Appunti di Algebra e Geometria

Ettore Forigo

Chapter 1

Insiemi

1.1 Cardinalità di Insiemi Finiti

$|A| = n \in \mathbb{N}$ dove n è il n° di elementi in A.

1.2 Multiinsiemi o Sistemi

Insieme con molteplicità, ovvero una collezione non ordinata di elementi con ripetizioni.

$$[a, b, c]$$

1.3 Insiemi Famosi

$\mathbb{N}$ = Numeri Naturali = $\{0, 1, 2, 3, ...\}$
$\mathbb{Z}$ = Numeri Interi
$\mathbb{Q}$ = Numeri Razionali
$\mathbb{R}$ = Numeri Reali
$\mathbb{C}$ = Numeri Complessi $\cong \mathbb{R} \times \mathbb{R} = \mathbb{R}^2$
$\mathbb{N}_0 = \mathbb{N} \setminus \{0\}$
$\mathbb{Q}^x = \mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$
$\mathbb{R}^x = \mathbb{R}^* = \mathbb{R} \setminus \{0\}$
$\mathbb{C}^x = \mathbb{C}^* = \mathbb{C} \setminus \{0\}$

1.4 Definizione di Sequenza (o Ennupla / n-upla)

Collezione ordinata di elementi.

$$(a, b, c)$$

Diciture per numeri di elementi:

2 - Paio (pair), coppia (couple) o tupla (tuple)
3 - Terna (triplet) o tripla (triple)
4 - Quaterna (quatern) o quadrupla (quadruple)

$(a, b) := \{\{a\}, \{a, b\}\}$
$(a, a) = \{\{a\}, \{a, a\}\} = \{\{a\}, \{a\}\} = \{\{a\}\}$

Alternativamente:
Sequenza di k elementi di A: $A^k = A \times (A \times (... \times A))$
k volte

Alternativamente:
$I_n = i \in \mathbb{N} : 0 < i \leq n$
Sequenza di n elementi di $A = a : I_n \to A$ (funzione di accesso)

Chapter 2

Relazioni

2.1 Definizione di Relazione

Si dice che $R \subseteq A \times B$ è una relazione (binaria, anche detta corrispondenza) tra due insiemi A e B.

Se:
$C = \{(a_1, b_1), (a_2, b_2)\}$

Si scrive:
$b_1 = C(a_1)$
$b_2 = C(a_2)$

2.1.1 Proprietà delle Relazioni

Totalità a Sinistra

Una relazione R tra A e B si dice **ovunque definita** (o totale a sinistra, duale della totalità a destra (suriettività)) se:

$$\forall x \in A. \exists y \in B : (x, y) \in R$$

Funzionalità

Una relazione R tra A e B si dice **funzionale** (duale dell'iniettività) se:

$$\forall x \in A. \exists y \in B : (x, y) \in R \implies \exists! y \in B : (x, y) \in R$$

Chapter 3

Funzioni

3.1 Definizione di Funzione

Una relazione f si dice funzione se è funzionale e ovunque definita.

"Funzione" si riferisce alla terna: associazione di elementi, dominio e codominio, non solo all'associazione di elementi. Specificare solo un'associazione non definisce una funzione: occorre specificare anche dominio e codominio. Infatti, due funzioni che hanno una "stessa" associazione di elementi ma diverso dominio e/o diverso codominio sono funzioni diverse.

Si scrive:
$f : A \to B$
dove A è il dominio di f e B è il codominio di f.

3.2 Proprietà delle Funzioni

3.2.1 Iniettività

Una funzione da A a B si dice **iniettiva** (injective) (duale della funzionalità) se:

$$\forall x, x' \in A.\, f(x) = f(x') \implies x = x'$$

3.2.2 Suriettività

Una funzione da A a B si dice **suriettiva** (surjective) (o totale a destra, duale della totalità a sinistra) se:

$$\forall y \in B.\, \exists x \in A : y = f(x)$$

(equivalentemente: $im(f) = codom(f)$)

3.2.3 Biiettività

Una funzione si dice **biiettiva** (bijective) (o biiezione, o anche corrispondenza 1 a 1 o biunivoca) se è sia iniettiva che suriettiva.

Osservazione:

$$f : A \to B \text{ è biiettiva } \implies |A| = |B|$$

A e B possono essere infiniti.

$|X| < |Y| \iff \exists$ una funzione iniettiva $X \to Y \wedge \nexists$ una biiezione $X \to Y$.

3.3 Definizione di Immagine

L'insieme di tutti i valori di $f : A \to B$ valutata in ogni elemento di un insieme $S \subseteq A$ si dice l'immagine di S tramite f:

$$f[S] = f(S) := \{f(s) \in B : s \in S \subseteq A\} \subseteq B$$

$$\mathrm{Im} f = im(f) = f[A]$$

L'immagine del dominio di una funzione f tramite f si dice immagine di f.

Il valore di $f : A \to B$ valutata in $x \in A$ si dice immagine di x tramite f.

$im(f) \subseteq codom(f)$

3.4 Definizione di Controimmagine

L'insieme degli elementi del dominio di una funzione $f : A \to B$ che f associa a tutti gli elementi di S si dice controimmagine, preimmagine o immagine inversa di S tramite f:

$$f^{-1}[S] = f^{-1}(S) := \{x \in A : f(x) \in S \subseteq B\} \subseteq A$$

3.5 Definizione di Restrizione

Detta anche restrizione del dominio o restrizione a sinistra.

$f : A \to B, X \subseteq A$

Si dice restrizione di f ad X la funzione:

$$f_X : X \to B$$
$$f_X(x) = f(x) \; \forall x \in X$$

O equivalentemente:

$$f_X : X \to B = \{(a,b) \in f : a \in X\}$$

O ancora:

$$f_X : X \to B = f \circ i$$

Dove $i : X \to A$ è l'inclusione di X in A data da $i(a) = a$.

3.6 Definizione di Troncatura

Detta anche corestrizione, restrizione del codominio o restrizione a destra.

Data $f : A \to B \wedge Im(f) \subseteq Y$, si dice **troncatura** di f ad Y la funzione:

$$f^Y : A \to Y = \{(a,y) \in A \times Y : y = f(a)\}$$

Osservazione:
Il codominio viene ristretto.

In generale prima si restringe e poi si tronca una funzione.

3.7 Composizione

L'elemento b che compone in $(g \circ f)$ è unico $\forall a \in A$.

3.8 Definizione di Funzione Inversa Destra

$f : A \to B$ ammette inversa destra $g : B \to A \mid (f \circ g) : B \to B$, $\forall x \in B.\, (f \circ g)(x) = x \iff f$ è suriettiva.

3.9 Definizione di Funzione Inversa Sinistra

$f : A \to B$ ammette inversa sinistra $g : B \to A \mid (g \circ f) : A \to A$, $\forall x \in A.\, (g \circ f)(x) = x \iff f$ è iniettiva.

3.10 Definizione di Funzione Inversa

$f : A \to B$ ammette inversa destra e sinistra $\implies$ f ammette inversa f^{-1} che coincide con l'inversa dentra e sinistra.

f ammette inversa $\iff$ f è biettiva.

3.11 Definizione di Successione

Una funzione f si dice successione se:

$$f : \mathbb{N} \to A$$

Chapter 4

Strutture Algebriche

4.1 Definizione di Operazione Binaria

Sia U un insieme. Si dice **operazione binaria** una funzione $o : U \times U \to U$.

4.2 Definizione di Struttura Algebrica

Una **struttura algebrica** è una collezione, in particolare una ennupla, data da un insieme ed una o più operazioni su di esso:

$$(U, o)$$

4.3 Definizione di Associatività

Si dice che $*$ è associativa se $\forall a, b, c \in A.\, a * (b * c) = (a * b) * c$.

4.4 Definizione di Elemento Neutro

Sia $(A, *)$ un insieme con una operazione binaria (magma):

$$* : A \times A \to A$$
$$(a, b) = a * b$$

Si dice che $e \in A$ è un **elemento neutro** per $*$ se:

$$\forall a \in A.\, e * a = a * e = a$$

4.5 Definizione di Elemento Inverso, Inverso Destro e Inverso Sinistro

Se $(X, *)$ ammette elemento neutro e si dice che $\forall x \in X$:

x' è inverso destro di x se $\exists x' \in X : x * x' = e$
x'' è inverso sinistro di x se $\exists x'' \in X : x'' * x = e$
x''' è inverso di x se x''' è inverso destro di $x \wedge x'''$ è inverso sinistro x.

4.6 Definizione di Commutatività

Si dice che $*$ è commutativa se $\forall a, b \in A. \, a * b = b * a$.

4.7 Definizione di Monoide (Monoid)

$(A, *)$ (magma) è detto **monoide** se $*$ è associativa (semigruppo) e ammette elemento neutro.

4.8 Definizione di Gruppo (Group)

$(A, *)$ è detto **gruppo** se è un monoide e ogni elemento di A ammette inverso (necessariamente unico, destro e sinistro, solitamente indicato con a^{-1}).

4.8.1 Sottogruppo

Un sottoinsieme di un gruppo è un sottogruppo se è a sua volta un gruppo con la stessa operazione

4.8.2 Esempi notevoli

$GL_n(\mathbb{K}) = \{M \in \mathbb{K}_{m,n} : det(M) \neq 0\}$, chiamato gruppo lineare generale (general linear group) (o gruppo di matrici), è un gruppo rispetto al prodotto di matrici (righe per colonne).

Esiste anche un suo sottogruppo, $SL_n(\mathbb{K})$, detto gruppo lineare speciale (special linear group), formato dalle matrici con determinante uguale a 1.

4.9 Definizione di Gruppo Abeliano (Abelian Group)

$(A, *)$ è detto **gruppo abeliano** o commutativo se oltre ad essere un gruppo, $*$ è commutativa.

4.10 Definizione di Sottrazione

La sottrazione è definita come somma con l'opposto di un elemento in $(\mathbb{Z}, +)$.

$a - b = a + (-b)$

4.11 Definizione di Gruppo Simmetrico

$S(\Omega) = \{f : \Omega \to \Omega \mid \text{f è biiettiva}\}$ è chiamato gruppo simmetrico (Symmetric Group) dell'insieme Ω.

È un gruppo rispetto alla composizione di funzioni.
Contiene tutte le possibili permutazioni degli elementi di Ω.
Tutti i gruppi simmetrici di insiemi aventi la stessa cardinalità sono isomorfi.
L'elemento neutro è la funzione *id*.

4.11.1 Gruppi Simmetrici Finiti (Finite Symmetric Group)

Se Ω è finito, il suo gruppo simmetrico si denota con S_n.
In genere in questi casi si preferisce considerare il gruppo delle permutazioni degli interi $1..n$ dato che è isomorfo.

4.12 Definizione di Anello Unitario (o con Unità) (Ring)

Un insieme A dotato di due operazioni binarie $\tilde{+}$ e $\tilde{\cdot}$ è un anello $(A, \tilde{+}, \tilde{\cdot})$ se:

$(A, \tilde{+})$ è un gruppo abelliano.
$(A, \tilde{\cdot})$ è un monoide.
$\tilde{\cdot}$ è distributiva rispetto a $\tilde{+}$.

4.12.1 Definizione di Anello (Rng)

Il requisito di monoide per $(A, \cdot)$ è rilassato a semigruppo.

4.12.2 Definizione di Anello Commutativo (Commutative Ring)

Se $\tilde{\cdot}$ è commutativa l'anello si dice commutativo.

4.13 Definizione di Corpo (Division Ring)

$(A, \tilde{+}, \tilde{\cdot})$ è un anello e $(A^*, \tilde{\cdot})$ è un gruppo, dove $A^* := A \setminus \{0\}$.

4.14 Definizione di Campo (Field)

Un campo (o corpo commutativo) $(\mathbb{K}, +, \cdot)$ è un anello commutativo unitario in cui $(\mathbb{K}^*, \cdot)$ è un gruppo abelliano, dove $\mathbb{K}^* := \mathbb{K} \setminus \{0\}$.

Alternativamente:

$(\mathbb{K}, +)$ è un gruppo abelliano con elemento neutro 0
$(\mathbb{K}^*, \cdot)$ è un gruppo abelliano con elemento neutro 1
$\cdot$ è distributiva rispetto a $+$.

4.15 Definizione di Spazio Vettoriale

$(V, \oplus, *)$ è detto spazio vettoriale (vector space) su di un campo $(\mathbb{K}, +, \cdot)$ se:

V è dotato di una operazione interna $\oplus : V \times V \to V$ detta (somma o legge di composizione interna)

V è dotato di una operazione esterna $* : \mathbb{K} \times V \to V$ (detta prodotto per scalare (gli elementi di $\mathbb{K}$ sono detti scalari) o legge di composizione esterna)

$(V, \oplus)$ è un gruppo abelliano

$*$ è distributiva rispetto a $\oplus$ (distributività a destra)

$*$ è distributiva rispetto a $+ : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ (distributività a sinistra, insieme alla precedente **pseudo-distributività**)

$*$ è **pseudo-associativa**:
$\forall a, b \in \mathbb{K}, \mathbf{v} \in V. \, (a \cdot b) * \mathbf{v} = a * (b * \mathbf{v})$

$*$ ammette elemento neutro sinistro $\in \mathbb{K}$ (**unitarietà**)

Notazione:
$\mathbb{K}(V)$

Un campo $\mathbb{K}$ è spazio vettoriale su se stesso con:
$* = \cdot$
$\oplus = +$

Curiosità:
Le ultime quattro proprietà dicono che il prodotto per scalare definisce un

omomorfismo tra l'anello del campo $\mathbb{K}$ $((\mathbb{K}, +, \cdot))$ e l'anello degli endomorfismi del gruppo $(V, \oplus)$.

4.15.1 Interpretazione Geometrica

Gli elementi di V sono vettori geometrici, cioè freccie orientate.
La somma di vettori è definita con la regola del parallelogramma.
Ogni vettore ammette inverso.
Il prodotto per scalare è un vettore con la stessa direzione di quello originale ma con lunghezza moltiplicata per lo scalare e verso in base al segno.

Chapter 5

Matrici

5.1 Matrici

Matrice $m \times n$ (righe $\times$ colonne) a coefficienti in $\mathbb{K}$:
$Mat_{m,n}(\mathbb{K}) = \mathbb{K}^{m,n} = \mathbb{K}_{m,n}$

Elementi $a_{i,j}$

$m \neq n \rightarrow$ matrice rettangolare
$m = n \rightarrow$ matrice quadrata

$A \in Mat_{m,n}(\mathbb{K})$

$\backslash$ = diagonale principale
$/$ = diagonale secondaria

5.2 Matrici quadrate particolari

5.2.1 Triangolare superiore

$a_{i,j} = 0 \ \forall i > j$

$$\begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix}$$

5.2.2 Triangolare inferiore

$a_{i,j} = 0 \ \forall j > i$

$$\begin{pmatrix} a & 0 & 0 \\ b & c & 0 \\ d & e & f \end{pmatrix}$$

5.2.3 Diagonale

$a_{i,j} = 0 \ \forall i > j$

$$\begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix}$$

5.2.4 Scalare (Diagonale)

con $a_{i,i} = k \in \mathbb{K}$

$$\begin{pmatrix} a & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & a \end{pmatrix}$$

5.2.5 Identica (o Identità) di ordine n (Scalare con $k = 1$)

$a_{i,i} = 1$

I_n

$$I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

5.2.6 Nulla $\underline{0}$

$a_{i,j} = 0 \ \forall i, j$

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

5.3 Matrice Trasposta

$A \in Mat_{m,n}(\mathbb{K})$

Matrice trasposta di A:
A^T

Righe e colonne scambiate.
$a_{i,j} = aj, i$

$A = (A^T)^T$

$A = A^T \implies A$ è simmetrica, A è quadrata

5.4 Somma tra matrici

Somma elemento per elemento (per matrici di dimensioni uguali)

$(Mat_{m,n}(\mathbb{K}), +)$ è un gruppo abeliano.

5.5 Prodotto per scalare

5.5.1 Proprietà

Distributivo rispetto all'addizione

5.6 Prodotto righe per colonne

5.6.1 Proprietà

Non commutativo
Associativo
Distributivo rispetto alla somma

$A \cdot B = \underline{0} \not\Longrightarrow A = \underline{0} \vee B = \underline{0}$

$(A \cdot B)^T = B^T \cdot A^T$

Se:

$$A \cdot X = B$$

dato che la divisione tra matrici non è definita, **non si scrive:**

$$X = B/A$$
$$X = \frac{B}{A}$$

ma:

$$X = A^{-1} \cdot B$$

5.7 Calcolo del determinante

Solo per matrici quadrate.

$|A|$

$det(A)$

5.7.1 2×2

Differenza prodotto diagonali

5.7.2 3×3 (Sarrus)

Differenza (somme prodotti diagonali e prodotti sovradiagonali).

Se A è triangolare superiore il determinante è il prodotto della diagonale

5.7.3 Regola di Laplace

$A \in Mat_n(\mathbb{K})$, $n \geq 2$

$|A| = \sum\limits_{j=1}^{n} (-1)^{i+j} a_{i,j} \cdot |A_{i,j}|$

Dove $A_{i,j}$ è la matrice ottenuta da A togliendo ad A la i-esima riga e la j-esima colonna.

Il valore $(-1)^{i+j}\,|A_{i,j}|$ è detto complemento algebrico di $a_{i,j}$.

Osservazione:
Il termine $(-1)^{i+j}$ indica che se la somma degli indici di riga e colonna è dispari, il segno nella somma va cambiato, altrimenti va mantenuto.
Osservazione:
Si può applicare Laplace per righe / colonne qualsiasi, ma per snellire i conti conviene scegliere righe / colonne con il maggior n° di 0.

5.7.4 Proprietà dei Determinanti

$|I_n| = 1$

$|A| = \prod_{i=1}^{n} a_{i,i}$

Quando A è triangolare / diagonale (anche rispetto alla diagonale secondaria, anche se in quel caso non si chiama triangolare / diagonale)

$|A| = |A^T|$

$|A \cdot B| = |A| \cdot |B|$

Osservazione:
In generale non vale per la somma.

Se in A c'è una riga / colonna nulla, allora $|A| = 0$

Scambiando righe e colonne il determinante cambia di segno.

Se una riga / colonna è combinazione lineare di altre righe / colonne, allora $|A| = 0$ e viceversa.

5.7.5 Definizione di Combinazione Lineare

Quando una riga / colonna si può scrivere utilizzando le altre righe / colonne combinate solo con operazioni di somma / prodotto e/o prodotto per scalare.

Osservazione:
Se una riga / colonna è multipla di un'altra riga / colonna allora è una sua combinazione lineare.

Sommando a una riga / colonna una combinazione lineare delle altre righe / colonne il determinante non cambia.

5.8 Definizione di Matrice Singolare

Una matrice quadrata si dice non singolare se il suo deteminante è $\neq 0$. Altrimenti si dice singolare.

5.9 Definizione di Matrice Inversa

Si dice inversa di A, se $\exists$, la matrice A^{-1} tale che:

$A \cdot A^{-1} = A^{-1} \cdot A = I_n$

Osservazione:
Sia $A \in Mat_n(\mathbb{K})$, $\exists A^{-1} \iff |A| \neq 0$

Cioè A ammette inversa se e solo se A è non singolare.

5.9.1 Calcolo della Matrice Inversa (Metodo del Complemento Algebrico)

Data $A = (a_{i,j}) \in Mat_n(\mathbb{K})$ si dice aggiunta di A la matrice $A_a \in Mat_n(\mathbb{K})$ ottenuta sostituendo in A ogni elemento col suo complemento algebrico (c).

$c_{i,j} = (-1)^{i+j} \, |A_{i,j}|$

$|A| \neq 0 \implies A^{-1} = \frac{1}{|A|} \cdot A_a^T$

5.10 Rango (Rank)

5.10.1 Definizione di Minore di Ordine p

Data una matrice $A \in Mat_{m,n}(\mathbb{K})$ si dice minore di ordine p una matrice quadrata di ordine p ottenuta da A sopprimendo $n-p$ colonne e $m-p$ righe.

5.10.2 Definizione di Rango

Data una matrice $A \in Mat_{m,n}(\mathbb{K})$ dire che il rango di A è p:

$rg(A) = p$
$r(A) = p$
$\rho(A) = p$

con $p \leq min(m, n)$

significa dire che A ha un minore non singolare di ordine p, e che ogni eventuale minore di ordine $p + 1$ è singolare.
$r(A) = 0 \iff A = \underline{0}$

Se $A \in Mat_n(\mathbb{K})$ allora $r(A) = n \iff |A| \neq 0$

A ha rango massimo $= A \in Mat_n(\mathbb{K})$, $r(A) = n$

$1 \leq rg(A) \leq min(m, n)$, $A \in Mat_{m,n}(\mathbb{K})$, $A \neq \underline{0}$

5.10.3 Teorema degli Orlati (Teorema di Kronecker)

$A \in Mat_{m,n}(\mathbb{K})$.
Il rango di A è $p \iff \exists$ in A un minore di ordine p (M_p) non singolare $\wedge$ ogni minore di ordine $p + 1$ che contiene completamente M_p è singolare.

5.10.4 Definizione di Contiene Completamente

Che ha al suo interno.