divisibile per } n \tag{4}$$

sappiamo quindi che essendo $\mathbb{Z}$ l'insieme quoziente è l'insieme di tutte le classi di equivalenza ovvero $\mathbb{Z}_n = \{[0], [1], ..., [n-1]\}$, su tale insieme sono definite somma e prodotto.

$$[z] + [z'] = [z + z'] \text{ e } [z] \cdot [z'] = [z \cdot z'] \tag{5}$$

si osserva che, l'anello $\mathbb{Z}_n$ e commutativo, unitario (poichè ha elemento neutro per la somma e=[0] e elemento neutro per il prodotto u=[1]) ed ha anche divisori

dello zero ovvero si infrange la regola $a \cdot b = 0 \Leftrightarrow a = 0 \vee b = 0$, poichè $[4] \cdot [3] = [12]$ e $[12] = [0]$ infatti $12 \sim_{12} 0 \Leftrightarrow 12 - 0$ è divisibile per 12, siccome 12 e 0 sono in relazione, l'insieme di equivalenza è identico, quindi $[12] = [0]$.

3.6 congruenze

Dati gli interi a, b, m si dice che a e b sono congruenti quando $a \equiv b (\text{mod } m) \Leftrightarrow \frac{a}{m} = \frac{b}{m}$ ovvero quando a e b hanno lo stesso resto se divisi per m, ad esempio $48 \equiv 3 (\text{mod } 5)$ perchè $\frac{48}{5} = 9$con resto 3 $\frac{3}{5} = 0$ con resto 3