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

Una sequenza (o ennupla / n-upla) è una 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)

$(a,b) \coloneqq \{\{a\},\{a,b\}\}$
$(a,a) = \{\{a\},\{a,a\}\} = \{\{a\},\{a\}\} = \{\{a\}\}$
$(a,...,y,z) = (a,(...,(y,z)))$

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

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

O anche:
$a_1 C b_1 \ a_2 C b_2$

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 associa ad ogni elemento di A almeno un elemento di B.

In simboli:

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

Funzionalità

Una relazione R tra A e B si dice **funzionale** (o univalente / unica a destra, duale dell'iniettività) se ogni elemento di A in R è associato ad un solo elemento di B.

In simboli:

$$\forall x \in A, y, z \in B.\, xRy \land xRz \implies y = z$$

Oppure:

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

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 f si dice **iniettiva** (injective) (duale della funzionalità) se non associa a due qualsiasi elementi distinti del dominio lo stesso elemento del codominio.

In simboli:

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

3.2.2 Suriettività

Una funzione f si dice **suriettiva** (surjective) (o totale a destra, duale della totalità a sinistra) se associa un elemento del dominio ad ogni elemento del codominio.

In simboli:

$$\forall y \in codom(f).\, \exists x \in dom(f) : y = f(x)$$

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

3.2.3 Biiettività

Una funzione f si dice **biiettiva** (bijective) (o biiezione, o anche corrispondenza 1 a 1 o biunivoca) se è sia iniettiva che suriettiva, cioè ad ogni elemento del dominio corrisponde uno ed un solo elemento del codominio.

In simboli:

$$\forall x, x' \in dom(f).\, x \neq x' \implies f(x) \neq f(x')$$
$$\forall y \in codom(f).\, \exists x \in dom(f) : y = f(x)$$

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 $S \subseteq A$ si dice l'immagine di S tramite f:

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

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

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 $S \subseteq B$ si dice controimmagine, preimmagine o immagine inversa di S tramite f:

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

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:

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

O equivalentemente:

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

O ancora:

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

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

Una notazione equivalente è:

$$f|_X = f_X$$

3.6 Definizione di Troncatura

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

$f : A \to B$, $Im(f) \subseteq Y$

Si dice **troncatura** di f ad Y la funzione:

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

Osservazione:
Il codominio viene ristretto.

Una notazione equivalente è:

$$f|^Y = f^Y$$

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

3.7 Composizione

$f : A \to B$, $g : B \to C$
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

Si dice **operazione binaria** (binary operation) una funzione $o : A \times B \to C$

4.1.1 Definizione di Operazione Binaria Interna

Si dice **operazione binaria interna** (o chiusa) (internal/closed binary operation) su di un insieme U una funzione $o : U \times U \to U$

4.1.2 Definizione di Operazione Binaria Esterna

Si dice **operazione binaria esterna** (external binary operation) una operazione binaria $o : B \times A \to A$

4.2 Definizione di Struttura Algebrica

Una **struttura algebrica** (algebraic structure) consiste in un insieme, una collezione (non vuota) di operazioni su di esso e un insieme finito di identità o proprietà, dette assiomi, che le operazioni devono soddisfare.

Si rappresenta con una ennupla contenente l'insieme e le operazioni:

(U, o)

4.3 Definizione di Magma

Un **magma** o gruppoide (grupoid) (struttura algebrica) $(A, *)$ è un insieme dotato di un'operazione binaria **interna**.

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

4.4 Definizione di Elemento Neutro

Se $(A, *)$ è un magma, si dice che $e \in A$ è un **elemento neutro** (identity element) per $*$ se è sia elemento neutro destro che elemento neutro sinistro per $*$, ovvero se operando e sia a destra che a sinistra con qualsiasi elemento di A si ottiene di nuovo il medesimo elemento.

In simboli:
$\forall a \in A. \, e * a = a * e = a$

4.4.1 Elemento Neutro Destro e Sinistro

Elemento Neutro Destro

Se $*$ è una operazione binaria $A \times B \to A$, si dice che $e \in B$ è un **elemento neutro destro** per $*$ se:

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

Elemento Neutro Sinistro

Se $*$ è una operazione binaria esterna $B \times A \to A$, si dice che $e \in B$ è un **elemento neutro sinistro** per $*$ se:

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

4.5 Definizione di Magma Unitario

Un magma $(A, *)$ è un **magma unitario** (unital magma) (struttura algebrica) se $*$ ammette elemento neutro.

4.6 Definizione di Associatività

Se $(A, *)$ è un magma si dice che $*$ è **associativa** se, quando l'operazione è usata in notazione infissa, spostando le parentesi (cambiando l'ordine di svolgimento delle operazioni, n.b. non l'ordine degli operandi) il risultato non cambia. Questo significa che le parentesi si possono aggiungere, rimuovere o spostare senza cambiare il significato dell'espressione e senza ambiguità.

In simboli:

$$\forall a, b, c \in A.\, a * (b * c) = (a * b) * c$$

4.7 Definizione di Semigruppo

Un magma $(A, *)$ è detto **semigruppo** (semigroup) (struttura algebrica) se $*$ è associativa.

4.8 Definizione di Monoide

Un semigruppo $(A, *)$ è detto **monoide** (monoid) (struttura algebrica) se $*$ ammette elemento neutro.

4.9 Definizione di Elemento Inverso

Sia $(A, *)$ un magma unitario con elemento neutro e.
Si dice che $\forall a \in A$:

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

4.10 Definizione di Gruppo

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

4.10.1 Sottogruppo

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

In generale un sottoinsieme di un insieme con una struttura algebrica è sua sottostruttura se anch'esso ha la medesima struttura algebrica.

4.10.2 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.

4.11 Definizione di Sottrazione

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

$$a - b \coloneqq a + (-b)$$

4.12 Definizione di Gruppo Simmetrico

$S(\Omega) = \{f : \Omega \to \Omega \mid \text{f è biiettiva}\}$ è chiamato **gruppo simmetrico** (symmetric group) (struttura algebrica) 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 (isomorphic).
L'elemento neutro è la funzione id ($id(x) \coloneqq x$).

4.12.1 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.

4.13 Definizione di Commutatività

Se $(A, *)$ è un magma si dice che $*$ è **commutativa** se scambiando l'ordine degli operandi il risultato non cambia.

In simboli:

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

4.14 Definizione di Gruppo Abeliano

Un gruppo $(A, *)$ è detto **abeliano** (abelian) (struttura algebrica) o commutativo se $*$ è commutativa.

4.15 Definizione di Distributività

Se $(A, *)$ e $(A, +)$ sono magmi, si dice che $*$ è distributiva rispetto a $+$ se è distributiva a destra e a sinistra rispetto a $+$.

Se $*$ è commutativa, distributività, distributività a destra e distributività a sinistra sono equivalenti.

4.15.1 Distributività a Destra

Una operazione binaria esterna $* : A \times B \to B$ si dice **distributiva a destra** rispetto all'operazione $+ : B \times B \to B$ di un magma $(A, +)$ se:

$$\forall a \in A, b, c \in B.\, a * (b + c) = (a * b) + (a * c)$$

4.15.2 Distributività a Sinistra

Una operazione binaria $* : A \times C \to A$ si dice **distributiva a sinistra** rispetto all'operazione $+ : A \times A \to A$ di un magma (A, +) se:

$$\forall a, b \in A, c \in C.\, (a + b) * c = (a * c) + (b * c)$$

4.16 Definizione di Anello

Un insieme A dotato di due operazioni binarie interne $\tilde{+}$ e $\tilde{\cdot}$ è un **anello** (rng/non-unital ring) (struttura algebrica) $(A, \tilde{+}, \tilde{\cdot})$ se:

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

4.16.1 Definizione di Anello Unitario

Un anello $(A, \tilde{+}, \tilde{\cdot})$ è un **anello unitario** (ring) (o con unità) (struttura algebrica) se $(A, \tilde{\cdot})$ è anche un monoide ($\tilde{\cdot}$ ammette elemento neutro).

4.16.2 Definizione di Anello Commutativo

Se $\tilde{\cdot}$ è commutativa l'anello si dice commutativo (commutative) (struttura algebrica).

4.17 Definizione di Corpo

Se $(A, \tilde{+}, \tilde{\cdot})$ è un anello e $(A^*, \tilde{\cdot})$ è un gruppo, dove $A^* \coloneqq A \setminus \{0\}$ e 0 è l'elemento neutro di $\tilde{+}$, allora $(A, \tilde{+}, \tilde{\cdot})$ è anche un corpo (division ring) (struttura algebrica).

4.18 Definizione di Campo

Un campo (field) (o corpo commutativo) $(\mathbb{K}, +, \cdot)$ è un anello unitario commutativo, con 0 elemento neutro di + e 1 elemento neutro di $\cdot$, in cui $0 \neq 1$ e $(\mathbb{K}^*, \cdot)$ è un gruppo abelliano, dove $\mathbb{K}^* := \mathbb{K} \setminus \{0\}$ (aggiunge il requisito di invertibilità di ogni elemento $\neq 0$ per la moltiplicazione).

Alternativamente:

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

4.18.1 Esempi notevoli

$(\mathbb{F}, \dot\vee, \wedge)$, $\mathbb{F} := \{0, 1\}$, $\dot\vee := XOR$, $\wedge := AND$
$(\mathbb{Q}, +, \cdot)$
$(\mathbb{R}, +, \cdot)$
$(\mathbb{C}, +, \cdot)$

4.19 Definizione di Spazio Vettoriale

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

$(V, \oplus)$ è un gruppo abelliano ($\oplus$ è detta somma (di vettori) o legge di composizione interna)

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

$*$ è **pseudo-associativa** (o compatibile con la moltiplicazione nel campo):
$\forall a, b \in \mathbb{K}, \bar{v} \in V. \, (a \cdot b) * \bar{v} = a * (b * \bar{v})$

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

$*$ è distributiva a destra rispetto a $\oplus$

$*$ è pseudo-distributiva a sinistra rispetto a $+$ (o compatibile con l'addizione nel campo, insieme alla precedente **pseudo-distributività**):

$\forall a, b \in \mathbb{K}, \bar{v} \in V. \, (a + b) * \bar{v} = (a * \bar{v}) \oplus (b * \bar{v})$

Curiosità:
Le ultime quattro proprietà (assiomi) dicono che il prodotto per scalare definisce un omomorfismo (trasformazione che preserva la struttura algebrica) (homomorphism, structure preserving map) tra l'anello del campo $\mathbb{K}$ ($(\mathbb{K}, +, \cdot)$) e l'anello degli endomorfismi (endomorphism ring) (morfismi da un oggetto a se stesso) del gruppo $(V, \oplus)$.

Notazione:

$V(\mathbb{K})$

L'elemento neutro della somma di vettori, il vettore nullo, è scritto $\underline{0}$.

Un campo $\mathbb{K}$ è spazio vettoriale su se stesso con:

$* := \cdot$

$\oplus := +$

$\mathbb{K}^n$ è dotato di struttura di spazio vettoriale su $\mathbb{K}$ rispetto a $\oplus$ e $*$ definiti componente per componente. $(\mathbb{K}^n, \oplus)$ è gruppo abelliano.

Tutti gli spazi vettoriali di dimensione uguale sono isomorfi.

4.19.1 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.

4.20 Definizione di Combinazione Lineare

$V(\mathbb{K})$ spazio vettoriale, $\bar{v}_1 ... \bar{v}_n \in V$

Si dice cominazione lineare dei vettori $\bar{v}_1 ... \bar{v}_n$ (necessariamente in numero finito) mediante gli scalari $\alpha_1 ... \alpha_n$ il vettore:

$$\bar{v} = \alpha_1 \bar{v}_1 + \alpha_2 \bar{v}_2 + ... + \alpha_n \bar{v}_n = \sum_{i}^{n \in \mathbb{N}} \alpha_i \bar{v}_i$$

4.21 Definizione di Sottospazio Vettoriale

$S \subseteq V$ è sottospazio vettoriale (linear subspace) (struttura algebrica) di $V(\mathbb{K})$ se:

S è dotato dell'operazione binaria interna di somma di $(V, +)$ ristretta ad $S \times S$ e troncata ad S ($Im(+_{S\times S}) \subseteq S$)

S è dotato dell'operazione binaria interna di prodotto per scalare di $V(\mathbb{K})$ ristretta a $\mathbb{K} \times S$ e troncata ad S ($Im(*_{\mathbb{K}\times S}) \subseteq S$)

$(S, +|^S_{S\times S}, *|^S_{\mathbb{K}\times S})$ è uno spazio vettoriale su $\mathbb{K}$

Se $S \subseteq V$ gli assiomi degli spazi vettoriali sono già verificati (devono valere per tutti gli elementi in V).
Dunque ciò a cui va fatta attenzione sono la presenza del vettore nullo ($\underline{0}$) in S e le proprietà di chiusura della somma di vettori e del prodotto per scalare.

Notazione:
$S \leq V(\mathbb{K})$ si legge come S è sottospazio vettoriale di $V(\mathbb{K})$

4.21.1 Albero decisionale

Se $V(\mathbb{K})$ è spazio vettoriale con operazioni $+$ e $*$, per determinare se $S \subseteq V$ è sottospazio vettoriale di V si può usare il seguente albero decisionale:

Le operazioni $+$ e $*$ di S sono diverse da quelle di V? $\rightarrow$ Non è sottospazio

$\underline{0}$ (vettore nullo) $\notin S$? $\rightarrow$ Non è sottospazio

$\neg(\forall \alpha \in \mathbb{K}, \bar{v} \in S.\, \alpha * \bar{v} \in S) \rightarrow$ Non è sottospazio

$\neg(\forall \bar{u}, \bar{v} \in S.\, \bar{u} + \bar{v} \in S) \rightarrow$ Non è sottospazio

È sottospazio

4.21.2 Teorema

S è sottospazio vettoriale di $V(\mathbb{K}) \iff S$ è chiuso rispetto alle combinazioni lineari

Ovvero:
$\forall \alpha, \beta \in \mathbb{K}, \bar{v}, \overline{w} \in S.\, \alpha\bar{v} + \beta\overline{w} \in S$

4.22 Definizione di Insieme di Generatori

Se $V(\mathbb{K})$ è uno spazio vettoriale, e $X \subseteq V(\mathbb{K})$ un insieme/sequenza/sistema di vettori di $V(\mathbb{K})$, si dice che $V(\mathbb{K})$ è **generato** da X se ogni vettore di $V(\mathbb{K})$ si può scrivere come combinazione lineare di un numero finito di elementi di X. X si dice **insieme di generatori** per $V(\mathbb{K})$.

Alternativamente:
X è insieme di generatori per $V(\mathbb{K}) \iff \mathcal{L}(X) = V$.

Uno spazio vettoriale è insieme di generatori per se stesso.
Aggiungere vettori ad un insieme di generatori fornisce ancora un insieme di generatori.

4.23 Definizione di Spazio Vettoriale Finitamente Generato

$V(\mathbb{K})$ è detto finitamente generato se $\exists X \subseteq V(\mathbb{K})$ con $|X| < \infty$ e X insieme di generatori per $V(\mathbb{K})$.

4.24 Definizione di Copertura Lineare

Siano $V(\mathbb{K})$ uno spazio vettoriale e $X \subseteq V(\mathbb{K})$.

$\mathcal{L}(X)$, detta **copertura lineare** (linear span) (o chiusura lineare) di X, è l'insieme di tutte le combinazioni lineari dei vettori in X.

In simboli:

$$\mathcal{L}_{V(\mathbb{K})}(X) = \mathcal{L}(X) = \langle X \rangle \coloneqq \left\{ \sum_{i}^{n\in\mathbb{N}} \alpha_i \bar{x}_i : \alpha_i \in \mathbb{K}, \bar{x}_i \in X \right\}$$

$$\mathcal{L}(\emptyset) \coloneqq \{\underline{0}\}$$

$\mathcal{L}(X)$ è sempre un sottospazio vettoriale di $V(\mathbb{K})$.
Inoltre, è il più piccolo sottospazio vettoriale di $V(\mathbb{K})$ che contiene X.

$A \subseteq B \implies \mathcal{L}(A) \subseteq \mathcal{L}(B)$
$A = \mathcal{L}(A) \iff A$ è sottospazio vettoriale.
$\mathcal{L}(\mathcal{L}(A)) = \mathcal{L}(A)$

4.25 Definizione di Sequenza Libera e Legata

Siano $V(\mathbb{K})$ uno spazio vettoriale ed $S = (\bar{v}_1, ..., \bar{v}_n)$ una sequenza di suoi vettori.

S è detta **libera** se l'unica combinazione lineare dei suoi elementi che da $\underline{0}$ è quella a coefficienti tutti nulli.

S è detta **legata** se esiste almeno una combinazione lineare dei suoi elementi a coefficienti non tutti nulli che da $\underline{0}$.

S è legata $=$ S non è libera.
$\underline{0} \in S \implies S$ è legata.
$\bar{v}_1 \in S \wedge \exists \alpha \neq 0 : \bar{v}_2 = \alpha \bar{v}_1 \in S \implies S$ è legata (quindi anche se ci sono due vettori uguali, con $\alpha = 1$).
X è libera $\wedge$ $Y \subseteq X \implies Y$ è libera.
X è legata $\wedge$ $X \subseteq Y \implies Y$ è legata.

4.25.1 Teorema

S è legata $\iff$ almeno uno dei suoi vettori si può scrivere come combinazione lineare dei rimanenti.

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.