Appunti di Algebra

Corso di Ingegneria e Scienze Informatiche - 1 anno

Mattia Ronchi

1 Introduzione

1.1 Relazioni

Una **relazione** é un sottoinsieme del prodotto cartesiano di due o piú insiemi.
Una relazione su A é un sottoinsieme di $A \times A$.

a_1 é in relazione con a_2 e si scrive $a_1 R a_2$.
Def. Una relazione é di **equivalenza** se rispetta le seguenti proprietá:

Riflessiva: $aRa \ \forall a \in A$ (ogni elemento é in relazione con se stesso)

Simmetrica: $a_1 R a_2 \implies a_2 R a_1 \ \forall a_1, a_2 \in A$

Transitiva: $a_1 R a_2 \wedge a_2 R a_3 \implies a_1 R a_3$

1.2 Funzioni/Applicazioni

$f : X \to Y$

f iniettiva: $\forall x_1, x_2 \in X, f(x_1) = f(x_2) \implies x_1 = x_2$
f suriettiva: $\forall y \in Y, \exists x \in A : y = f(x)$
f biettiva: $\forall y \in Y, \exists! x \in A : y = f(x)$

1.3 Insiemi numerici

L'insieme dei numeri razionali $\mathbb{Q}$ introduce gli inversi del prodotto (es. $3 \to \frac{1}{3}$).
L'insieme dei numeri reali $\mathbb{R}$ introduce limiti, radici e altri valori.
L'insieme dei numeri complessi $\mathbb{C}$ introduce le radici di indice pari di numeri negativi tramite l'unitá immaginaria i e i suoi multipli. Un numero complesso é esprimibile in forma polare come $a + ib$, con $a, b \in R$.

1.4 Campi

$(K, +, \cdot)$ é un campo se:

$+, \cdot$ sono associative $(a+(b+c) = (a+b)+c)$, commutative $(a+b = b+a)$ e distributive $(a(b+c) = ab+ac)$

esistono elementi **neutri** (0 per la somma ($a + 0 = a$), 1 per il prodotto ($a \cdot 1 = a$)) e **opposti** ($-a$ per la somma ($a - a = 0$), x^{-1} per il prodotto ($x \cdot x^{-1} = 1$), che restituscono il valore neutro

Alcuni insiemi campi sono $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

1.4.1 Campi finiti

Dato un numero intero $n \geq 0$, definiamo su $\mathbb{Z}$ la relazione di equivalenza

$$a \equiv b(n) \iff \exists k \in Z : a - b = k \cdot n$$

essa rispetta tutte e 3 le proprietá elencate sopra.

Definiamo $[b] = \{a \in Z : a \equiv b(n)\}$ e $Z_n = \{[0], [1], ..., [n-1]\}$.
Es. in $Z_2 = \{[0], [1]\}$, $[0]$ sono i numeri pari, $[1]$ quelli dispari.

Definiamo su Z_n le operazioni:

$$[a] + [b] = [a + b], [a] \cdot [b] = [a \cdot b]$$

Es. Possiamo scrivere, con la notazione dei campi finiti, il prodotto tra numeri interi:
Dato Z_2: $[0] \cdot [0] = [0], [0] \cdot [1] = [0 \cdot 1] = [0], [1] \cdot [1] = [1 \cdot 1] = [1]$.

Z_n é un campo $\iff$ n é **primo**. Se n non é primo, non esisterá l'inverso di un fattore di n, ovvero non esisterá nessuna classe di elementi che se moltiplicata con la classe del fattore restituisca classe 1.

1.5 Spazi vettoriali

Uno **spazio vettoriale** definito su un campo K é un insieme V con due operazioni:

$$+ : V \times V \to V \ (v_1, v_2) \to v_1 + v_2)$$

$$\cdot : K \times V \to V \ (a, v \to av)$$

che verificano le seguenti proprietá: $+$ é commutativa, associativa, con elem. neutri (vettore nullo) e opposti ($-v$), $\cdot$ é associativa, distribuitiva rispetto alla somma e con elemento neutro.

Per ogni campo K, K^n é uno spazio vettoriale su K.
$K^n = \{(x_1, x_2, ..., x_n), x_i \in K, \forall i = 1, ..., n\}$
$v = (x_1, x_2, ..., x_n), u = (y_1, y_2, ..., y_n)$
$v + u = (x_1 + y_1, x_2 + y_2, ..., x_n + y_n)$
$av = (ax_1, ax_2, ..., ax_n), a \in K$