Note del Corso di GEOMETRIA 1
A.A. 2023/2024

Prof. Valentina Beorchia

17 ottobre 2023

Indice

Capitolo 1

Preliminari di algebra

1.1 Operazioni su insiemi

Definizione 1.1.1 (Prodotto cartesiano)**.** Dati due insiemi A, B, il loro **prodotto cartesiano**, indicato con $A \times B$, è l'insieme delle coppie ordinate (a, b) con $a \in A$ e $b \in B$, cioè $A \times B = \{(a, b) \mid a \in A, b \in B\}$.

Esempi 1.1.2. 1. Se $A = \{1, 2, 3\}$, $B = \{a, b\}$, allora

$$A \times B = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}.$$

2. Sia $\mathbb{R}$ l'insieme dei numeri reali, allora

$$\mathbb{R} \times \mathbb{R} = \{(x, y) \mid x \in \mathbb{R}, y \in \mathbb{R}\} = \mathbb{R}^2.$$

Notiamo che le coppie sono *ordinate, dunque per esempio* $(1, 2) \neq (2, 1)$.

Definizione 1.1.3 (Operazione interna)**.** Sia S un insieme non vuoto. Un'**operazione interna in S o legge di composizione interna in** S è un'applicazione

$$S \times S \to S$$

avente dominio $S \times S$ e codominio S. Una tale operazione può essere denotata con uno dei simboli $*$, oppure $+$, oppure $\cdot$, oppure con altri simboli; nel primo caso, scriveremo che essa associa ad una coppia (a, b) l'elemento $a * b$ di S.

Il termine "applicazione" è sinomino di "funzione". Un altro termine usato a volte con lo stesso significato è "mappa".

Esempi 1.1.4. Esempi di operazioni interne.

(i) $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, la somma è un'operazione interna in $\mathbb{Z}$;
$(a, b) \to a + b$; per esempio
$(1, 2) \to 1 + 2 = 3$.

(ii) $\cdot : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$, il prodotto è un'operazione interna in $\mathbb{Q}$;

$(x, y) \to x \cdot y$; per esempio

$(1, 2) \to 1 \cdot 2 = 2$.

(iii) Sia $X \neq \emptyset$ un insieme non vuoto e sia F l'insieme delle applicazioni di X in X, cioè aventi X sia come dominio sia come codominio.

Si noti che F non è vuoto, in quanto contiene almeno l'applicazione identica $id_X : X \to X$, definita da $id_X(x) = x$ per ogni $x \in X$.

Possiamo definire un'operazione interna in F, data dalla *composizione di applicazioni* $\circ : F \times F \to F$, data da $(f, g) \to f \circ g$, dove $f \circ g$ è l'applicazione tale che

$$(f \circ g)(x) = f(g(x))$$

per ogni $x \in X$.

Gli esempi (i) e (ii) sono esempi di operazioni numeriche.

1.2 Gruppi

Definizione 1.2.1 (Gruppo)**.** Sia G un insieme e $*$ sia un'operazione interna in G. La coppia $(G, *)$ è detta un **gruppo** se valgono le seguenti proprietà:

(i) *Proprietà associativa*: per ogni $a, b, c \in G$, si ha $a * (b * c) = (a * b) * c$;

(ii) *Esistenza dell'elemento neutro*: esiste $e \in G$ tale che, per ogni $a \in G$, si ha $e * a = a * e = a$; l'elemento e è detto elemento neutro di G;

(iii) *Esistenza dei simmetrici, o reciproci*: per ogni $a \in G$ esiste $a' \in G$ tale che $a * a' = e = a' * a$. L'elemento a' è detto reciproco di a.

Se l'operazione è indicata additivamente, ossia con il simbolo $+$, l'elemento neutro è detto "zero" e indicato con il simbolo 0, mentre il reciproco di a è detto opposto di a e indicato con $-a$.

Se l'operazione è indicata moltiplicativamente, ossia con il simbolo $\cdot$ oppure $\times$, l'elemento neutro è detto "uno" o unità di G e indicato con 1 o 1_G, mentre il reciproco di a è detto inverso di a e indicato con a^{-1}.

Definizione 1.2.2 (Gruppo abeliano)**.** Un gruppo $(G, *)$ è detto **gruppo abeliano**, o commutativo, se vale la *proprietà commutativa*, cioè per ogni $a, b \in G$ si ha $a * b = b * a$.

Esempi 1.2.3.

1. $(\mathbb{Z}, +)$ è un gruppo abeliano.
2. $(\mathbb{Z}, \cdot)$ non è un gruppo: la proprietà associativa è soddisfatta, e l'1 esiste, però alcuni elementi non hanno l'inverso in $\mathbb{Z}$; si dice che "non sono invertibili" in $\mathbb{Z}$. Per esempio 0 non ha inverso, e anche 2 non è invertibile in $\mathbb{Z}$, in quanto si ha $2 \cdot z \neq 1$ per ogni $z \in \mathbb{Z}$.
3. $(\mathbb{Q}, +)$ è un gruppo abeliano.

4. $(\mathbb{Q} \setminus \{0\}, \cdot)$ è un gruppo abeliano.

   Infatti, osserviamo innanzitutto che il prodotto è un'operazione interna in $\mathbb{Q} \setminus \{0\}$, perchè il prodotto di due numeri razionali non nulli è non nullo. Inoltre, vale la proprietà associativa, l'elemento neutro è l'1, e per ogni $q \in \mathbb{Q} \setminus \{0\}$ esiste $q^{-1} = \frac{1}{q}$ che verifica $q \cdot \frac{1}{q} = \frac{1}{q} \cdot q = 1$.

5. Sia $X \neq \emptyset$ un insieme e sia $B(X) = \{f : X \to X \mid f \text{ biiettiva}\}$ l'insieme delle applicazioni biiettive di X in sè; date $f, g \in B(X)$, denotiamo con $f \circ g$ la funzione composta.

   Si ha che $(B(X), \circ)$ è un gruppo. Infatti:

   (i) se $f, g : X \to X$ sono biiettive, anche $f \circ g$ lo è, dunque la composizione è un'operazione interna in $B(X)$;

   (ii) la composizione di funzioni è associativa: $(f \circ g) \circ h = f \circ (g \circ h)$. Infatti, per ogni $x \in X$ si ha $((f \circ g) \circ h)(x) = f(g(h(x))) = (f \circ (g \circ h))(x)$.

   (iii) l'applicazione identica $id_X : x \to x$, per ogni $x \in X$, è l'elemento neutro di $B(X)$;

   (iv) ricordiamo che un'applicazione è biiettiva se e solo se esiste l'applicazione inversa $f^{-1} : X \to X$, che verifica
   $$f(x) = y \iff f^{-1}(y) = x.$$
   Infatti f è suriettiva e iniettiva, se e solo se, preso comunque un elemento $y \in X$, esiste ed è unico $x \in X$ tale che $f(x) = y$. L'applicazione f^{-1} è l'elemento inverso di f rispetto all'operazione $\circ$.

Osserviamo che tutti i gruppi "numerici" sono abeliani. Invece il gruppo $B(X)$ non è abeliano se X ha almeno tre elementi.

Per esempio, sia $X = \{1, 2, 3\}$. Consideriamo $f : X \to X$ data da

$$f(1) = 2, f(2) = 3, f(3) = 1,$$

e $g : X \to X$ data da

$$g(1) = 1, g(2) = 3, g(3) = 2.$$

Si ha che $f \circ g \neq g \circ f$, in quanto esiste almeno un elemento $x \in X$ tale che $(f \circ g)(x) \neq (g \circ f)(x)$.

Osserviamo che in questo caso $B(X)$ ha sei elementi, corrispondenti alle permutazioni dell'insieme X; si veda il Capitolo ....

Esercizi 1.

1. Costruire un esempio in cui $f \circ g \neq g \circ f$ in modo analogo al precedente, per X insieme di n elementi, con $n \geq 3$ qualunque.
2. Se X ha n elementi, quanti elementi ha $B(X)$?

Proposizione 1.2.4. *Sia $(G, *)$ un gruppo. Si ha:*

1. *l'elemento neutro in G è unico;*
2. *ogni elemento $g \in G$ ha un unico reciproco.*

Dimostrazione. 1. Supponiamo che e, e' siano entrambi elementi neutri di G, ossia elementi di G tali che, per ogni $g \in G$, si ha $e * g = g * e = g$ e $e' * g = g * e' = g$. Allora $e * e' = e'$ perchè e è neutro, ma anche $e * e' = e$ perchè e' è neutro. Dunque $e = e'$.

2. Supponiamo che g', g'' siano entrambi reciproci di g. Allora si ha $g * g' = g' * g = e$ e anche $g * g'' = g'' * g = e$. Quindi

$$g' = g' * e = g' * (g * g'') = \text{per la proprietà associativa} = (g' * g) * g'' = e * g'' = g''.$$

In conclusione si ha $g' = g''$. □

1.3 Relazioni d'equivalenza

Per questa sezione si vedano anche gli appunti del corso propedeutico.

Una **relazione** in un insieme X è una proprietà che una coppia ordinata di elementi di X può verificare o meno. Per esempio la relazione "$<$" "minore" ha senso negli insiemi numerici $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$; la relazione "$||$" "parallelo" ha senso nell'insieme delle rette del piano, o dei piani dello spazio.

In maniera più formale:

Definizione 1.3.1. Una relazione in X è un sottinsieme R del prodotto cartesiano $X \times X$. In tal caso si dirà che x è in relazione R con y se la coppia ordinata $(x, y) \in R$. Si scrive anche xRy.

Per esempio la relazione $<$ in $\mathbb{Z}$ corrisponde al sottinsieme di $\mathbb{Z} \times \mathbb{Z}$: $\{(x, y) \mid x < y\}$. Analogamente la relazione $\leq$ corrisponde al sottinsieme di $\mathbb{Z} \times \mathbb{Z}$: $\{(x, y) \mid x \leq y\}$. La relazione di parallelismo nell'insieme delle rette del piano corrisponde alle coppie di rette (r, r') tali che r, r' sono distinte e parallele oppure sono uguali.

Simboli spesso usati per denotare relazioni sono $\equiv$, $\sim$, $\simeq$, $\cong$, ecc.

Un altro esempio di relazione, in $\mathbb{R}$, è il seguente: $x \sim y$ se e solo se $x^2 = y$.

Noi saremo interessati a un tipo particolare di relazioni dette relazioni d'equivalenza.

Definizione 1.3.2 (Relazione d'equivalenza). Sia X un insieme e $\sim$ una relazione in X. Si dice che $\sim$ è una **relazione d'equivalenza** se valgono le tre proprietà:

1. riflessiva: per ogni $x \in X$ $x \sim x$;
2. simmetrica: se $x \sim y$ allora $y \sim x$;
3. transitiva: se $x \sim y$ e $y \sim z$ allora $x \sim z$.

Esempi 1.3.3.

1. L'uguaglianza è una relazione d'equivalenza in qualunque insieme X.
2. "Essere congruenti" è una relazione d'equivalenza nell'insieme dei triangoli del piano.
3. $\leq, <$ non sono relazioni d'equivalenza.

Il prossimo è un esempio fondamentale. Denotiamo con $\mathbb{N}$ l'insieme dei numeri naturali: $\mathbb{N} = \{0, 1, 2, 3 \ldots\}$.

Definizione 1.3.4 (Congruenza modulo n). Si fissi un naturale $n \in \mathbb{N}$. La relazione di congruenza modulo n è la relazione in $\mathbb{Z}$ così definita:

$$x \equiv y \pmod{n} \iff \exists\, k \in \mathbb{Z} \,:\, x - y = kn.$$

Si scrive anche $x \equiv_n y$. Si legge "x è congruo a y modulo n.

Proposizione 1.3.5. *La relazione di congruenza modulo n è una relazione d'equivalenza in $\mathbb{Z}$.*

Dimostrazione. Verifichiamo che sono soddisfatte le tre proprietà richieste:

1. simmmetria: $x - x = 0x$ per ogni $x \in \mathbb{Z}$.
2. riflessività: se $x \equiv_n y$, si ha $x - y = kn$ per un opportno $k \in \mathbb{Z}$. Allora $y - x = (-k)n$.
3. transitività: se $x \equiv_n y$ e $y \equiv_n z$, esistono $k, h \in \mathbb{Z}$ tali che $x - y = kn$, $y - z = hn$; ma allora $x - z = (x - y) + (y - z) = kn + hn = (k + h)n$, il che prova che $x \equiv_n z$. □

D'ora in poi supporremo sempre $n \geq 2$.

Proposizione 1.3.6. *$x \equiv_n y$ se e solo se x e y hanno lo stesso resto nella divisione per n.*

Dimostrazione. Infatti se x e y hanno lo stesso resto nella divisione per n, si ha: $x = qn + r$, $y = q'n + r$, dove $0 \leq r \leq n - 1$. Quindi $x - y = (qn + r) - (q'n + r) = (q - q')n$ e perciò $x \equiv_n y$.

Viceversa, se $x \equiv_n y$, si ha $x = y + kn$. Se r è il resto della divisione di y per n, vale anche $y = qn + r$ con $0 \leq r \leq n - 1$; perciò si ha $x = (qn + r) + kn = (q + k)n + r$, dunque r è anche il resto della divisione di x per n. □

Definizione 1.3.7 (**Classi d'equivalenza e insieme quoziente).** Sia X un insieme in cui è definita una relazione d'equivalenza $\sim$, sia $x \in X$. La **classe d'equivalenza** di x è il sottinsieme di X formato dagli elementi equivalenti a x:

$$[x] = \{y \in X \mid y \sim x\}.$$

Tale insieme si denota anche $[x]_\sim$.

L'insieme delle classi d'equivalenza è detto **insieme quoziente** di X rispetto alla relazione $\sim$ e si indica $X/\sim$.

L'insieme quoziente è un sottoinsieme dell'insieme $\mathcal{P}(X)$ delle parti di X, cioè l'insieme di tutti i sottoinsiemi di X.

Osserviamo che $x \in [x]$ per la proprietà riflessiva. Quindi nessun elemento dell'insieme quoziente $X/\sim$ è l'insieme vuoto $\emptyset$. Inoltre le classi d'equivalenza ricoprono X, ossia X è l'unione delle classi d'equivalenza $[x]$, al variare di $x \in X$.

Definizione 1.3.8 (**Partizione).** Una **partizione** di un insieme X è un sottinsieme Π dell'insieme delle parti di X che gode delle proprietà:

1. nessun elemento di Π è vuoto;
2. l'unione degli insiemi di Π è uguale a X;
3. se $S, T \in \Pi$, e $S \neq T$ allora $S \cap T = \emptyset$.

Dunque due elementi di una partizione Pi o sono disgiunti o sono uguali.

Proposizione 1.3.9. *L'insieme quoziente $X/\sim$ di una relazione d'equivalenza in X è una partizione di X.*

Dimostrazione. Le prime due proprietà sono già state osservate. Per provare la terza, consideriamo due classi d'equivalenza $[x], [y]$ tali che $[x] \cap [y] \neq \emptyset$. Allora esiste $z \in [x] \cap [y]$, cioè $z \sim x$ e $z \sim y$. Per le proprietà simmetrica e transitiva segue che $x \sim y$. Proviamo che di conseguenza $[x] = [y]$. Infatti, se $u \in [x]$, allora $u \sim x$, ma $x \sim y$, dunque per la proprietà transitiva $u \sim y$ e segue che $u \in [y]$. Abbiamo così provato che $[x] \subset [y]$. L'inclusione opposta è analoga. □

Esempi 1.3.10.

1. L'insieme quoziente $\mathbb{Z}/\equiv_n$ si denota $\mathbb{Z}_n$. Affermiamo che tale insieme ha n elementi, uno per ciascuno degli n possibili resti della divisione per n: $0, 1, 2, \ldots, n - 1$.

Infatti, se x ha resto r nella divisione per n, $x = qn + r$ dunque $x \equiv_n r$. Inoltre, è immediato verificare che le classi $[r]$ per $0 \leq r \leq n-1$ sono a due a due distinte.

Gli elementi di $\mathbb{Z}_n$ si denotano anche $[r]_n$ o $\bar{r}$. Dunque $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$.

Un insieme S si dice **finito** se esiste un numero naturale n tale che S è in biiezione con l'insieme $\{1, 2, 3, \ldots, n-1, n\}$. Dunque $\mathbb{Z}_n$ è un insieme finito con n elementi.

1.4 Operazioni in $\mathbb{Z}_n$

Sia $n \geq 2$. Nell'insieme $\mathbb{Z}_n$ si possono definire due operazioni, di somma e di prodotto, **indotte** dalle operazioni in $\mathbb{Z}$.

Siano $\bar{x}, \bar{y} \in \mathbb{Z}_n$. Definiamo

$$\bar{x} + \bar{y} = \overline{x+y}, \quad \bar{x} \cdot \bar{y} = \overline{x \cdot y}.$$

Il prodotto si denota anche semplicemente $\bar{x}\bar{y}$. Queste operazioni di somma e prodotto sono **ben definite**, in quanto non dipendono dai particolari rappresentanti scelti per le due classi. Infatti, sia $\bar{x} = \bar{x}'$ e $\bar{y} = \bar{y}'$. Allora si ha $x' = x + kn, y' = y + hn$, per $k, h \in \mathbb{Z}$ opportuni. Quindi $(x+y) - (x'+y') = (x+y) - (x+kn+y+hn) = -(k+h)n$, da cui segue che $x + y \equiv_n x' + y'$.

Analogamente $xy - x'y' = xy - (x+kn)(y+hn) = -(xh + yk + khn)n$ e perciò $xy \equiv_n x'y'$.

Dalle proprietà della somma in $\mathbb{Z}$ seguono facilmente le proprietà della somma in $\mathbb{Z}_n$:

1. proprietà associativa: $(\bar{x} + \bar{y}) + \bar{z} = \bar{x} + (\bar{y} + \bar{z})$;
2. la classe $\bar{0}$ è l'elemento neutro della somma;
3. $\overline{-x} = -\bar{x}$;
4. proprietà commutativa: $\bar{x} + \bar{y} = \bar{y} + \bar{x}$. Ne segue

Proposizione 1.4.1. *$(\mathbb{Z}_n, +)$ è un gruppo abeliano.*

Analogamente, dalle proprietà del prodotto in $\mathbb{Z}$ segue che valgono le seguenti proprietà del prodotto in $\mathbb{Z}_n$:

1. proprietà associativa: $(\bar{x}\bar{y})\bar{z} = \bar{x}(\bar{y}\bar{z})$;
2. $\bar{1}$ è l'unità per il prodotto;
3. proprietà commutativa: $\bar{x}\bar{y} = \bar{y}\bar{x}$;
4. proprietà distributiva: $(\bar{x} + \bar{y})\bar{z} = \bar{x}z + \bar{y}z$.

1.5 Campi

Definizione 1.5.1 (Campo). Sia K un insieme dotato di due operazioni, chiamate somma e prodotto e denotate con $+$ e $\cdot$. La terna $(K, +, \cdot)$ si dice un **campo** se valgono le seguenti proprietà:

1. K è un gruppo abeliano rispetto alla somma;
2. proprietà associativa del prodotto;
3. esiste elemento unità;
4. ogni elemento **non nullo** di K ammette inverso;
5. proprietà commutativa del prodotto;

6. proprietà distributiva del prodotto rispetto alla somma: per ogni $a, b, c \in K$ si ha: $(a+b)\cdot c = ac + bc$.

Esempi 1.5.2.
1. Campi numerici: $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$,
2. $(\mathbb{Z}, +, \cdot)$ non è un campo perché soltanto 1 e -1 hanno inverso.

Proposizione 1.5.3 (Proprietà generali dei campi)**.** *1. Per ogni $a \in K$ $0 \cdot a = 0$;*
2. Legge di annullamento del prodotto. Se $a \cdot b = 0$, allora $a = 0$ oppure $b = 0$;
3. Sia -1 l'opposto di 1 e $a \in K$. Allora $(-1)\cdot a = -a$.

Dimostrazione. 1. Usando la proprietà che 0 è elemento neutro per la somma e la proprietà distributiva si ottiene:

$$0 \cdot a = (0+0)a = 0 \cdot a + 0 \cdot a.$$

Sommando $-(0 \cdot a)$ a ambo i membri, si ottiene $0 \cdot a = 0$.

2. Sia $a \cdot b = 0$. Se $a = 0$ abbiamo finito, sia dunque $a \neq 0$. Allora esiste a^{-1}. Moltiplicando ambo i membri a sinistra per a^{-1} otteniamo

$$a^{-1} \cdot (a \cdot b) = (a^{-1} \cdot a) \cdot b = 1 \cdot b = b;$$

ma $a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 = 0$ per il punto precedente, dunque $b = 0$.

3. $(-1)\cdot a + a = (-1)\cdot a + 1 \cdot a =$ proprietà distributiva $= ((-1)+1)\cdot a = 0 \cdot a = 0$. Analogamente $a + (-1)\cdot a = 0$. □

La legge di annullamento del prodotto garantisce che $K \setminus \{0\}$ è chiuso rispetto al prodotto. Si pu o anche esprimere dicendo che in K non vi sono divisori dello zero. Dunque le condizioni 2 – 5 della definizione di campo si possono riassumere dicendo che $(K \setminus \{0\}, \cdot)$ è un gruppo abeliano.

D'ora in poi lavorando in un campo K useremo spesso le notazioni compatte:
$a - b = a + (-b)$
$ab = a \cdot b$
$\frac{a}{b} = a/b = ab^{-1}$.

Vogliamo ora determinare per quali n $\mathbb{Z}_n$ è un campo. A tale scopo consideriamo la tabella di moltiplicazione di $\mathbb{Z}_n \setminus \{0\}$ per $n = 2, 3, 4, 5$. Per semplicità di scrittura indicheremo gli elementi di $\mathbb{Z}_n$ omettendo il segno sopra.

$n = 2$

$\cdot$	1
1	1

$n = 3$

$\cdot$	1	2
1	1	2
2	2	1

$n = 4$

$\cdot$	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

$n = 5$

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Dalle tabelle segue che $\mathbb{Z}_4$ non è un campo, perchè $\bar{2}$ non è invertibile, mentre $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5$ lo sono. In effetti, vale il seguente teorema.

Teorema 1.5.4. *Sia $n \geq 2$. Allora $\mathbb{Z}_n$ è un campo se e solo se n è un numero primo.*

Dimostrazione. Supponiamo dapprima che n non sia primo, e dimostriamo che $\mathbb{Z}_n$ non è un campo. Infatti, se n non è primo, esistono due interi a, b con $1 < a, b < n$ tali che $n = ab$. Passando alle classi di equivalenza nel quoziente $\mathbb{Z}_n$ si ottiene $\bar{n} = \bar{0} = \bar{a}\bar{b}$, che contraddice la Proposizione 1.5.3, punto 2, in quanto $\bar{a} \neq 0$ e $\bar{b} \neq 0$: $\bar{a}$ e $\bar{b}$ sono divisori dello zero.

Supponiamo ora che n sia primo e vogliamo dimostrare che $\mathbb{Z}_n$ è un campo.

Useremo le due seguenti proprietà.

1. Siano p un numero primo e $a, b \in \mathbb{Z}$. Se $p|ab$, allora o $p|a$ o $p|b$ (il segno | significa "divide"). Tale proprietà segue immediatamente dal Teorema fondamentale dell'aritmetica, ossia dall'esistenza e unicità della scomposizione in fattori primi.

2. *Principio della piccionaia.* Se X è un insieme **finito** e $f : X \to X$ è un'applicazione iniettiva, allora f è anche suriettiva, e quindi è una biiezione. Infatti, se f è iniettiva, f stabilisce una biiezione fra X e $f(X)$, dunque pure $f(X)$ è finito e ha lo stesso numero di elementi di X. Essendo $f(X) \subset X$ segue che $f(X) = X$.

Fissiamo dunque $\bar{a} \in \mathbb{Z}_n$, con n primo. Supponiamo $\bar{a} \neq 0$. Vogliamo dimostrare che $\bar{a}$ è invertibile. Consideriamo l'applicazione $\varphi : \mathbb{Z}_n \to \mathbb{Z}_n$ definita da $\varphi(\bar{x}) = \bar{a}\bar{x}$: φ è la moltiplicazione per $\bar{a}$.

Osserviamo dapprima che φ è iniettiva. Infatti, se $\varphi(\bar{x}) = \varphi(\bar{y})$ ciò significa che $\bar{a}\bar{x} = \bar{a}\bar{y}$. Per definizione del prodotto in $\mathbb{Z}_n$, allora $\overline{ax} = \overline{ay}$, e quindi $ax \equiv ay \pmod{n}$. Perciò n divide $ax - ay = a(x - y)$. Dalla proprietà 1. segue che o $n|a$ o $n|x - y$. La prima è impossibile perchè $\bar{a} \neq 0$ per ipotesi, dunque $n|x - y$, ossia $\bar{x} = \bar{y}$; abbiamo così provato che φ è iniettiva.

Dunque per il Principio della piccionaia φ è anche suriettiva. Allora l'immagine di $\mathbb{Z}_n$ in φ, $\varphi(\mathbb{Z}_n)$ è tutto $\mathbb{Z}_n$. Quindi per ogni elemento $\bar{z}$ di $\mathbb{Z}_n$ esiste un $\bar{y} \in \mathbb{Z}_n$ tale che $\bar{z} = \varphi(\bar{y}) = \bar{a}\bar{y}$. In particolare se consideriamo l'unit à $\bar{1} \in \mathbb{Z}_n$, esiste un $\bar{y}$ tale che $\bar{1} = \bar{a}\bar{y}$: tale $\bar{y}$ è l'inverso di $\bar{a}$ in $\bar{Z}_n$.

□

Esercizi 2.

1. In $\mathbb{R}^2$ si definiscano le seguenti operazioni:

   somma : $(x, y) + (x', y') = (x + x', y + y')$;

   prodotto : $(x, y)(x', y') = (xx' - yy', xy' + yx')$.

   Verificare che $\mathbb{R}^2$ con tali operazioni è un campo.

   Questo è un modo per introdurre il campo dei numeri complessi $\mathbb{C}$.

Capitolo 2

Spazi vettoriali

2.1 Vettori applicati e vettori liberi

L'algebra lineare e la geometria affine sono due teorie che sono state sviluppate negli ultimi due secoli sul modello dell'algebra dei vettori liberi su una retta, in un piano o in uno spazio fisico, le cui proprietà sono una conseguenza degli assiomi classici della geometria euclidea. L'algebra lineare come strumento si è rivelata molto potente, perché applicabile a svariati contesti diversi, ha permesso di organizzare la geometria dello spazio euclideo in modo più efficiente sia dal punto di vista teorico che dal punto di vista computazionale rispetto all'approccio antico, e perché è alla base della moderna Analisi Funzionale.

È utile, in ogni caso, richiamare e rivedere velocemente la geometria e le operazioni con i vettori applicati e i vettori liberi, che permette di comprendere meglio la scelta delle definizione e degli assiomi dell'algebra lineare, e sarà di aiuto durante tutto il corso per la comprensione degli argomenti più complicati.

Consideriamo un piano o uno spazio "fisico". Un **vettore applicato** è un segmento orientato, ed è assegnato dando un punto di applicazione (il punto iniziale), la sua direzione (la retta su cui giace, detta anche giacitura), il suo modulo (la lunghezza del segmento, che è un numero reale ≥ 0), e il suo verso (uno dei due possibili versi di percorrenza della retta di giacitura). Osserviamo che tra i vettori applicati vi è anche il vettore nullo, identificabile con un punto del piano; per esso la direzione è indeterminata (esso giace su qualunque retta passante per il punto), e così pure il verso.

Un vettore applicato può essere caratterizzato anche come il dato di una coppia di punti, e precisamente: un punto iniziale A, punto di applicazione, ed un punto finale B, e verrà indicato con

$$\vec{AB}.$$

I vettori del tipo $\vec{AA}$, cioè tali che il punto di applicazione coincide con il punto finale, sono detti vettori applicati nulli.

Definizione 2.1.1. La **somma di due vettori applicati** del tipo $\vec{AB}$ e $\vec{BC}$ è per definizione il vettore

$$\vec{AB} + \vec{BC} := \vec{AC}.$$

Osservazione 1. La somma di un vettore $\vec{AB}$ con un vettore nullo del tipo $\vec{AA}$ oppure $\vec{BB}$ verifica:

$$\vec{AA} + \vec{AB} = \vec{AB}, \qquad \vec{AB} + \vec{BB} = \vec{AB}.$$

Inoltre la somma verifica la proprietà associativa:

$$\vec{AB} + (\vec{BC} + \vec{CD}) = (\vec{AB} + \vec{BC}) + \vec{CD}.$$

Definizione 2.1.2. La **moltiplicazione di un vettore applicato per uno scalare** è definita come segue: per ogni vettore applicato $\vec{AB}$ e per ogni numero reale $a \in \mathbb{R}$, il vettore $a \cdot \vec{AB}$ è quel vettore geometrico che ha

- la stessa direzione di $\vec{AB}$,
- lunghezza pari a quella di $\vec{AB}$ moltiplicata per il valore assoluto $|a|$ di a,
- verso concorde con $\vec{AB}$ se $a > 0$, altrimenti ha verso opposto. Se $a = 0$ si pone $0 \cdot \vec{AB} = \vec{AA}$.

Vediamo ora la nozione di *vettore libero*. Due vettori applicati sono detti **equipollenti** se hanno la stessa direzione, la stessa lunghezza e lo stesso verso; in altre parole se giacciono su due rette parallele e se, muovendo una delle due rette parallelamente a se stessa, è possibile sovrapporre i due vettori in modo che i relativi punti iniziali e finali coincidano.

Si osservi che l'equipollenza è una relazione di equivalenza nell'insieme dei vettori applicati. Infatti ci si convince facilmente che valgono le seguenti proprietà: riflessiva, simmetrica e transitiva. Un **vettore libero o geometrico** è una classe di equivalenza di vettori applicati per la relazione di equipollenza (in questo contesto si dice anche classe di equipollenza). Denoteremo tra le parentesi quadre $[\vec{AB}]$ le classi di equipollenza dei vettori applicati ed i corrispondenti vettori liberi con le lettere minuscole:

$$\vec{u} = [\vec{AB}].$$

Il vettore nullo $\vec{0}$ è quel vettore rappresentato da un vettore applicato del tipo $\vec{AA}$.

Denoteremo con $\mathcal{V}^1$, $\mathcal{V}^2$ e $\mathcal{V}^3$ gli insiemi di vettori liberi della retta, del piano e dello spazio rispettivamente.

Osservazione 2. Fissato un punto O del piano o dello spazio, ogni vettore geometrico $\vec{v}$ 'e rappresentato da un unico vettore applicato $\vec{OP}$. Questa affermazione segue dal quinto postulato della geometria euclidea.

Nell'insieme dei vettori geometrici è possibile definire due operazioni: la somma di vettori e la moltiplicazione per uno scalare reale.

Definizione 2.1.3. La **somma di due vettori geometrici** $\vec{v} = [\vec{AB}]$ e $\vec{u} = [\vec{BC}]$ è così definita:

$$\vec{v} + \vec{u} = [\vec{AB}] + [\vec{BC}] := [\vec{AB} + \vec{BC}] = [\vec{AC}].$$

Osservazione 3. Si può verificare facilmente che la definizione è **ben posta**, cioè non dipende dai due rappresentanti scelti.

Inoltre, se i vettori $\vec{v}$ e $\vec{u}$ non sono allineati o nulli, la somma si può definire anche tramite la **regola del parallelogramma**:

se $\vec{v} = [\vec{OP}]$ e $\vec{u} = [\vec{OQ}]$, si costruisce il parallelogramma di lati OP ed OQ e si denota con R il quarto vertice di tale parallelogramma. La somma $\vec{v} + \vec{u}$ risulta uguale al vettore geometrico rappresentato da $\vec{OR}$.

Osservazione 4. L'operazione di somma tra due vettori geometrici soddisfa le seguenti proprietà:

- **Proprietà associativa**: per ogni scelta di una terna di vettori geometrici $\vec{u}, \vec{v}, \vec{w}$, si ha:

$$(\vec{u} + \vec{v}) + \vec{w} = \vec{u} + (\vec{v} + \vec{w}).$$

  Sfruttando questa proprietà possiamo, ad esempio, scrivere espressioni come $\vec{u} + \vec{v} + \vec{w}$.

- **Proprietà commutativa**: per ogni coppia di vettori geometrici $\vec{v}$ e $\vec{u}$ si ha

$$\vec{v} + \vec{u} = \vec{u} + \vec{v}.$$

- **Esistenza dell'elemento neutro**: se denotiamo con $\vec{0}$ il vettore nullo, allora per ogni vettore geometrico $\vec{v}$ vale:

$$\vec{v} + \vec{0} = \vec{0} + \vec{v} = \vec{v}.$$

- **Esistenza dell'opposto**: per ogni vettore geometrico $\vec{v}$, esiste il suo opposto, cioè un vettore geometrico $-\vec{v}$, tale che

$$\vec{v} + (-\vec{v}) = (-\vec{v}) + \vec{v} = \vec{0},$$

  dove $\vec{0}$ è il vettore nullo.

  Infatti, si consideri un rappresentante $\vec{AB}$ di $\vec{v}$, e si definisca $-\vec{v}$ come la classe di equipollenza di $\vec{BA}$.

  In seguito, per ogni coppia di vettori $\vec{v}, \vec{w}$, scriveremo semplicemente

$$\vec{v} - \vec{w}$$

  in luogo di

$$\vec{v} + (-\vec{w}).$$

Nell'insieme dei vettori geometrici, oltre alla somma di due vettori, possiamo definire la moltiplicazione per scalari in modo analogo sfruttando la moltiplicazione per scalari con vettori applicati.

Definizione 2.1.4. Per ogni vettore geometrico $\vec{v} = [\vec{AB}]$ e per ogni numero reale $a \in \mathbb{R}$ poniamo

$$a \cdot \vec{v} := [a \cdot \vec{AB}].$$

Anche in questo caso è facile verificare che la definizione è ben posta, cioè non dipende dal rappresentante.

Proprietà dell'operazione di moltiplicazione per scalari: per ogni coppia di vettori geometrici $\vec{v}, \vec{w}$ e per ogni coppia di scalari $a, b \in \mathbb{R}$, si ha:

- $1 \cdot \vec{v} = \vec{v}$;
- $(-1) \cdot \vec{v} = -\vec{v}$;
- $(a + b) \cdot \vec{v} = a \cdot \vec{v} + b \cdot \vec{v}$; $(ab) \cdot \vec{v} = a \cdot (b \cdot \vec{v})$; $a \cdot (\vec{v} + \vec{w}) = a \cdot \vec{v} + a \cdot \vec{w}$.

2.2 Spazi vettoriali

Sul modello dell'insieme dei vettori geometrici con le due operazioni appena descritte e le loro proprietà introduciamo la seguente definizione di spazio vettoriale. Osserviamo che la nuovo definizione è molto generale e comprende spazi di natura molto diversa.

Definizione 2.2.1. Uno **spazio vettoriale reale** o **$\mathbb{R}$-spazio vettoriale** è un insieme non vuoto V su cui sono definite due operazioni, una somma

$$\begin{aligned} + : V \times V &\to V, \\ (v, w) &\to v + w, \end{aligned}$$

ed un prodotto per scalari

$$\begin{aligned} \cdot : \mathbb{R} \times V &\to V, \\ (a, v) &\to a \cdot v, \end{aligned}$$

in modo che siano soddisfatti i seguenti assiomi, per ogni $u, v, w \in V$, e per ogni $a, b \in \mathbb{R}$:

1. V1: **proprietà associativa**:
$$(u + v) + w = u + (v + w);$$
2. V2: **proprietà commutativa**:
$$u + v = v + u;$$
3. V3: **esistenza del vettore nullo**: esiste $0 \in V$ tale che
$$0 + v = v + 0 = v;$$
4. V4: **esistenza dell'opposto**: per ogni $v \in V$, esiste un vettore $-v \in V$ tale che
$$v + (-v) = (-v) + v = 0;$$
5. V5: **distributiva di $\cdot$ rispetto a $+$**:
$$a \cdot (u + v) = a \cdot u + a \cdot v;$$
6. V6: **distributiva di $\cdot$ rispetto alla somma di $\mathbb{R}$**:
$$(a + b) \cdot v = a \cdot v + b \cdot v;$$
7. V7: $(ab) \cdot v = a \cdot (b \cdot v)$;
8. V8: per ogni $v \in V$ si ha
$$1 \cdot v = v.$$

Notiamo che abbiamo utilizzato lo stesso simbolo 0 per denotare sia il vettore nullo che lo zero come numero reale, per non appesantire la notazione. Inoltre, nel seguito, espressioni del tipo $v+(-w)$ verranno semplificate con $v - w$.

Esempio 2.2.2. 1. L'insieme dei vettori geometrici della retta $\mathcal{V}^1$, del piano $\mathcal{V}^2$ o dello spazio $\mathcal{V}^3$ con le operazioni descritte all'inizio del capitolo è uno spazio vettoriale su $\mathbb{R}$.

2. L'insieme dei numeri reali $\mathbb{R}$ è uno spazio vettoriale su $\mathbb{R}$ con le usuali definizioni di somma tra numeri reali e prodotto tra numeri reali, dove questa volta il prodotto

$$\cdot : \mathbb{R} \times \mathbb{R} \to \mathbb{R}, \qquad (a, b) \to a \cdot b$$

viene considerato come operazione "esterna", nel senso che $\mathbb{R}$ gioca sia il ruolo di insieme degli scalari che il ruolo di spazio dei vettori.

3. il prodotto cartesiano

$$\mathbb{R} \times \mathbb{R} = \mathbb{R}^2 := \left\{ \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mid x_1 \in \mathbb{R},\ x_2 \in \mathbb{R} \right\}$$

con l' operazione di somma così definita:

$$+ : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}^2, \qquad \left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \right) \to \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} := \begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 \end{pmatrix}$$

e di moltiplicazione per uno scalare:

$$\cdot : \mathbb{R} \times \mathbb{R}^2 \to \mathbb{R}^2, \qquad \left(c, \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \right) \to c \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} := \begin{pmatrix} c \cdot x_1 \\ c \cdot x_2 \end{pmatrix}$$

verifica gli assiomi per uno spazio vettoriale reale.

4. Più in generale, per ogni $n \in \mathbb{N}$, il prodotto cartesiano di $\mathbb{R}$ per se stesso n -volte:

$$\mathbb{R}^n = \left\{ \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \mid x_1 \in \mathbb{R},\ x_2 \in \mathbb{R}, \ldots, x_n \in \mathbb{R} \right\}$$

con l' operazione di somma così definita:

$$+ : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}^2, \qquad \left(\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}, \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} \right) \to \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} := \begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 \\ \vdots \\ x_n + y_n \end{pmatrix}$$

e di moltiplicazione per uno scalare:

$$\cdot : \mathbb{R} \times \mathbb{R}^2 \to \mathbb{R}^2, \qquad \left(c, \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \right) \to c \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} := \begin{pmatrix} c \cdot x_1 \\ c \cdot x_2 \\ \vdots \\ c \cdot x_n \end{pmatrix}$$

verifica gli assiomi per uno spazio vettoriale reale.

5. L'insieme delle funzioni reali
$$\mathcal{F} := \{f | f : \mathbb{R} \to \mathbb{R}\},$$
con l'operazione di somma (definita puntalmente):
$$+ : \mathcal{F} \times \mathcal{F} \to \mathcal{F}, \qquad (f, g) \to f + g \ : \ (f + g)(r) := f(r) + g(r),$$
e la moltiplicazione per uno scalare
$$\cdot : \mathbb{R} \times \mathcal{F} \to \mathcal{F}, \qquad (c, f) \to c \cdot f \ : \ (c \cdot f)(r) := c \cdot f(r)$$
è uno spazio vettoriale reale.

6. L'insieme dei polinomi reali in una indeterminata:
$$\mathbb{R}[x] := \{p(x) \mid p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0, \ a_n, a_{n-1}, \ldots, a_1, a_0 \in \mathbb{R}\}$$
con l'usuale somma tra polinomi e l'usuale prodotto per uno scalare è uno spazio vettoriale reale.

2.3 Sottospazi vettoriali

Definizione 2.3.1. Sia V uno spazio vettoriale su un campo $\mathbb{K}$. Un sottoinsieme non vuoto $W \subseteq V$ si dice **sottospazio vettoriale** di V se valgono le seguenti condizioni:

- (W1) per ogni $w_1 \in W$ e per ogni $w_2 \in W$ si ha
$$w_1 + w_2 \in W;$$
- (W2) per ogni $W \in W$ e per ogni scalare $a \in \mathbb{K}$ si ha
$$a \cdot w \in W.$$

Osservazione 5. Osserviamo che un sottospazio vettoriale W è a sua volta uno spazio vettoriale su $\mathbb{K}$ con le operazioni ereditate da V. È facile verificare che valgono gli assiomi $V1, \ldots, V8$ di spazio vettoriale.

Esempio 2.3.2. di sottospazi vettoriali

1. Il sottoinsieme $W = V$ risulta in modo evidente un sottospazio vettoriale, detto **sottospazio vettoriale improprio**.
2. Il sottoinsieme formato dal solo vettore nullo $\{0\} \subseteq V$ è un sottospazio vettoriale, percheé verifica $W1$ e $W2$, e si chiama **sottospazio vettoriale banale**. Osserviamo che è il più piccolo sottospazio (e anche spazio) vettoriale.
3. Il sottoisieme di $\mathcal{F}(\mathbb{R}, \mathbb{R})$ costituito dalle funzioni **limitate**:
$$\mathcal{L}(\mathbb{R}, \mathbb{R}) := \{f \mid f : \mathbb{R} \to \mathbb{R}, \ f \text{ limitata}\} \subset \mathcal{F}(\mathbb{R}, \mathbb{R})$$
è un sottospazio vettoriale. Ricordiamo la definizione: $f : \mathbb{R} \to \mathbb{R}$ si dice limitata se $\exists \ M > 0$, $M \in \mathbb{R}$, tale che $|f(r)| \leq M$ per ogni $r \in \mathbb{R}$.

4. Nello spazio delle funzioni
$$\mathcal{F}(\mathbb{R},\mathbb{R}) = \{f \mid f : \mathbb{R} \to \mathbb{R}\}$$
il sottoinsieme delle funzioni continue
$$\mathcal{C}^0(\mathbb{R},\mathbb{R}) := \{f \mid f : \mathbb{R} \to \mathbb{R} \text{ continua}\}$$
è un sottospazio vettoriale perché la somma di funzioni continue e la moltiplicazione di uno scalare per una funzione continua sono ancora funzioni continue.

   Analogamente si può verificare facilmente che il sottoinsieme delle funzioni derivabili con derivata continua
$$\mathcal{C}^1(\mathbb{R},\mathbb{R}) := \{f \mid f : \mathbb{R} \to \mathbb{R} \text{ derivabile e } f' \text{ continua}\}$$
è un sottospazio vettoriale.

   Inoltre si ha
$$\mathcal{C}^0(\mathbb{R},\mathbb{R}) \supset \mathcal{C}^1(\mathbb{R},\mathbb{R}),$$
e $\mathcal{C}^1(\mathbb{R},\mathbb{R})$ risulta anche sottospazio vettoriale di $\mathcal{C}^0(\mathbb{R},\mathbb{R})$.

5. Consideriamo lo spazio vettoriale $\mathbb{R}[x]$ dei polinomi in una indeterminata a coefficienti in $\mathbb{R}$.

   Il sottoinsieme dei polinomi di grado minore o uguale a un grado fissato $d \in \mathbb{N}$
$$\mathbb{R}[x]_{\leq d} := \{p(x) \mid \deg p(x) \leq d\}$$
risulta un sottospazio vettoriale.

Esempio 2.3.3. Sottoinsiemi che non sono sottospazi vettoriali

1. La circonferenza
$$S := \{\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mid x_1^2 + (x_2 - 1)^2 = 1\} \subseteq \mathbb{R}^2$$
non è un sottospazio vettoriale; infatti, ad esempio
$$\begin{pmatrix} 0 \\ 2 \end{pmatrix} \in S, \text{ ma } -\begin{pmatrix} 0 \\ 2 \end{pmatrix} = \begin{pmatrix} 0 \\ -2 \end{pmatrix} \notin S.$$

2. In generale, ogni sottoinsieme **limitato** di $\mathbb{R}^2$ e di $\mathbb{R}^n$ in generale non è un sottospazio vettoriale; infatti, la condizione $W2$ implica che i vettori di un sottospazio vettoriale possano assumere "lunghezze" (vedremo la definizione in seguito) arbitrariamente grandi.

3. Le rette del piano che non passano per l'origine non sono sottospazi vettoriali, perché non contengono il vettore nullo.

4. Consideriamo lo spazio vettoriale $\mathbb{R}[x]$ dei polinomi in una indeterminata a coefficienti in $\mathbb{R}$.

   Il sottoinsieme dei polinomi di grado **uguale a un grado fissato** $d \in \mathbb{N}$
$$\mathbb{R}[x]_d := \{p(x) \mid \deg p(x) = d\}$$
non risulta un sottospazio vettoriale, perché non verifica la $W1$. Ad esempio, la somma dei due polinomi
$$x^d - 1, \quad -x^d + 3$$
non è un polinomio di grado d: $x^d - 1 + (-x^d + 3) = 2$, polinomio costante, di grado zero.

Proposizione 2.3.4. *Sia V uno spazio vettoriale su $\mathbb{K}$, e siano*

$$U \subseteq V, \quad W \subseteq V$$

due suoi sottospazi vettoriali.
Allora l'intersezione

$$U \cap W \subseteq V$$

è ancora un sottospazio vettoriale.

Dimostrazione. Verifichiamo che vale la $W1$ per $U \cap W$:
siano $u_1, u_2 \in U \cap W \subseteq U$; siccome U è sottospazio vettoriale, si ha

$$u_1 + u_2 \in U.$$

Ma abbiamo anche $u_1, u_2 \in U \cap W \subseteq W$; siccome W è sottospazio vettoriale, si ha

$$u_1 + u_2 \in W.$$

Quindi $u_1 + u_2 \in U \cap W$.
Verifichaimo ora la $W2$: sia $u \in U \cap W$ e sia $c \in \mathbb{K}$; essendo $U \cap W \subseteq U$ ed essendo U sottospazio vettoriale, si ha

$$c \cdot u \in U.$$

Analogamente, essendo $U \cap W \subseteq W$ ed essendo W sottospazio vettoriale, si ha

$$c \cdot u \in W.$$

Concludiamo quindi nuovamente che $c \cdot u \in U \cap W$. □

Osservazione 6. Sia V uno spazio vettoriale su $\mathbb{K}$, e siano

$$U \subseteq V, \quad W \subseteq V$$

due suoi sottospazi vettoriali.
In generale l'unione

$$U \cup W$$

non è un sottospazio vettoriale.

Ci chiediamo allora quale sia il più piccolo sottospazio vettoriale contenente due dati sottospazi. Abbiamo la seguente:

Definizione 2.3.5. Sia V uno spazio vettoriale su $\mathbb{K}$, e siano

$$U \subseteq V, \quad W \subseteq V$$

due suoi sottospazi vettoriali. Il **sottospazio vettoriale somma** $U + W$ è così definito:

$$U + V := \{v \in V \mid \exists u \in U, \exists w \in W, \text{ tali che } v = u + w\},$$

è dato cioè da tutte le possibili somme di vettori di U con vettori di W.

Lemma 2.3.6. *Il sottospazio somma $U + W \subseteq V$ è un sottospazio vettoriale.*
Inoltre, $U + W$ è il più piccolo sottospazio vettoriale contenente $U \cup W$.

Dimostrazione. Esercizio. □

2.4 Combinazioni lineari e sottospazi vettoriali finitamente generati

Definizione 2.4.1. Dati $v_1, \dots, v_k \in V$, una **combinazione lineare** di $v_1, \dots, v_k$ a coefficienti in $\mathbb{K}$ è un vettore del tipo

$$c_1 v_1 + \cdots + c_k v_k \in V, \quad c_1, \dots, c_k \in \mathbb{K}.$$

Definizione 2.4.2. Se $v_1, \dots, v_k \in V$ è un numero finito di vettori di V, definiamo

$$\mathrm{Span}(v_1, \dots, v_k) := \{a_1 \cdot v_1 + \dots a_k \cdot v_k \mid a_1, \dots, a_k \in \mathbb{K}\},$$

che risulta un sottospazio vettoriale (verificare per esercizio).

Esempio 2.4.3.

- Sia V uno spazio vettoriale non banale, e sia $v \in V$ un vettore non nullo: $v \neq 0$. Allora

  $$\mathrm{Span}(v) = \{c \cdot v \mid c \in \mathbb{K}\},$$

  consiste cioè di tutti i vettori proporzionali a v. Il sottospazio vettoriale $\mathrm{Span}(v)$ viene chiamato **retta vettoriale**, e il vettore v viene chiamato **generatore**.

- Sia V uno spazio vettoriale non banale e siano $v, w \in V$ due vettori non nulli: $v \neq 0$, $w \neq 0$. Allora

  $$\mathrm{Span}(v, w) = \{a \cdot v + b \cdot w \mid a \in \mathbb{K}, b \in \mathbb{K}\},$$

  consiste cioè di tutte le possibili somme di vettori proporzionali a v e w.

  Nel caso che w non sia proporzionale a v, $\mathrm{Span}(v, w)$ viene chiamato **piano vettoriale**. Nel caso che w sia invece proporzionale a v, si può verificare facilmente che vale

  $$w = c \cdot v \Rightarrow \mathrm{Span}(v, w) = \mathrm{Span}(v) = \mathrm{Span}(w),$$

  quindi si ottiene nuovamente una retta vettoriale.

Osservazione 7. Osserviamo, in particolare, che i vettori $v_1, \dots, v_k \in \mathrm{Span}(v_1, \dots, v_k)$; infatti, si ha

$$v_1 = 1 \cdot v_1 + 0 \cdot v_2 + \cdots + 0 \cdot v_k, v_2 = 0 \cdot v_1 + 1 \cdot v_2 + \cdots + 0 \cdot v_k, \dots,$$

$$v_k = 0 \cdot v_1 + 0 \cdot v_2 + \cdots + 1 \cdot v_k.$$

Inoltre, per ogni $l < k$, abbiamo

$$\mathrm{Span}(v_1, \dots, v_l) \subseteq \mathrm{Span}(v_1, \dots, v_k).$$

Infatti, ogni $v \in \mathrm{Span}(v_1, \dots, v_l)$ soddisfa

$$v = c_1 \cdot v_1 + c_2 \cdot v_2 + \cdots + c_l \cdot v_l,$$

e tale relazione si può riscrivere nella forma:

$$v = c_1 \cdot v_1 + c_2 \cdot v_2 + \cdots + c_l \cdot v_l + 0 \cdot v_{l+1} + \cdots + 0 \cdot v_k,$$

quindi v è anche combinazione lineare di $v_1, \dots, v_k$.

Notiamo, però, che $l < k$ non implica, in generale,

$$\mathrm{Span}(v_1, \dots, v_l) \subsetneq \mathrm{Span}(v_1, \dots, v_k),$$

come ad esempio nel seguente caso:

$$\mathrm{Span}\left(\begin{pmatrix} 1 \\ 1 \end{pmatrix}\right) = \mathrm{Span}\left(\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 5 \\ 5 \end{pmatrix}\right) \subset \mathbb{R}^2.$$

Esempi 2.4.4. • Consideriamo i vettori

$$v_1 = \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \quad v_2 = \begin{pmatrix} -1 \\ 1 \end{pmatrix} \in \mathbb{R}^2.$$

Osserviamo che il vettore $w = \begin{pmatrix} 3 \\ 0 \end{pmatrix}$ si puó scrivere come combinazione lineare di v_1 e v_2:

$$w = \begin{pmatrix} 3 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \end{pmatrix} - 2 \begin{pmatrix} -1 \\ 1 \end{pmatrix} = v_1 - 2v_2,$$

quindi $w \in \mathrm{Span}(v_1, v_2)$.

Definizione 2.4.5. Sia V uno spazio vettoriale su un campo $\mathbb{K}$ e siano

$$v_1, \ldots, v_k \in V$$

vettori di V. Diremo che $v_1, \ldots, v_k$ **generano** V se

$$V = \mathrm{Span}\,(v_1, \ldots, v_k),$$

e quindi per ogni vettore $v \in V$ esistono dei coefficienti $\lambda_1, \ldots, \lambda_k$ tali che

$$v = \lambda_1\, v_1 + \cdots + \lambda_k\, v_k.$$

In questo caso V si dirà **finitamente generato**.

2.5 Dipendenza e indipendenza lineare

Definizione 2.5.1. Siano $v_1, \ldots, v_k \in V$; essi si dicono **linearmente dipendenti** se uno di loro si può scrivere come combinazione lineare degli altri.

Esempio 2.5.2. I vettori di $\mathbb{R}^2$

$$v_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix},\ v_2 \begin{pmatrix} 1 \\ 2 \end{pmatrix},\ v_3 = \begin{pmatrix} 3 \\ 4 \end{pmatrix}$$

sono linearmente dipendenti, perché $v_3 = 2v_1 + v_2$, ma v_1 e v_2 non sono linearmente dipendenti, e nemmeno v_1 e v_3, così come v_2 e v_3 non sono linearmente dipendenti (verificare).

Definizione 2.5.3. Siano $v_1, \ldots, v_k \in V$; essi si dicono **linearmente indipendenti** se non sono linearmente dipendenti.

La dipendenza e l'indipendenza lineari possono essere caratterizzate nel modo seguente, che può essere scelto come definizione alternativa:

Proposizione 2.5.4. *I vettori $v_1, \ldots, v_k \in V$ sono linearmente dipendenti $\iff$ esiste una loro combinazione lineare con coefficienti non tutti nulli che dia il vettore nullo:*

$$a_1v_1 + a_2v_2 + \cdots + a_kv_k = 0, \quad a_i \text{ non tutti nulli.}$$

Conseguentemente abbiamo:

Proposizione 2.5.5. *I vettori $v_1, \dots, v_k \in V$ sono linearmente indipendenti $\iff$ l' unica loro combinazione lineare che dia il vettore nullo è quella con tutti i coefficienti nulli:*

$$a_1 v_1 + a_2 v_2 + \cdots + a_k v_k = 0 \Rightarrow a_1 = a_2 = \cdots = a_k = 0.$$

Osservazione 8.

1. Nel caso $k = 1$, abbiamo che un vettore v_1 è linearmente dipendente $\iff$ esiste una combinazione lineare
$$a_1 v_1 = 0,$$
con $a_1 \neq 0$, cioè $\iff$ $v_1 = 0$ è il vettore nullo.
Conseguentemente, v_1 è linearmente indipendente $\iff$ $v_1 \neq 0$.

2. Due vettori v_1 e v_2 sono linearmente dipendenti $\iff$ esiste $c \in \mathbb{K}$ tale che
$$v_2 = cv_1, \quad \text{oppure } v_1 = cv_2,$$
cioè $\iff$ v_1 e v_2 sono **proporzionali**.
Come conseguenza, due vettori v_1 e v_2 sono linearmente indipendenti $\iff$ non sono proporzionali.

3. Consideriamo dei vettori $v_1, \dots, v_k$ e supponiamo che uno di essi sia nullo:
$$v_i = 0.$$
Allora $v_1, \dots, v_k$ sono linearmente dipendenti; infatti si ha
$$0 \cdot v_1 + \cdots + 1 \cdot v_i + \cdots + 0 \cdot v_k = 0$$
è una loro combinazione lineare con coefficienti non tutti nulli, che dà il vettore nullo.

4. Se tra i vettori $v_1, \dots, v_k$ ce ne sono due uguali
$$v_i = v_j,$$
allora $v_1, \dots, v_k$ sono linearmente dipendenti; infatti, la combinazione lineare
$$0 \cdot v_1 + \cdots + 1 \cdot v_i + \cdots + (-1) v_j + \cdots + 0 \cdot v_k =$$
$$= 0 \cdot v_1 + \cdots + 1 \cdot v_i + \cdots + (-1) v_i + \dots 0 \cdot v_k = 0$$
dà luogo al vettore nullo e non tutti i coefficienti sono nulli.

2.6 Basi

Abbiamo osservato che quando uno dei vettori considerati è combinazione lineare degli altri, esso è irrilevante ai fini dello spazio generato. È quindi naturale cercare di considerare solo insiemi *minimali* di generatori, cioè insiemi in cui togliendo un qualunque vettore, lo spazio generato dai rimanenti è strettamente più piccolo. Queste considerazioni inducono a dare la seguente definizione.

Definizione 2.6.1. Sia V uno spazio vettoriale su un campo $\mathbb{K}$. Un sottoinsieme di vettori

$$\mathcal{B} = \{v_1, \dots, v_n\}$$

si dice **base di** V (finita) se valgono le seguenti:

1. (B1) $v_1, \dots, v_n$ generano V;
2. (B2) $v_1, \dots, v_n$ sono linearmente indipendenti.

Proposizione 2.6.2. *Un sottoinsieme $\{v_1, \dots, v_n\}$ di V è una base di V se e solo se per ogni ettore $v \in V$, esistono e sono unici dei coefficienti $\lambda_1, \dots, \lambda_n$ tali che*

$$v = \lambda_1 v_1 + \cdots + \lambda_n v_n.$$

In tal caso gli scalari $\lambda_1, \dots, \lambda_n$ si chiamano **coordinate di** v **nella base** $\{v_1, \dots, v_n\}$.

Dimostrazione. Sia $\{v_1, \dots, v_n\}$ una base di V. Poiché sono dei generatori di V, ogni vettore $v \in V$ si può scrivere come combinazione lineare

$$v = \lambda_1 v_1 + \cdots + \lambda_n v_n.$$

Supponiamo che si abbia anche

$$v = \mu_1 v_1 + \cdots + \mu_n v_n.$$

Sottraendo la seconda equazione alla prima otteniamo

$$0 = (\lambda_1 - \mu_1) v_1 + \cdots + (\lambda_n - \mu_n) v_n.$$

Essendo $\{v_1, \dots, v_n\}$ una base, i vettori sono anche linearmente indipendenti, quindi si ha

$$\lambda_1 = \mu_1, \dots, \lambda_n = \mu_n,$$

da cui la tesi.

Viceversa, supponiamo che ogni vettore di V si possa esprimere in modo unico nella forma

$$v = \lambda_1 v_1 + \cdots + \lambda_n v_n.$$

Da ciò segue, in particolare, che i vettori $\{v_1, \dots, v_n\}$ formano un insieme di generatori di V.

Mostriamo infine che sono linearmente indipendenti. Consideriamo una loro combinazione lineare che dia il vettore nullo:

$$c_1 v_1 + \cdots + c_n v_n = 0.$$

Siccome il vettore nullo ammette la rappresentazione

$$0 = 0 \cdot v_1 + \cdots + 0 \cdot v_n,$$

per l'ipotesi di unicità della rappresentazione di ogni vettore come combinazione lineare dei vettori $\{v_1, \dots, v_n\}$, si ha che necessariamente

$$c_1 = 0, \dots, c_n = 0,$$

quindi $v_1, \dots, v_n$ sono anche linearmente indipendenti, e formano una base. □

Esempio 2.6.3. Sia $V = \mathbb{K}^n$. Allora si ha una base naturale, detta **base canonica $\mathcal{E}$ di $\mathbb{K}^n$:**

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \; e_2 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \; \ldots, e_n = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}.$$

Infatti, i vettori di $\mathcal{E}$ formano un insieme di generatori; dato un vettore

$$v = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$$

arbitrario, esso si esprime come combinazione lineare nel modo seguente:

$$\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = b_1 \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + b_2 \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} + \cdots + b_n \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}.$$

Inoltre, si può verificare facilmente che i vettori di $\mathcal{E}$ sono linearmente indipendenti.

Osservazione 9. Sottolineiamo nell' esempio precedente che nella base canonica $\mathcal{E}$ di $\mathbb{K}^n$ le **coordinate di un vettore coincidono con le sue componenti**.

Capitolo 3

Matrici

3.1 Matrici: prime definizioni

Definizione 3.1.1. Siano $m, n \in \mathbb{N}$ e sia mK un campo. Una **matrice** $m \times n$ **a coefficienti in** $\mathbb{K}$ è una tabella rettangolare di $m \cdot n$ elementi di $\mathbb{K}$ del tipo

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix},$$

dove $a_{ij} \in \mathbb{K}$ per ogni $i \in \{1, \dots, m\}$ e per ogni $j \in \{1, \dots, n\}$.

Verrá usate anche la seguente notazione per denotare una matrice:

$$A = (a_{ij})_{1 \leq i \leq m, 1 \leq j \leq n}.$$

Per ogni $i = 1, \dots, m$, la **riga** i**-esima** di A è la matrice $1 \times n$

$$A_{(i)} = (a_{i1}\ a_{i2}\ \dots a_{in}).$$

Per ogni $j = 1, \dots, n$, la **colonna** j**-esima** di A è la matrice $m \times 1$

$$A^{(j)} = \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{pmatrix}$$

L'elemento a_{ij} è detto **elemento di posto** i, j; tale elemento verrà indicato anche con

$$(A)_{ij}.$$

Osserviamo, infine, che i è l'indice di riga e j l'indice di colonna.

Definizione 3.1.2. Se $m = n$, cioè il numero di righe è uguale al numero di colonne, la matrice si dice **matrice quadrata di ordine** n.

Definizione 3.1.3. L'insieme di tutte le matrici $m \times n$ a coefficienti in $\mathbb{K}$ si denota con $M_{m,n}(\mathbb{K})$. L'insieme delle matrici quadrate di ordine n a coefficienti in $\mathbb{K}$ si denota con $M_n(\mathbb{K})$.

Definizione 3.1.4. Siano $A = (a_{ij}), B = (b_{ij}) \in M_{m,n}(\mathbb{K})$, e sia $c \in \mathbb{K}$. La **somma** di A e B si definisce come la matrice $A + B \in M_{m,n}(\mathbb{K})$ il cui elemento di posto i, j è $a_{ij} + b_{ij}$ per ogni $i \in \{1, \dots, m\}$ e $j \in \{1, \dots, n\}$; possiamo scrivere:

$$(A + B)_{ij} = (A)_{ij} + (B)_{ij}.$$

Il **prodotto di** A **per lo scalare** c è la matrice $c \cdot A \in M_{m,n}(\mathbb{K})$ il cui elemento di posto i, j è dato da $c \cdot a_{ij}$, per ogni $i \in \{1, \dots, m\}$ e $j \in \{1, \dots, n\}$.

Proposizione 3.1.5. *$M_{m,n}(\mathbb{K})$ con le operazioni di somma e prodotto per scalari definite sopra, è uno spazio vettoriale sul campo $\mathbb{K}$. Il vettore nullo è la matrice nulla, cioè la matrice con $0 \in \mathbb{K}$ al posto i, j, per ogni $i \in \{1, \dots, m\}$ e $j \in \{1, \dots, n\}$.*

Dimostrazione. Esercizio. □

Esempio 3.1.6. Una base per lo spazio vettoriale delle matrici $M_{m,n}(\mathbb{K})$ è data da

$$E_{11} := \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}, \; E_{12} := \begin{pmatrix} 0 & 1 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}, \; \dots, E_{mn} := \begin{pmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix},$$

ovvero dalle matrici E_{ij} che hanno il coefficiente 1 nella posizione i, j e zero altrove.

Infatti, ogni matrice $A = (a_{ij})$ si può scrivere in modo unico come

$$A = a_{11}E_{11} + a_{12}E_{12} + \dots + a_{mn}E_{mn} = \sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij}E_{ij}.$$

Anche questa base viene detta **base canonica dello spazio delle matrici**.

Osservazione 10. Analogamente agli spazi $\mathbb{R}^n$ possiamo definire gli spazi

$$\mathbb{K}^n = \left\{ \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix} \mid c_1, c_2, \dots, c_n \in \mathbb{K} \right\},$$

detto **prodotto cartesiano** del campo $\mathbb{K}$ per se stesso n volte. I suoi elementi sono sequenze ordinate di n scalari di $\mathbb{K}$.

Come nel caso reale, in $\mathbb{K}^n$ possiamo definire una somma e una moltiplicazione per uno scalare, che lo rendono uno spazio vettoriale su $\mathbb{K}$:

$$\begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix} + \begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_n \end{pmatrix} = \begin{pmatrix} c_1 + d_1 \\ c_2 + d_2 \\ \vdots \\ c_n + d_n \end{pmatrix},$$

$$a \cdot \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix} = \begin{pmatrix} a\, c_1 \\ a\, c_2 \\ \vdots \\ a\, c_n \end{pmatrix}$$

Osservazione 11. Possiamo vedere gli elementi di $\mathbb{K}^n$ come matrici $n \times 1$ a coefficienti in $\mathbb{K}$. Sotto questa identificazione, le operazioni di somma e prodotto per scalari definite in $\mathbb{K}^n$ coincidono con quelle di $M_{n,1}(\mathbb{K})$, quindi possiamo identificare

$$\mathbb{K}^n = M_{n,1}(\mathbb{K})$$

come spazi vettoriali.

3.2 Matrice trasposta

Definizione 3.2.1. Sia $A \in M_{m,n}(\mathbb{K})$. La **matrice trasposta di** A è la matrice

$${}^tA \in M_{n,m}(\mathbb{K})$$

il cui elemento di posto i, j è l'elemento di posto j, i di A, per ogni $i \in \{1, \dots, n\}$ e $j \in \{1, \dots, m\}$, ovvero:

$$({}^tA)_{ij} = (A)_{ji}.$$

Proposizione 3.2.2. *Siano $A, B \in M_{m,n}(\mathbb{K})$. Allora si ha:*

1. ${}^t(A + B) = {}^tA + {}^tB$;
2. ${}^t({}^tA) = A$.

Dimostrazione. 1. Dimostriamo che per ogni $i \in \{1, \dots, m\}$ e per ogni $j \in \{1, \dots, n\}$, gli elementi di posto i, j di ${}^t(A + B)$ e di ${}^tA + {}^tB$ coincidono; si ha:

$$({}^t(A + B))_{ij} = (A + B)_{ji} = (A)_{ji} + (B)_{ji};$$

inoltre:

$$({}^tA + {}^tB)_{ij} = ({}^tA)_{ij} + ({}^tB)_{ij} = (A)_{ji} + (B)_{ji},$$

quindi l'uguaglianza della tesi vale.

2. Si ha

$$({}^t({}^tA))_{ij} = ({}^tA)_{ji} = (A)_{ij},$$

quindi l'uguaglianza è verificata.

□

Definizione 3.2.3. Sia $A = (a_{ij}) \in M_n(\mathbb{K})$. La **diagonale principale** è quella parte di A composta dagli elementi di posto i, i, per ogni $i = 1, \dots, n$.

A è detta **diagonale** se $a_{ij} = 0$ per ogni $i \neq j$.

A è **simmetrica** se $A = {}^tA$.

La **matrice unità** $n \times n$è la matrice $\mathbb{I}_n \in M_n(\mathbb{K})$ il cui elemento di posto i, j è dato da 1 se $i = j$ e 0 se $i \neq j$. Useremo spesso il **simbolo di Kronecker** δ_{ij} così definito:

$$\delta_{ij} := \begin{cases} 1 \text{ se } i = j \\ 0 \text{ se } i \neq j \end{cases}$$

La matrice unità ha quindi al posto i, j l'elemento δ_{ij}.

3.3 Il prodotto righe per colonne

Definizione 3.3.1. Siano

$$A = (a_{11}\ a_{12} \dots a_{1n}) \in M_{1,n}(\mathbb{K}), \quad B = \begin{pmatrix} b_{11} \\ b_{21} \\ \vdots \\ b_{n1} \end{pmatrix} \in M_{n,1}(\mathbb{K}).$$

Il **prodotto** $A \cdot B$ è lo scalare definito come segue:

$$A \cdot B = a_{11}b_{11} + a_{12}b_{21} + \cdots + a_{1n}b_{n1} \in \mathbb{K}.$$

Più in generale, se $A \in M_{m,n}(\mathbb{K})$ e $B \in M_{n,p}(\mathbb{K})$, il **prodotto righe per colonne**

$$A \cdot B \in M_{m,p}(\mathbb{K})$$

è quella matrice $m \times p$ il cui elemento di posto i, j è dato dal prodotto della i-esima riga di A e la j-esima colonna di B:

$$(A \cdot B)_{ij} = A_{(i)} \cdot B^{(j)} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj}.$$

Notiamo che nel prodotto righe per colonne, il numero delle colonne della matrice a sinistra A deve coincidere con il numero delle righe della matrice a destra B.

Osservazione 12. Osserviamo che se A e B sono matrici quadrate dello stesso ordine:

$$A, B \in M_n(\mathbb{K}),$$

è sempre possibile moltiplicare $A \cdot B$, ma in generale si ha $A \cdot B \neq B \cdot A$; si vedano gli esercizi assegnati per esempi e controesempi.

Proposizione 3.3.2. *1. Siano $A, B \in M_{m,n}(\mathbb{K})$, $C, D \in M_{n,p}(\mathbb{K})$, $c \in \mathbb{K}$. Allora valgono le seguenti uguaglianze:*

$$(A + B) \cdot C = A \cdot C + B \cdot C, \quad A \cdot (C + D) = A \cdot C + A \cdot D,$$

$$A \cdot (c \cdot C) = c \cdot (A \cdot C) = (c \cdot A) \cdot C, \quad A \cdot \mathbb{I}_n = \mathbb{I}_m \cdot A = A.$$

2. Siano $A \in M_{m,n}(\mathbb{K})$, $B \in M_{n,p}(\mathbb{K})$, $C \in M_{p,q}(\mathbb{K})$. Allora vale la seguente uguaglianza:

$$(A \cdot B) \cdot C = A \cdot (B \cdot C).$$

3. *Siano* $A \in M_{m,n}(\mathbb{K}), \quad B \in M_{n,p}(\mathbb{K})$. *Allora vale la seguente uguaglianza:*

$$^t(A \cdot B) =^t B \cdot {}^t A.$$

Dimostrazione. Dimostriamo solo l'uguaglianza 3). Si ha

$$(^t(A \cdot B))_{ij} = (A \cdot B)_{ji} = A_{(j)} \cdot B^{(i)} =$$

$$= a_{j1}b_{1i} + a_{j2}b_{2i} + \cdots + a_{jn}b_{ni}.$$

D'altra parte si ha

$$(^tB \cdot {}^t A)_{ij} = (^tB)_{(i)} \cdot (^tA)^{(j)} = b_{1i}a_{j1} + b_{2i}a_{j2} + \cdots + b_{ni}a_{jn} = a_{j1}b_{1i} + a_{j2}b_{2i} + \cdots + a_{jn}b_{ni}.$$

□

3.4 Matrice inversa

Definizione 3.4.1. Una matrice quadrata $A \in M_n(\mathbb{K})$ si dice invertibile, se esiste una matrice quadrata dello stesso ordine $M \in M_n(\mathbb{K})$ tale che sono verificate le seguenti uguaglianze:

$$A \cdot M = M \cdot A = \mathbb{I}_n.$$

Proposizione 3.4.2. *Sia data una matrice quadrata* $A \in M_n(\mathbb{K})$.

1. *Se A è invertibile, allora esiste un' unica matrice* $M \in M_n(\mathbb{K})$, *tale che* $A \cdot M = M \cdot A = \mathbb{I}_n$. *Tale M si dice* **matrice inversa di** *A e si indica con* A^{-1}.

2. *Se A è invertibile e* $M \in M_n(\mathbb{K})$ *è tale che*

   $$A \cdot M = \mathbb{I}_n,$$

   allora $M = A^{-1}$.

   Lo stesso vale se $M \cdot A = \mathbb{I}_n$.

3. *Se* $A, B \in M_n(\mathbb{K})$ *sono invertibili, allora anche* $A \cdot B$ *è invertibile, e*

   $$(A \cdot B)^{-1} = B^{-1} \cdot A^{-1}.$$

Dimostrazione. 1. Se esistesse un' altra $N \in M_n(\mathbb{K})$ tale che $A \cdot N = N \cdot A = \mathbb{I}_n$. Allora sfruttando il fatto che $N \cdot \mathbb{I}_n = N$, che $\mathbb{I}_n = A \cdot M$, la proprietà associativa del prodotto righe per colonne, e che $\mathbb{I}_n \cdot M = M$, abbiamo:

$$N = N \cdot \mathbb{I}_n = N \cdot (A \cdot M) = (N \cdot A) \cdot M = \mathbb{I}_n \cdot M = M,$$

quindi le due matrici sono uguali.

2. Dobbiamo dimostrare che anche $M \cdot A = \mathbb{I}_n$. Ma siccome A è invertibile, esiste la sua inversa A^{-1}. Quindi

$$M \cdot A = \mathbb{I}_n \cdot M \cdot A = (A^{-1} \cdot A) \cdot M \cdot A = A^{-1} \cdot (A \cdot M) \cdot A = A^{-1} \cdot \mathbb{I}_n \cdot A = A^{-1} \cdot A = \mathbb{I}_n.$$

3. È sufficiente osservare che

$$(A \cdot B) \cdot B^{-1} \cdot A^{-1} = A \cdot (B \cdot B^{-1}) \cdot A^{-1} = A \cdot A^{-1} = \mathbb{I}_n,$$

e che $B^{-1} \cdot A^{-1} \cdot (A \cdot B) = \mathbb{I}_n$.

□

Osservazione 13. Notiamo che $A \neq 0$ non implica che A sia invertibile. Si consideri ad esempio la matrice

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Osserviamo che A non è invertibile. Infatti, se esistesse

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

tale che $A \cdot M = \mathbb{I}_2$, allora si avrebbe

$$\begin{cases} a + b = & 1 \\ a + b = & 0 \\ c + d = & 0 \\ c + d = & 1, \end{cases}$$

ma il sistema non ha soluzione.

Capitolo 4

Sistemi lineari

4.1 Sistemi di equazioni lineari

Siano $m, n \in \mathbb{N} \setminus \{0\}$, e sia $\mathbb{K}$ un campo.

Definizione 4.1.1.

- Un **sistema di m equazioni lineari a coefficienti in $\mathbb{K}$ in n incognite** è un sistema di equazioni della seguente forma:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n & = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n & = b_2 \\ \dots & \dots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n & = b_m, \end{cases}$$

  dove $a_{11}, a_{12}, \dots, a_{mn} \in \mathbb{K}$ sono i **coefficienti**, $x_1, \dots, x_n$ sono le **incognite**, n è l' **ordine**, $b_1, \dots, b_m \in \mathbb{K}$ sono i **termini noti**, del sistema lineare.

- Una **soluzione** del sistema lineare è una n-upla ordinata (vettore colonna)

$$s = \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{pmatrix} \in \mathbb{K}^n$$

  tale che, se si sostituisce ad x_i il valore $s_i \in \mathbb{K}$, per ogni $i = 1, \dots, n$, le m equazioni sono simultaneamente soddisfatte.

- Il sistema lineare si dice **omogeneo**, rispettivamente **non omogeneo**, se

$$b_1 = b_2 = \cdots = b_m = 0,$$

  rispettivamente se $b_j \neq 0$, per qualche $j = 1, \dots, m$.

- Il sistema lineare si dice **compatibile** (rispettivamente **incompatibile**), se possiede una soluzione (rispettivamente, se non ha alcuna soluzione).

Osservazione 14. Ogni sistema lineare omogeneo è compatibile, infatti il vettore nullo

$$0 = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \in \mathbb{K}^n$$

è una sua soluzione, detta soluzione banale. Ogni altra soluzione si dice soluzione non banale.

Esempio 4.1.2. 1. Il sistema lineare di ordine 2

$$\begin{cases} 2x_1 + 3x_2 = 1 \\ 2x_1 + 3x_2 = 2 \end{cases}$$

è incompatibile.

2. Il sistema lineare

$$\begin{cases} 2x_1 + 3x_2 = 1 \\ x_1 + x_2 = 0 \end{cases}$$

è compatibile ed ammette l'unica soluzione $s = \begin{pmatrix} -1 \\ 1 \end{pmatrix}$.

3. Il sistema lineare

$$\begin{cases} 2x_1 + 3x_2 = 1 \\ 4x_1 + 6x_2 = 2 \end{cases}$$

è compatibile ed ammette infinite soluzioni date da $s = \begin{pmatrix} \frac{1-3t}{2} \\ t \end{pmatrix}$; per ogni valore di $t \in \mathbb{R}$, otteiamo una soluzione del sistema.

Definizione 4.1.3. La **matrice dei coefficienti** del sistema lineare

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \cdots \qquad\qquad\qquad\qquad\quad \cdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m, \end{cases}$$

è la matrice A di tipo $m \times n$ a coefficienti in $\mathbb{K}$, il cui elemento di posto ij è il coefficiente a_{ij} del sistema lineare, per ogni $i = 1, \ldots, m$, $j = 1, \ldots, n$, cioè

$$A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ldots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix}.$$

Il **vettore dei termini noti** è il vettore colonna

$$b = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}.$$

Osserviamo che se mettiamo le incognite in colonna

$$X := \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix},$$

allora il precedente sistema lineare si può scrivere nella seguente forma:

$$A \cdot X = b,$$

dove A è la matrice dei coefficienti, b il vettore dei termini noti, ed il prodotto è il prodotto righe per colonne.

La **matrice completa** associata al precedente sistema lineare è la matrice

$$(A|b) = \left(\begin{array}{cccc|c} a_{11} & a_{12} & \dots & a_{1n} & b_1 \\ a_{21} & a_{22} & \dots & a_{2n} & b_2 \\ \vdots & \vdots & \dots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} & b_m \end{array}\right).$$

Teorema 4.1.4. di struttura per le soluzioni dei sistemi lineari omogenei *Sia $A \cdot X = 0$ un sistema lineare omogeneo di ordine n a coefficienti in $\mathbb{K}$. Per ogni coppia di soluzioni*

$$s, s' \in \mathbb{K}^n$$

di $A \cdot X = 0$ e per ogni scalare

$$c \in \mathbb{K},$$

si ha che

$$s + s', \quad cs \in \mathbb{K}^n$$

sono soluzioni di $A \cdot X = 0$.

In particolare, l'insieme delle soluzioni del sistema lineare omogeneo $A \cdot X = 0$ è un sottospazio vettoriale di $\mathbb{K}^n$ (per la definizione di sottospazio vettoriale si veda il prossimo capitolo).

Dimostrazione. Siccome $s, s' \in \mathbb{K}^n$ sono soluzioni del sistema lineare omogeneo in considerazione, si ha che $A \cdot s = 0$ ed $A \cdot s' = 0$. Dobbiamo provare che $A \cdot (s + s') = 0$ e che $A \cdot (cs) = 0$.

Per la proprietà distributiva del prodotto righe per colonne sulla somma di matrici (in questo caso s, s' sono vettori colonna, quindi si possono considerare come matrici di tipo $n \times 1$), si ha che

$$A \cdot (s + s') = A \cdot s + A \cdot s' = 0 + 0 = 0.$$

Segue che $s + s' \in \mathbb{K}^n$ è una soluzione del sistema lineare omogeneo.

Per dimostrare che $A \cdot (cs) = 0$, basta osservare che il prodotto per scalari commuta con il prodotto tra matrici, quindi

$$A \cdot (cs) = cA \cdot s = c0 = 0.$$

□

Teorema 4.1.5. di struttura per le soluzioni dei sistemi lineari *Sia $A \cdot X = b$ un sistema lineare di ordine n, e sia $\widetilde{s} \in \mathbb{K}^n$ una sua soluzione.*

Allora $s \in \mathbb{K}^n$ è soluzione del sistema lineare, se e solo se

$$s = \widetilde{s} + s_0,$$

dove $s_0 \in \mathbb{K}^n$ è una soluzione del sistema lineare omogeneo associato $A \cdot X = 0$.

Dimostrazione. Sia $s \in \mathbb{K}^n$ una soluzione arbitraria del sistema lineare $A \cdot X = b$. Osserviamo che

$$s = \widetilde{s} + (s - \widetilde{s}),$$

quindi basta verificare che $s - \widetilde{s}$ è soluzione del sistema lineare omogeneo associato $A \cdot X = 0$. Sfruttando la proprietà distributiva del prodotto righe per colonne tra matrici si ha

$$A \cdot (s - \widetilde{s}) = A \cdot s + A \cdot (-\widetilde{s}) = A \cdot s - A \cdot (\widetilde{s}) = b - b = 0,$$

dove nella seconda uguaglianza abbiamo sfruttato il fatto che $-\widetilde{s} = (-1)\widetilde{s}$ e la commutatività del prodotto righe per colonne con il prodotto per scalari.

Viceversa, per ogni soluzione $s_0 \in \mathbb{K}^n$ del sistema lineare omogeneo associato, $\widetilde{s} + s_0$ è una soluzione del sistema lineare, poiché

$$A \cdot (\widetilde{s} + s_0) = A \cdot \widetilde{s} + A \cdot s_0 = b + 0 = b.$$

□

4.2 Sistemi lineari con matrici dei coefficienti a scala

Definizione 4.2.1. Sia $A = (a_{ij}) \in M_{m,n}(\mathbb{K})$ e sia $r \in \{0, 1, \dots, m\}$ il numero delle righe di A diverse dalla riga nulla. La matrice A è detta **a scala** se:

- $r = 0$ (quindi A è la matrice nulla),
- oppure $r > 0$, $A_{(i)} \neq (0\ 0 \dots 0)$ per ogni $i \in \{1, \dots, r\}$ e, posto

  $$j_i = \min\{j \mid a_{ij} \neq 0\},$$

  si ha che $j_1 < j_2 < \cdots < j_r$.

  Se A è a scala, gli elementi $a_{1j_1}, \dots, a_{rj_r}$ si dicono i **pivot** di A.

Proposizione 4.2.2. *Sia $A \cdot X = b$ un sistema lineare di ordine n, formato da m equazioni, a coefficienti in $\mathbb{K}$. Supponiamo che $A \in M_{m,n}(\mathbb{K})$ sia una matrice a scala, e sia $r \in 0, \dots, m$ il numero di righe non nulle di A.*

Allora il sistema lineare $A \cdot X = b$ è compatibile $\iff$

$$b_{r+1} = b_{r+2} = \cdots = b_m = 0.$$

Dimostrazione. Dimostriamo l' implicazione $\Rightarrow$:

Per ipotesi il sistema lineare $A \cdot X = b$ è compatibile, quindi ha una soluzione

$$s = \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{pmatrix}$$

per cui vale $A \cdot s = b$. In particolare, per ogni $i = 1, \ldots, m$, la componente i-esima del vettore $A \cdot s \in \mathbb{K}^n$ è data dal prodotto (righe per colonne) della i-esima riga di A per s, cioè $A_{(i)} \cdot s$.

Sia ora $i > r$; per definizione di r abbiamo che

$$A_{(i)} \cdot s = 0,$$

perció $b_i = 0$.

Implicazione $\Leftarrow$:

Supponiamo che $b_i = 0$ per ogni $i > r$, e dimostriamo che è sempre possibile trovare una soluzione del sistema lineare $A \cdot X = b$. A tale scopo, procediamo risolvendo tutte le equazioni partendo dall' ultima equazione ed andando a ritroso.

Precisamente, le equazioni dalla $(r+1)$-esima alla m-esima sono tutte del tipo $0 = 0$, quindi sono soddisfatte per ogni scelta di $s_1, \ldots, s_n \in \mathbb{K}$,ponendo $x_1 = s_1, \ldots, x_n = s_n$. L' equazione r-esima è della forma seguente:

$$a_{r,j_r} x_{j_r} + a_{r,j_r+1} x_{j_r+1} + \cdots + a_{r,n} x_n = b_r.$$

Siccome $a_{r,j_r} \neq 0$, essendo l' r-esimo pivot di A, possiamo ricavare x_{j_r} in funzione di $x_{j_r+1}, x_{j_r+2}, \ldots, x_n$, ed otteniamo:

$$x_{j_r} = \frac{1}{a_{r,j_r}}(b_r - a_{r,j_r+1} x_{j_r+1} - \cdots - a_{r,n} x_n).$$

Quindi, per ogni $s_1, \ldots, s_{j_r-1} \in \mathbb{K}$ e per ogni $s_{j_r+1}, \ldots, s_n \in \mathbb{K}$, otteniamo una soluzione della equazione r-esima del sistema lineare ponendo

$$x_1 = s_1, \ldots, x_{j_r-1} = s_{j_r-1}, \ldots, x_n = s_n \in \mathbb{K}, x_{j_r} = \frac{1}{a_{r,j_r}}(b_r - a_{r,j_r+1} s_{j_r+1} - \cdots - a_{r,n} s_n).$$

Ora consideriamo l' equazione $(r-1)$-esima. Essa è della forma seguente:

$$a_{r-1,j_{r-1}} x_{j_{r-1}} + a_{r-1,j_{r-1}+1} x_{j_{r-1}+1} + \cdots + a_{r-1,n} x_n = b_{r-1}.$$

Dividendo ambo i membri per $a_{r-1,j_{r-1}}$, che è $\neq 0$, ricaviamo $x_{j_{r-1}}$ in funzione di $x_{j_{r-1}+1}, \ldots, x_n$. Quindi, sostituendo ad x_{j_r} il valore determinanto in precedenza, vediamo che è possibile trovare degli scalari $s_1, s_2, \ldots, s_n \in \mathbb{K}$, tali che $s = \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{pmatrix} \in \mathbb{K}^n$ sia simultaneamente soluzione delle equazioni dalla $(r-1)$-esima alla m-esima del sistema lineare. Procedendo in questo modo vediamo che il sistema lineare $A \cdot X = b$ ha (almeno) una soluzione e quindi è compatibile.

□

4.3 Il metodo di gradinizzazione di Gauß

Definizione 4.3.1. Due sistemi lineari dello stesso ordine sono **equivalenti** se hanno le stesse soluzioni.

Il metodo di Gau_ per stabilire la compatibilità ed eventualmente per trovare le soluzioni di un sistema lineare $A \cdot X = b$, consiste nel trasformare tale sistema in uno ad esso equivalente $\widetilde{A} \cdot X = \widetilde{b}$, con matrice dei coefficienti $\widetilde{A}$ a scala. Quindi si stabilisce la compatibilità di $\widetilde{A} \cdot X = \widetilde{b}$, ed eventualmente se ne trovano le soluzioni, tramite la Proposizione 4.2.2. Per trasformare $A \cdot X = b$ in $\widetilde{A} \cdot X = \widetilde{b}$ si effettuano in modo opportuno le cosiddette **operazioni elementari**.

1. OE1 **Operazione elementare 1 (OE1)**. Questa operazione consiste nello scambio di due equazioni tra di loro. Nella pratica, per risolvere un dato sistema lineare, sarà spesso più comodo effettuare le operazioni elementari direttamente sulla matrice completa $(A \mid b)$. In tal caso la OE1 consiste nello scambio di due righe di $(A \mid b)$ tra di loro.
2. OE2 **Operazione elementare 2 (OE2)**. Questa operazione consiste nella moltiplicazione di ambo i membri di una equazione per uno stesso scalare non nullo. La corrispondente operazione sulla matrice completa $(A \mid b)$ consiste nella moltiplicazione di una sua riga per uno scalare non nullo.
3. OE3 **Operazione elementare 3 (OE3)**. Con questa operazione si sostituisce una equazione con l' equazione che si ottiene sommando ad essa un multiplo di un' altra equazione. La corrispondente operazione sulla matrice completa $(A \mid b)$ consiste nel sostituire una sua riga, ad esempio $(A \mid b)_{(i)}$, con la somma $(A \mid b)_{(i)} + c(A \mid b)_{(j)}$, per qualche $j \neq i$ e $c \in \mathbb{K}$.

Proposizione 4.3.2. *Le operazioni elementari 1, 2 e 3 trasformano un dato sistema lineare in uno ad esso equivalente.*

Dimostrazione. Sia $A \cdot X = b$ un dato sistema lineare di ordine n, con m equazioni, a coefficienti in $\mathbb{K}$. Chiaramente scambiando l' ordine delle sue equazioni, si ottiene un sistema lineare equivalente ad esso. Lo stesso vale se si moltiplica ambo i membri di una equazione per uno scalare non nullo.

Consideriamo quindi l' OE3, e precisamente sostituiamo l' equazione i-esima di $A \cdot X = b$ con l' equazione che si ottiene sommando ad essa c-volte l' equazione j-esima, per qualche $c \in \mathbb{K}$ e per qualche $j \neq i$. Denotiamo con $\widetilde{A} \cdot X = \widetilde{b}$ il sistema lineare che si ottiene in questo modo. Ricordiamo che, per ogni $k = 1, \ldots, m$, la k-esima equazione di $A \cdot X = b$ si può scrivere come segue: $A_{(k)} \cdot X = b_k$, dove $A_{(k)}$ è la k-esima riga di A, b_k è la k-esima componente di $b \in \mathbb{K}^m$, ed il prodotto è quello righe per colonne. Analogamente la k-esima equazione di $\widetilde{A} \cdot X = \widetilde{b}$ si scrive come $\widetilde{A}_{(k)} \cdot X = \widetilde{b}_k$, dove

$$\widetilde{A}_{(k)} = \begin{cases} A_{(k)}, & \text{se } k \neq i, \\ A_{(i)} + cA_{(j)}, & \text{se } k = i, \end{cases} \qquad \widetilde{b}_k = \begin{cases} b_k, & \text{se } k \neq i, \\ b_i + cb_j, & \text{se } k = i, \end{cases}$$

Dimostriamo ora che $A \cdot X = b$ e $\widetilde{A} \cdot X = \widetilde{b}$ sono equivalenti. Sia $s \in \mathbb{K}^n$ una soluzione di $A \cdot X = b$; abbiamo quindi

$$A_{(k)} \cdot s = b_k, \ \forall k = 1, \ldots, m.$$

Quindi

$$\widetilde{A}_{(k)} \cdot s = \widetilde{b}_k, \ \forall k \neq i,$$

e per $k = i$

$$\widetilde{A}_{(i)} \cdot s = (A_{(i)} + cA_{(j)}) \cdot s = A_{(i)} \cdot s + cA_{(j)} \cdot s = b_i + cb_j = \widetilde{b}_i.$$

Ne segue che s è soluzione di $\widetilde{A} \cdot X = \widetilde{b}$.

Viceversa, se $s \in \mathbb{K}^n$ è una soluzione di $\widetilde{A} \cdot X = \widetilde{b}$, allora

$$\widetilde{A}_{(k)} \cdot s = \widetilde{b}_k, \ \forall k = 1, \dots, m.$$

Quindi

$$A_{(k)} \cdot s = b_k, \ \forall k \neq i,$$

e per $k = i$

$$A_{(i)} \cdot s = (\widetilde{A}_{(i)} - c\widetilde{A}_{(j)}) \cdot s = \widetilde{A}_{(i)} \cdot s - c\widetilde{A}_{(j)} \cdot s = \widetilde{b}_i - c\widetilde{b}_j = b_i.$$

Ne segue che s è soluzione di $A \cdot X = b$, ed i due sistemi lineari sono equivalenti. □

Teorema 4.3.3. *Sia dato un sistema lineare $A \cdot X = b$. È sempre possibile trasformare $A \cdot X = b$, per mezzo delle operazioni elementari, in uno ad esso equivalente, $\widetilde{A} \cdot X = \widetilde{b}$, con matrice dei coefficienti $\widetilde{A}$ a scala.*

Dimostrazione. Sia n il numero di incognite e sia m il numero delle sue equazioni. Possiamo supporre $A \neq 0$, altrimenti A è già a scala. Sia quindi $j \in \{1, \dots, n\}$ il più piccolo indice di colonna tale che $A^{(j)} \neq 0 \in \mathbb{K}^m$, e sia $i \in \{1, \dots, m\}$ un indice di riga tale che $a_{ij} \neq 0 \in \mathbb{K}$.

ALGORITMO DI GAUß

- Scambiando tra di loro la prima con la i-ma riga di $(A|b)$ (operazione OE1), possiamo supporre che sia

  $$a_{1j} \neq 0.$$

  Abbiamo quindi una matrice del tipo

  $$\left(\begin{array}{ccccccc|c} 0 & \dots & 0 & a_{1j} & a_{1,j+1} & \dots & a_{1n} & b_1 \\ 0 & \dots & 0 & a_{2j} & a_{2,j+1} & \dots & a_{2n} & b_2 \\ \vdots & \dots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots \\ 0 & \dots & 0 & a_{mj} & a_{m,j+1} & \dots & a_{mn} & b_m \end{array}\right)$$

- Per mezzo di una OE3, sostituiamo le righe di $(A|b)$ dalla seconda alla m-esima con

  $$(A|b)_{(k)} - \frac{a_{kj}}{a_{1j}}(A|b)_{(1)}, \ \forall k = 2, \dots, m$$

  e troviamo una matrice del tipo

  $$\left(\begin{array}{ccccccc|c} 0 & \dots & 0 & a_{1j} & a_{1,j+1} & \dots & a_{1n} & b_1 \\ 0 & \dots & 0 & 0 & a'_{2,j+1} & \dots & a'_{2n} & b'_2 \\ \vdots & \dots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots \\ 0 & \dots & 0 & 0 & a'_{m,j+1} & \dots & a'_{mn} & b'_m \end{array}\right)$$

- Applichiamo i punti precedenti alla sottomatrice

  $$\left(\begin{array}{ccccccc|c} 0 & \dots & 0 & a'_{2,j+1} & a'_{2,j+2} & \dots & a'_{2n} & b'_2 \\ \vdots & \dots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots \\ 0 & \dots & 0 & a'_{m,j+1} & a'_{m,j+2} & \dots & a'_{mn} & b'_m \end{array}\right).$$

Alla fine del procedimento troviamo una matrice $(\widetilde{A}|\widetilde{b})$ a scala. □

Osservazione 15. Nel caso in cui $V = \mathbb{K}^n$, possiamo stabilire se k vettori $v_1, \dots, v_k$ sono dei generatori per $\mathbb{K}^n$ studiando un sistema lineare. Più precisamente, se esprimiamo i vettori $v_1, \dots, v_k$ in componenti:

$$v_1 = \begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{n1} \end{pmatrix}, \qquad v_2 = \begin{pmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{n2} \end{pmatrix}, \qquad \dots, \qquad v_k = \begin{pmatrix} a_{1k} \\ a_{2k} \\ \vdots \\ a_{nk} \end{pmatrix},$$

allora un vettore $v = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$ è una loro combinazione lineare se si può scrivere come

$$\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = c_1 \begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{n1} \end{pmatrix} + c_2 \begin{pmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{n2} \end{pmatrix} + \dots + c_k \begin{pmatrix} a_{1k} \\ a_{2k} \\ \vdots \\ a_{nk} \end{pmatrix} = \begin{pmatrix} c_1 a_{11} + c_2 a_{12} + \dots + c_k a_{1k} \\ c_1 a_{21} + c_2 a_{22} + \dots + c_k a_{2k} \\ \vdots \\ c_1 a_{n1} + c_2 a_{n2} + \dots + c_k a_{nk} \end{pmatrix} =$$

$$= \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1k} \\ a_{21} & a_{22} & \dots & a_{2k} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nk} \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_k \end{pmatrix}.$$

Se poniamo

$$A := \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1k} \\ a_{21} & a_{22} & \dots & a_{2k} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nk} \end{pmatrix},$$

abbiamo che v è combinazione lineare di $v_1, \dots, v_k$ se e solo se il sistema lineare

$$A \cdot X = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$$

ammette almeno una soluzione $\begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_k \end{pmatrix}$, cioè se e solo se $A \cdot X = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$ è compatibile.

Osservazione 16. Nel caso in cui $V = \mathbb{K}^n$, possiamo stabilire se k vettori $v_1, \dots, v_k$ sono linearmente dipendenti studiando un sistema omogeneo di equazioni lineari. Più precisamente, se esprimiamo i vettori $v_1, \dots, v_k$ in componenti:

$$v_1 = \begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{n1} \end{pmatrix}, \qquad v_2 = \begin{pmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{n2} \end{pmatrix}, \qquad \dots, \qquad v_k = \begin{pmatrix} a_{1k} \\ a_{2k} \\ \vdots \\ a_{nk} \end{pmatrix},$$

allora una loro combinazione lineare si può scrivere come

$$c_1 \begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{n1} \end{pmatrix} + c_2 \begin{pmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{n2} \end{pmatrix} + \dots + c_k \begin{pmatrix} a_{1k} \\ a_{2k} \\ \vdots \\ a_{nk} \end{pmatrix} = \begin{pmatrix} c_1 a_{11} + c_2 a_{12} + \dots + c_k a_{1k} \\ c_1 a_{21} + c_2 a_{22} + \dots + c_k a_{2k} \\ \vdots \\ c_1 a_{n1} + c_2 a_{n2} + \dots + c_k a_{nk} \end{pmatrix} =$$

$$= \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1k} \\ a_{21} & a_{22} & \dots & a_{2k} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nk} \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_k \end{pmatrix}.$$

Se poniamo

$$A := \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1k} \\ a_{21} & a_{22} & \dots & a_{2k} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nk} \end{pmatrix},$$

abbiamo che $v_1, \dots, v_k$ sono linearmente dipendenti se e solo se il sistema lineare omogeneo

$$A \cdot X = 0$$

ammette una soluzione non banale $\begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_k \end{pmatrix}$.

Infine, possiamo equivalentemente affermare che $v_1, \dots, v_k$ sono linearmente indipendenti se e solo se il sistema lineare omogeneo

$$A \cdot X = 0$$

ammette solo la soluzione banale (la soluzione nulla).

Capitolo 5

Dimensione

5.1 Dimensione di spazi vettoriali

In questa sezione vogliamo definire la dimensione di uno spazio vettoriale finitamente generato. Per questo proposito vediamo un risultato che ci permetterà di dedurre che ogni base di uno spazio vettoriale finitamente generato ha lo stesso numero di elementi.

Lemma 5.1.1. di Steinitz *Sia V uno spazio vettoriale e sia $\{v_1, \dots, v_n\}$ una base di V.*
Allora $\forall p > n$ e per ogni scelta di vettori $w_1, \dots, w_p$, essi sono linearmente dipendenti.

Dimostrazione. I vettori $w_1, \dots, w_p$ si scrivono in modo unico come combinazioni lineari dei vettori della base $\{v_1, \dots, v_n\}$:

$$\begin{aligned} w_1 = &\quad c_{11}v_1 + c_{21}v_2 + \cdots + c_{n1}v_n, \\ w_2 = &\quad c_{12}v_1 + c_{22}v_2 + \cdots + c_{n2}v_n, \\ \vdots &\quad \vdots \\ w_p = &\quad c_{1p}v_1 + c_{2p}v_2 + \cdots + c_{np}v_n. \end{aligned}$$

Denotiamo con $\begin{pmatrix} c_{1i} \\ c_{2i} \\ \vdots \\ c_{ni} \end{pmatrix}$ la colonna delle coordinate di w_i.

Una combinazione lineare $a_1w_1 + a_2w_2 + \cdots + a_pw_p = 0$ dà il vettore nullo se e solo se le coordinate dei vettori w_i soddisfano

$$a_1 \begin{pmatrix} c_{11} \\ c_{21} \\ \vdots \\ c_{n1} \end{pmatrix} + a_2 \begin{pmatrix} c_{12} \\ c_{22} \\ \vdots \\ c_{n2} \end{pmatrix} + \cdots + a_p \begin{pmatrix} c_{1p} \\ c_{2p} \\ \vdots \\ c_{np} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

quindi se e solo se

$$\begin{pmatrix} c_{11} & c_{12} & \dots & c_{1p} \\ c_{21} & c_{22} & \dots & c_{2p} \\ \vdots & \vdots & \vdots & \vdots \\ c_{n1} & c_{n2} & \dots & c_{np} \end{pmatrix} \cdot \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_p \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}. \tag{5.1}$$

Quindi $w_1, \dots, w_p$ sono linearmente dipendenti se e solo se il sistema lineare omogeneo

$$\begin{pmatrix} c_{11} & c_{12} & \dots & c_{1p} \\ c_{21} & c_{22} & \dots & c_{2p} \\ \vdots & \vdots & \vdots & \vdots \\ c_{n1} & c_{n2} & \dots & c_{np} \end{pmatrix} \cdot X = 0$$

di n equationi in p incognite ha una soluzione non nulla.

Per l' ipotesi $p > n$, vediamo che la generica soluzione dipende da almeno $p - n \geq 1$ parametri; fissando per tali parametri dei valori non nulli, si ottiene una soluzione non nulla del sistema lineare omogeneo. □

Come conseguenza si ha il seguente importante risultato.

Teorema 5.1.2. *Sia V uno spazio vettoriale. Se $\{v_1, \dots, v_n\}$ e $\{w_1, \dots, w_m\}$ sono due basi di V, allora*

$$n = m.$$

Dimostrazione. Essendo $\{v_1, \dots, v_n\}$ e $w_1, \dots, w_m$ linearmente indipendenti, per il Lemma 5.1.1 di Steinitz si ha

$$m \leq n.$$

Infatti, se si avesse $m > n$, i vettori $w_1, \dots, w_m$ sarebbero linearmente dipendenti.

Analogamente, essendo $\{w_1, \dots, w_m\}$ una base e $v_1, \dots, v_n$ linearmente indipendenti, si ha

$$n \leq m,$$

da cui la tesi.

□

Definizione 5.1.3. Dato uno spazio vettoriale V, definiamo la **dimensione di** V come segue:

- se $V = \{0\}$, poniamo $\dim V := 0$;
- se $V \neq \{0\}$ e V è finitamente generato, poniamo $\dim V :=$ numero di vettori di una sua qualunque base.

Esempio 5.1.4. Per $V = \mathbb{K}^n$ abbiamo visto che c'è la base canonica $\mathcal{E}$, che consta di n vettori, quindi

$$\dim \mathbb{K}^n = n.$$

Esempio 5.1.5. In $V = M_{m,n}(\mathbb{K})$ c'è la base canonica, che consta di $m \cdot n$ vettori, quindi

$$\dim M_{m,n}(\mathbb{K}) = m \cdot n.$$

Esempio 5.1.6. Consideriamo il campo complesso $\mathbb{C}$. Esso è uno spazio vettoriale su $\mathbb{C}$ stesso, e come tale ha dimensione

$$\dim \mathbb{C} = 1.$$

Osserviamo, pero', che $\mathbb{C}$ si può dotare anche di una struttura di spazio vettoriale su $\mathbb{R}$ come segue:

$$+ : \mathbb{C} \times \mathbb{C} \to \mathbb{C},$$

dove la somma è quella usuale tra numeri complessi, e la moltiplicazione per uno scalare reale è definita da

$$\cdot : \mathbb{R} \times \mathbb{C} \to \mathbb{C}, \quad c \cdot (a + ib) = ac + ibc.$$

Con questa struttura, una base di $\mathbb{C}$ è data da

$$\{1, i\},$$

e quindi

$$\dim_{\mathbb{R}} \mathbb{C} = 2.$$

Vediamo ora che in uno spazio di cui si conosce la dimensione, per individuare una sua base non è necessario verificare sia di avere dei generatori sia l'indipendenza lineare.

Proposizione 5.1.7. *Sia V uno spazio vettoriale di dimensione*

$$\dim V = n.$$

Allora valgono le seguenti:

1. *se $v_1, \ldots, v_n$ sono linearmente indipendenti $\Rightarrow$ $v_1, \ldots, v_n$ formano una base di V; in particolare, sono anche dei generatori per V.*
2. *se $v_1, \ldots, v_n$ sono dei generatori per $V \Rightarrow$ $v_1, \ldots, v_n$ formano una base di V, in particolare sono anche linearmente indipendenti.*

Dimostrazione. 1. Siccome $v_1, \ldots, v_n$ sono linearmente indipendenti, per il Teorema di Completamento si possono completare a una base di V. Essendo $\dim V = n$, ogni base di V ha esattamente n vettori, quindi non è necessario aggiungere alcun vettore all' insieme $\{v_1, \ldots, v_n\}$, che risulta una base. In particolare, $\{v_1, \ldots, v_n\}$ è un insieme di generatori.

2. Se $v_1, \ldots, v_n$ sono un insieme di generatori per V, per il Teorema di Estrazione da essi si può estrarre una base di V. Essendo $\dim V = n$, ogni base di V ha esattamente n vettori, quindi non è necessario scartare alcun vettore dall' insieme $\{v_1, \ldots, v_n\}$, che risulta una base. In particolare, $v_1, \ldots, v_n$ sono linearmente indipendenti.

□

Esempio 5.1.8. In particolare, sapendo che $\dim \mathbb{R}^2 = 2$, per trovare una base di $\mathbb{R}^2$ è sufficiente scegliere 2 vettori linearmente indipendenti, cioè 2 vettori non nulli e non proporzionali.

5.2 Dimensione di sottospazi vettoriali

Sia V uno spazio vettoriale di dimensione finita, e sia $W \subseteq V$ un suo sottospazio vettoriale. In questa sezione daremo una limitazione sulla dimensione di W.

Osservazione 17. Sia $W \subseteq V$ un sottospazio vettoriale di V spazio vettoriale su $\mathbb{K}$, e consideriamo W come spazio vettoriale su $\mathbb{K}$. Se $w_1, \dots, w_k \in W$ sono vettori linearmente indipendenti in $W \Rightarrow w_1, \dots, w_k$ sono linearmente indipendenti anche in V.

Infatti, essendo entrambi W e V spazi vettoriali su $\mathbb{K}$, la condizione di indipendenza lineare come vettori di W o di V è la stessa.

Osservazione 18. Se V è finitamente generato e $W \subseteq V$ è un suo sottospazio vettoriale $\Rightarrow$ anche W è finitamente generato.

Infatti, sia $\dim V = n$, e fissiamo $w_1, \dots, w_k \in W$ vettori linearmente indipendenti in W. Se $W = \mathrm{Span}(w_1, \dots, w_k)$, allora W è finitamente generato.

Se $W \supsetneq \mathrm{Span}(w_1, \dots, w_k)$, allora possiamo scegliere un vettore

$$w_{k+1} \notin \mathrm{Span}(w_1, \dots, w_k), \quad w_{k+1} \in W.$$

Per il Lemma **??**, i vettori $w_1, \dots, w_k, w_{k+1}$ sono linearmente indipendenti. Ripetiamo il procedimento. Siccome per l' Osservazione 17 vettori linearmente indipendenti in W sono anche linearmente indipendenti in V, e siccome in V ci sono al più n vettori linearmente indipendenti per il Lemma 5.1.1 di Steinitz, il procedimento termina dopo un numero finito di passi. Quindi troviamo un numero finito di vettori di W che generano W.

Corollario 5.2.1. *Ogni sottospazio vettoriale W di V, spazio vettoriale finitamente generato, è del tipo*

$$W = \mathrm{Span}(w_1, \dots, w_m)$$

per opportui vettori $w_1, \dots, w_m \in W$.

Proposizione 5.2.2. *Sia V uno spazio vettoriale finitamente generato e sia $W \subseteq V$ un sottospazio vettoriale. Allora valgono:*

1. $\dim W \leq \dim V$;
2. $\dim W = \dim V \iff W = V$.

Dimostrazione. 1. Sia $\{w_1, \dots, w_k\}$ una base di W. I vettori $w_1, \dots, w_k$ sono linearmente indipendenti anche in V, per l' Osservazione 17. Per il Teorema di Completamento, possiamo completare l' insieme $\{w_1, \dots, w_k\}$ a una base $\mathcal{B}$ di V. Quindi si ha

$$\dim W = \#\{w_1, \dots, w_k\} \leq \#\mathcal{B} = n = \dim V.$$

2. Se $W = V$, è chiaro che hanno la stessa dimensione.

   Viceversa, supponiamo $\dim W = \dim V = n$, e fissiamo una base $\{w_1, \dots, w_n\}$ di W. Per l' Osservazione 17 i vettori $w_1, \dots, w_n$ sono linearmente indipendenti anche in V. Infine, essi formano una base di V per la Proposizione 5.1.7, primo punto. Quindi

   $$W = \mathrm{Span}(w_1, \dots, w_n) = V.$$

□

5.3 Formula di Grassmann

In questa sezione vediamo una formula che lega la dimensione di un'intersezione di sottospazi vettoriali con la dimensione del sottospazio somma.

Teorema 5.3.1. Formula di Grassmann *Siano*

$$W_1 \subseteq V, \quad W_2 \subseteq V$$

due sottospazi vettoriali di uno spazio vettoriale finitamente generato V. Allora vale

$$\dim(W_1 \cap W_2) = \dim W_1 + \dim W_2 - \dim(W_1 + W_2). \tag{5.2}$$

Dimostrazione. Fissiamo una base di $W_1 \cap W_2$:

$$\mathcal{B}_{W_1 \cap W_2} = \{w_1, \dots, w_r\}, \quad r = \dim W_1 \cap W_2.$$

Essendo $W_1 \cap W_2 \subseteq W_1$ un sottospazio vettoriale, per il Teorema del Completamento, possiamo completare i vettori $w_1, \dots, w_r$ ad una base di W_1:

$$\mathcal{B}_{W_1} = \{w_1, \dots, w_r, v_1, \dots, v_s\}, \quad r + s = \dim W_1.$$

Analogamente, essendo $W_1 \cap W_2 \subseteq W_2$ un sottospazio vettoriale, per il Teorema del Completamento, possiamo completare i vettori $w_1, \dots, w_r$ ad una base di W_2:

$$\mathcal{B}_{W_2} = \{w_1, \dots, w_r, u_1, \dots, u_k\}, \quad r + k = \dim W_2.$$

Vogliamo dimostrare che

$$\dim(W_1 + W_2) = \dim W_1 + \dim W_2 - \dim(W_1 \cap W_2) = r + s + r + k - r = r + s + k.$$

A tale scopo affermiamo che

$$\mathcal{B}_{W_1} \cup \mathcal{B}_{W_2} = \{w_1, \dots, w_r, v_1, \dots, v_s, u_1, \dots, u_k\}$$

è una base di $W_1 + W_2$.

Infatti, $\{w_1, \dots, w_r, v_1, \dots, v_s, u_1, \dots, u_k\}$ sono dei generatori per $W_1 + W_2$: sia $w \in W_1 + W_2$; per definizione di spazio somma, w si può scrivere nella forma

$$w = z_1 + z_2, \quad z_1 \in W_1, \quad z_2 \in W_2,$$

per opportuni vettori z_1 e z_2. I due vettori, a loro volta, si possono scrivere come combinazioni lineari delle basi di W_1 e W_2, rispettivamente:

$$z_1 = a_1 w_1 + \cdots + a_r w_r + b_1 v_1 + \cdots + b_s v_s, \quad z_2 = c_1 w_1 + \cdots + c_r w_r + d_1 u_1 + \cdots + d_k u_k,$$

e quindi

$$w = (a_1 + c_1) w_1 + \cdots + (a_r + c_r) w_r + b_1 v_1 + \cdots + b_s v_s + d_1 u_1 + \cdots + d_k u_k,$$

cioè ogni vettore di $W_1 + W_2$ è combinazione lineare dei $\{w_1, \dots, w_r, v_1, \dots, v_s, u_1, \dots, u_k\}$.

Mostriamo, infine, che $w_1, \dots, w_r, v_1, \dots, v_s, u_1, \dots, u_k$ sono linearmente indpendenti. Considerimao una loro combinazione lineare che dia il vettore nullo:

$$\alpha_1 w_1 + \cdots + \alpha_r w_r + \beta_1 v_1 + \cdots + \beta_s v_s + \delta_1 u_1 + \cdots + \delta_k u_k = 0. \tag{5.3}$$

Questa relazione può essere riscritta nella forma

$$\alpha_1 w_1 + \cdots + \alpha_r w_r + \beta_1 v_1 + \cdots + \beta_s v_s = -\delta_1 u_1 - \cdots - \delta_k u_k,$$

quindi il vettore $-\delta_1 u_1 - \cdots - \delta_k u_k \in W_2$ è anche combinazione lineare dei vettori della base di W_1, quindi

$$-\delta_1 u_1 - \cdots - \delta_k u_k \in W_1 \cap W_2.$$

Come conseguenza può essere scritto come combinazione lineare dei vettori della base $\mathcal{B}_{W_1 \cap W_2}$:

$$-\delta_1 u_1 - \cdots - \delta_k u_k = \gamma_1 w_1 + \cdots + \gamma_r w_r,$$

da cui

$$\gamma_1 w_1 + \cdots + \gamma_r w_r + \delta_1 u_1 + \cdots + \delta_k u_k = 0.$$

Quest'ultima è una combinazione lineare dei vettori di $\mathcal{B}_{W_2}$, che sono linearmente indipendenti, quindi

$$\gamma_1 = \cdots = \gamma_r = \delta_1 = \cdots = \delta_k = 0.$$

Quindi la relazione (5.3) diventa

$$\alpha_1 w_1 + \cdots + \alpha_r w_r + \beta_1 v_1 + \cdots + \beta_s v_s = 0,$$

che è una combinazione lineare dei vettori di $\mathcal{B}_{W_1}$, che sono linearmente indipendenti, quindi

$$\alpha_1 = \cdots = \alpha_r = \beta_1 = \cdots = \beta_s = 0.$$

□

Corollario 5.3.2. *Siano*

$$W_1 \subseteq V, \quad W_2 \subseteq V$$

due sottospazi vettoriali di uno spazio vettoriale con $\dim V = n$*. Allora vale*

$$\dim(W_1 \cap W_2) \geq \dim W_1 + \dim W_2 - n. \tag{5.4}$$

Dimostrazione. Basta osservare che essendo $W_1 + W_2 \subseteq V$, per la Proposizione 5.2.2, primo punto, si ha

$$\dim W_1 + W_2 \leq n.$$

□

Esempio 5.3.3. In particolare, se W_1 e W_2 sono due piani vettoriali di $\mathbb{R}^3$, abbiamo che

$$\dim(W_1 \cap W_2) \geq 2 + 2 - 3 = 1,$$

cioè due piani vettoriali si intersecano sempre almeno lungo una retta vettoriale.

Capitolo 6

Rango di matrici

6.1 Rango: definizione e prime proprietà

Definizione 6.1.1. Sia $A \in M_{m,n}(\mathbb{K})$ una matrice di tipo $m \times n$ a coefficienti nel campo $\mathbb{K}$. Il **rango** di A è la dimensione del sottospazio vettoriale di $\mathbb{K}^m$ generato dalle colonne di A:

$$\mathrm{rg}(A) := \dim \mathrm{Span}(A^{(1)}, A^{(2)}, \ldots, A^{(n)}), \quad \mathrm{Span}(A^{(1)}, A^{(2)}, \ldots, A^{(n)}) \subseteq \mathbb{K}^m.$$

In diversi libri di testo, il rango definito qui sopra viene chiamato rango per colonne di A, mentre il rango per righe si definisce come la dimensione del sottospazio vettoriale di $\mathbb{K}^n$ generato dalle righe di A, cioè

$$\dim \mathrm{Span}(A_{(1)}, A_{(2)}, \ldots, A_{(m)}), \quad \mathrm{Span}(A_{(1)}, A_{(2)}, \ldots, A_{(m)}) \subseteq \mathbb{K}^n.$$

Osserviamo che il rango per righe di A coincide con il rango della matrice trasposta di A.

Osservazione 19.

1. $\mathrm{rg}(A)$ è uguale al massimo numero di colonne linearmente indipendenti di A.
2. l' inclusione $\mathrm{Span}(A^{(1)}, A^{(2)}, \ldots, A^{(n)}) \subseteq \mathbb{K}^m$ implica in particolare che

   $$\mathrm{rg}(A) \leq m.$$

   Inoltre, siccome $\mathrm{Span}(A^{(1)}, A^{(2)}, \ldots, A^{(n)})$ è generato da n vettori, si ha anche

   $$\mathrm{rg}(A) \leq n.$$

   Quindi

   $$\mathrm{rg}(A) \leq \min\{m, n\}.$$

Esempio 6.1.2.

1. Se A è la matrice nulla: $A = 0$, allora $\mathrm{rg}(A) = 0$. Viceversa, se $\mathrm{rg}(A) = 0$, allora $A = 0$.
2. $\mathrm{rg}(\mathbb{I}_n) = n$. Infatti le colonne della matrice unità sono i vettori della base canonica di $\mathbb{K}^n$:

   $$(\mathbb{I}_n)^{(1)} = e_1, \ldots, (\mathbb{I}_n)^{(n)} = e_n.$$

Proposizione 6.1.3. *Sia $A \in M_{m,n}(\mathbb{K})$, e sia $\widetilde{A}$ una matrice ottenuta da A tramite una sequenza di operazioni elementari. Allora valgono le seguenti affermazioni:*

1. $\mathrm{rg}(A) = \mathrm{rg}(\widetilde{A})$;
2. *se $\widetilde{A}$ è a scala,* $\mathrm{rg}(\widetilde{A})$ *è uguale al numero r delle righe non nulle di $\widetilde{A}$.*
   Inoltre $A^{(j_1)}, \ldots, A^{(j_r)}$ sono linearmente indipendenti, dove $\widetilde{a}_{1,j_1}, \ldots, \widetilde{a}_{r,j_r}$ sono i pivot di $\widetilde{A}$.
3. $\mathrm{rg}({}^tA) = \mathrm{rg}({}^t\widetilde{A})$.
4. $\mathrm{rg}({}^t\widetilde{A}) = \mathrm{rg}(\widetilde{A})$.
5. $\mathrm{rg}(A) = \mathrm{rg}({}^tA)$.

Dimostrazione. 1. Per dimostrare questa affermazione usiamo un risultato che vedremo più avanti, il Teorema di dimensione. Questo teorema afferma che

$$\mathrm{rg}(A) = n - \dim(W), \tag{6.1}$$

dove

$$W = \{s \in \mathbb{K}^n | A \cdot s = 0\}$$

è il sottospazio vettoriale di $\mathbb{K}^n$ formato dalle soluzioni del sistema omogeneo di equazioni lineari

$$A \cdot X = 0.$$

Se $\widetilde{A}$ si ottiene da A per mezzo di operazioni elementari, allora il sistema di equazioni lineari

$$\widetilde{A} \cdot X = 0$$

è equivalente ad $A \cdot X = 0$, cioè $\widetilde{W} = W$, dove $\widetilde{W} = \{s \in \mathbb{K}^n | \widetilde{A} \cdot s = 0\}$ è il sottospazio di $\mathbb{K}^n$ delle soluzioni di $\widetilde{A} \cdot X = 0$. Usando la formula (6.1) abbiamo quindi:

$$\mathrm{rg}(A) = n - \dim(W) = n - \dim(\widetilde{W}) = \mathrm{rg}(\widetilde{A}).$$

2. Supponiamo ora che $\widetilde{A}$ sia a scala, e sia r il numero delle righe non nulle di $\widetilde{A}$. Sia $\widetilde{a}_{ij}$ l' elemento di posto i, j di $\widetilde{A}$. Siccome $\widetilde{A}$ è a scala, si ha che $a_{ij} = 0$, se $i > r$, quindi $\widetilde{A}^{(j)} \in \mathrm{Span}(e_1, \ldots, e_r)$ per ogni $j = 1, \ldots, n$, dove $\widetilde{A}^{(j)}$ è la colonna j-esima di $\widetilde{A}$ ed $e_1, \ldots, e_r$ sono i primi r vettori della base canonica di $\mathbb{K}^n$. Da questo segue che

$$\mathrm{Span}(\widetilde{A}^{(1)}, \ldots, \widetilde{A}^{(n)}) \subseteq \mathrm{Span}(e_1, \ldots, e_r),$$

quindi

$$\mathrm{rg}(\widetilde{A}) = \dim \mathrm{Span}(\widetilde{A}^{(1)}, \ldots, \widetilde{A}^{(n)}) \leq \dim \mathrm{Span}(e_1, \ldots, e_r) = r.$$

Per dimostrare che $\mathrm{rg}(\widetilde{A}) = r$, è sufficiente dimostrare che le colonne

$$\widetilde{A}^{(j_1)}, \ldots, \widetilde{A}^{(j_r)}$$

sono linearmente indipendenti, dove $\widetilde{a}_{1j_1}, \widetilde{a}_{2j_2}, \ldots, \widetilde{a}_{rj_r}$ sono i pivot di $\widetilde{A}$. A tale scopo, consideriamo una combinazione lineare

$$\lambda_1 \widetilde{A}^{(j_1)} + \cdots + \lambda_r \widetilde{A}^{(j_r)} = 0 \tag{6.2}$$

e supponiamo che essa dia il vettore nullo. Osserviamo che il membro sinistro della (6.2) è un vettore della forma seguente:

$$\begin{pmatrix} \lambda_1\widetilde{a}_{1j_1} + \lambda_2\widetilde{a}_{1j_2} + \cdots + \lambda_r\widetilde{a}_{1j_r} \\ \lambda_2\widetilde{a}_{2j_2} + \ldots \lambda_r\widetilde{a}_{2j_r} \\ \vdots \\ \lambda_r\widetilde{a}_{rj_r} \\ 0 \\ \vdots \\ 0 \end{pmatrix}. \tag{6.3}$$

Siccome $\widetilde{a}_{1j_1} \neq 0, \widetilde{a}_{2j_2} \neq 0, \ldots, \widetilde{a}_{rj_r} \neq 0$, il vettore (6.3) è nullo se e solo se $\lambda_r = \lambda_{r-1} = \cdots = \lambda_1 = 0$. Concludiamo quindi che le colonne $\widetilde{A}^{(j_1)}, \ldots, \widetilde{A}^{(j_r)}$ sono linearmente indipendenti e $\mathrm{rg}(\widetilde{A}) = r$.

Dimostriamo ora che le colonne $A^{(j_1)}, \ldots, A^{(j_r)}$ di A, sono linearmente indipendenti, dove $j_1, j_2, \ldots, j_r$ sono gli indici di colonna dei pivot $\widetilde{a}_{1j_1}, \widetilde{a}_{2j_2}, \ldots, \widetilde{a}_{rj_r}$ di $\widetilde{A}$.

A tale scopo, consideriamo una combinazione lineare

$$\beta_1 A^{(j_1)} + \cdots + \beta_r A^{(j_r)} = 0 \tag{6.4}$$

e supponiamo che essa dia il vettore nullo. Definiamo il vettore $s = \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{pmatrix} \in \mathbb{K}^n$ come segue:

$$s_i := \begin{cases} 0, & \text{se } i \neq j_1, \ldots j_r; \\ \beta_i, & \text{se } i = j_k,\ k = 1, \ldots, r. \end{cases}$$

Con questa scelta abbiamo

$$A \cdot s = \beta_1 A^{(j_1)} + \cdots + \beta_r A^{(j_r)},$$

quindi per la (6.4) si ha

$$A \cdot s = 0.$$

Siccome $\widetilde{A}$ è ottenuta da A per mezzo di operazioni elementari, abbiamo che vale anche

$$\widetilde{A} \cdot s = 0.$$

Osserviamo che

$$\widetilde{A} \cdot s = \beta_1 \widetilde{A}^{(j_1)} + \cdots + \beta_r \widetilde{A}^{(j_r)},$$

e siccome $\widetilde{A}^{(j_1)}, \ldots, \widetilde{A}^{(j_r)}$ sono linearmente indipendenti, concludiamo che $\beta_1 = \cdots = \beta_r = 0$, quindi anche $A^{(j_1)}, \ldots, A^{(j_r)}$ sono linearmente indipendenti.

3. È sufficiente dimostrare l' enunciato nel caso in cui $\widetilde{A}$ si ottiene da A per mezzo di una operazione elementare di tipo 1, rispettivamente di tipo 2 o 3. Supponiamo dapprima che A sia ottenuta da A scambiando

la riga i-esima con quella j-esima, per qualche $i \neq j, i, j \in \{1, \dots, m\}$. Questo corrisponde allo scambio della colonna i-esima con la j-esima di ${}^tA$, quindi

$$({}^t\widetilde{A})^{(k)} = \begin{cases} ({}^tA)^{(k)}, & \text{se } k \neq i, j, \\ ({}^tA)^{(j)}, & \text{se } k = i, \\ ({}^tA)^{(i)}, & \text{se } k = j. \end{cases}$$

Da questo segue immediatamente che

$$\mathrm{Span}(({}^tA)^{(1)}, \dots, ({}^tA)^{(m)}) = \mathrm{Span}(({}^t\widetilde{A})^{(1)}, \dots, ({}^t\widetilde{A})^{(m)}),$$

perciò $\mathrm{rg}({}^tA) = \mathrm{rg}({}^t\widetilde{A})$.

Supponiamo ora che $\widetilde{A}$ si ottenga da A per mezzo di una operazione elementare di tipo 3, precisamente sostituendo la riga j-esima con $A_{(j)} + cA_{(i)}$, per qualche $i \neq j, i, j \in \{1, \dots, m\}$, e $c \in \mathbb{K}$. Allora

$$({}^t\widetilde{A})^{(k)} = \begin{cases} ({}^tA)^{(k)}, & \text{se } k \neq j, \\ ({}^tA)^{(j)} + c({}^tA)^{(i)}, & \text{se } k = j, \end{cases}$$

ed in questo caso abbiamo:

$$\mathrm{Span}(({}^tA)^{(1)}, \dots, ({}^tA)^{(m)}) = \mathrm{Span}(({}^tA)^{(1)}, \dots, ({}^tA)^{(j-1)}, ({}^tA)^{(j)} + c({}^tA)^{(i)}, \dots, ({}^tA)^{(m)}) =$$

$$= \mathrm{Span}(({}^t\widetilde{A})^{(1)}, \dots, ({}^t\widetilde{A})^{(m)}),$$

perciò $\mathrm{rg}({}^tA) = \mathrm{rg}({}^t\widetilde{A})$.

Si verifica analogamente che se $\widetilde{A}$ si ottiene da A per mezzo di una operazione elementare di tipo 2, allora $\mathrm{rg}({}^tA) = \mathrm{rg}({}^t\widetilde{A})$.

4. Per i punti 1 e 3 appena dimostrati, è sufficiente dimostrare che

$$\mathrm{rg}(\widetilde{A}) = \mathrm{rg}({}^t\widetilde{A}),$$

dove $\widetilde{A}$ è una matrice a scala ottenuta da A per mezzo di operazioni elementari.

Per il punto 2 abbiamo che $\mathrm{rg}(\widetilde{A}) = r$, dove r è il numero delle righe non nulle di A. Dimostriamo quindi che $\mathrm{rg}({}^t\widetilde{A}) = r$.

A tale scopo, sia

$$c_1({}^t\widetilde{A})^{(1)} + \cdots + c_m({}^t\widetilde{A})^{(m)} \in \mathbb{K}^n \tag{6.5}$$

una combinazione lineare delle colonne di ${}^t\widetilde{A}$, e supponiamo che sia uguale al vettore nullo. Osserviamo che

$$({}^t\widetilde{A})^{(r+1)} = \cdots = ({}^t\widetilde{A})^{(m)} = 0,$$

quindi possiamo omettere queste colonne nella (6.5). Inoltre tale combinazione lineare ha la forma:

$$\begin{pmatrix} 0 \\ \vdots \\ 0 \\ \lambda_1 \widetilde{a}_{1j_1} \\ \vdots \\ \lambda_1 \widetilde{a}_{1j_2} + \lambda_2 \widetilde{a}_{2j_2} \\ \vdots \\ \lambda_1 \widetilde{a}_{1j_r} + \dots \lambda_r \widetilde{a}_{rj_r} \\ \vdots \end{pmatrix}. \tag{6.6}$$

Siccome $\widetilde{a}_{1j_1} \neq 0, \widetilde{a}_{2j_2} \neq 0, \dots, \widetilde{a}_{rj_r} \neq 0$, il vettore (6.6) è nullo se e solo se $\lambda_1 = \lambda_2 = \dots = \lambda_r = 0$. Concludiamo quindi che le colonne $({}^t\widetilde{A})^{(1)}, \dots, ({}^t\widetilde{A})^{(r)}$ sono linearmente indipendenti e $\mathrm{rg}({}^t\widetilde{A}) = r$.

□

Teorema 6.1.4. *(Rouché-Capelli). Un sistema lineare $A \cdot X = b$ di m equazioni lineari in n incognite è compatibile* $\iff$

$$\mathrm{rg}(A|b) = \mathrm{rg}(A).$$

In tal caso la sua generica soluzione dipende da $n - r$ parametri, dove $r = \mathrm{rg}(A)$.

La dimostrazione del Teorema di Rouché-Capelli seguirà dal seguente risultato:

Lemma 6.1.5. *Un sistema lineare $A \cdot X = b$ di m equazioni lineari di ordine n è compatibile* $\iff$

$$b \in \mathrm{Span}(A^{(1)}, A^{(2)}, \dots, A^{(n)}). \tag{6.7}$$

Dimostrazione. Abbiamo che $A \cdot X = b$ è compatibile $\iff$ esiste $s = \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{pmatrix} \in \mathbb{K}^n$ tale che $A \cdot s = b$ $\iff$

$$A^{(1)}s_1 + A^{(2)}s_2 + \dots + A^{(n)}s_n = b \iff b \in \mathrm{Span}(A^{(1)}, A^{(2)}, \dots, A^{(n)}).$$

□

Dimostrazione. (Teorema di Rouché - Capelli) Per il Lemma 6.1.5 il sistema $A \cdot X = b$ è compatibile se e solo se $b \in \mathrm{Span}(A^{(1)}, A^{(2)}, \dots, A^{(n)})$. Si può verificare facilmente che tale condizione è soddisfatta se e solo se

$$\mathrm{Span}(A^{(1)}, A^{(2)}, \dots, A^{(n)}) = \mathrm{Span}(A^{(1)}, A^{(2)}, \dots, A^{(n)}, b).$$

Siccome in generale vale

$$\mathrm{Span}(A^{(1)}, A^{(2)}, \dots, A^{(n)}) \subseteq \mathrm{Span}(A^{(1)}, A^{(2)}, \dots, A^{(n)}, b),$$

i due sottospazi vettoriali sono uguali se e solo se hanno la stessa dimensione, cioè se e solo se $\mathrm{rg}(A) = \mathrm{rg}(A|b)$.

Supponiamo ora che $A \cdot X = b$ sia compatibile. Il teorema di struttura per le soluzioni dei sistemi di equazioni lineari afferma che $S = \{\widetilde{s} + s_0 \mid s_0 \in W\}$, dove $S = \{s \in \mathbb{K}^n | A \cdot s = b\}$ è l' insieme delle soluzioni, $\widetilde{s}$ è una soluzione particolare, e

$$W = \{s_0 \in \mathbb{K}^n | A \cdot s_0 = 0\}$$

è il sottospazio vettoriale di $\mathbb{K}^n$ delle soluzioni del sistema lineare omogeneo associato. Per il Teorema della Dimensione, che vedremo in seguito, $\dim(W) = n - \mathrm{rg}(A) = n - r$. Fissiamo una base $\{v_1, \ldots, v_{n-r}\}$ di W; allora ogni soluzione si scrive nella forma seguente

$$s = \widetilde{s} + c_1 v_1 + \cdots + c_{n-r} v_{n-r},$$

al variare dei parametri $c_1, \ldots, c_{n-r} \in \mathbb{K}$. Quindi le soluzioni di $A \cdot X = b$ dipendono da $n - r$ parametri. □

6.2 Rango e invertibilità

Il seguente teorema afferma che una matrice quadrata è invertibile se e solo se ha rango massimo.

Teorema 6.2.1. *Sia $A \in M_n(\mathbb{K})$. Allora A è invertibile se e solo se $\mathrm{rg}(A) = n$.*

Dimostrazione. Supponiamo che A sia invertibile. Sia $M \in M_n(\mathbb{K})$ la matrice inversa di A, quindi $A \cdot M = \mathbb{I}_n$. Osserviamo che quest ultima equazione si può riscrivere come segue:

$$A \cdot M^{(i)} = e_i,\ i = 1, \ldots, n, \tag{6.8}$$

dove e_i è l' i-esimo vettore della base canonica di $\mathbb{K}^n$. Come visto nel Lemma 6.1.5, questo implica che

$$e_1, \ldots, e_n \in \mathrm{Span}(A^{(1)}, A^{(2)}, \ldots, A^{(n)}),$$

quindi

$$\mathbb{K}^n = \mathrm{Span}(e_1, \ldots, e_n) \subseteq \mathrm{Span}(A(1), \ldots, A(n)) \subseteq \mathbb{K}^n,$$

da cui $\mathrm{Span}(A(1), \ldots, A(n)) = \mathbb{K}^n$ e e $\mathrm{rg}(A) = n$.

Viceversa, supponiamo che $\mathrm{rg}(A) = n$, e consideriamo i sistemi lineari

$$A \cdot X = e_i,\ i = 1, \ldots, n. \tag{6.9}$$

Osserviamo che per ogni i, il rango della matrice completa $(A \mid e_i)$ soddisfa:

$$n \geq \mathrm{rg}(A \mid e_i) \geq \mathrm{rg}(A) = n,$$

quindi $\mathrm{rg}(A \mid e_i) = \mathrm{rg}(A)$. Per il Teorema di Rouché - Capelli i sistemi (6.9) sono compatibili per ogni $i = 1, \ldots, n$, e la generica soluzione dipende da $n - n = 0$ parametri, cioè è unica. Inserendo i vettori soluzione nelle colonne di una matrice si ottiene una $M \in M_n(\mathbb{K})$ tale che

$$A \cdot M = \mathbb{I}_n.$$

Con un ragionamento analogo si può dimostrare che vale anche

$$M \cdot A = \mathbb{I}_n,$$

e quindi A è invertibile e si ha

$$M = A^{-1}.$$

□

6.3 Calcolo della matrice inversa con l' algoritmo di Gauss

Se $A \in M_n(\mathbb{K})$ è invertibile, per calcolare la sua inversa A^{-1} si può procedere come segue. Ricordiamo che A^{-1} è quella matrice $M \in M_n(\mathbb{K})$ tale che $A \cdot M = \mathbb{I}_n$. Quindi, per ogni $i = 1, \dots, n$, la colonna i-esima $M^{(i)}$ di M è l' unica soluzione del sistema di equazioni lineari

$$A \cdot X = e_i,$$

dove $e_i \in \mathbb{K}^n$ è l' i-esimo vettore della base canonica di $\mathbb{K}^n$. Notiamo che è possibile risolvere questi sistemi lineari simultaneamente, per $i = 1, \dots, n$, nel seguente modo. Consideriamo la matrice

$$(A \mid \mathbb{I}_n) \in M_{n,2n}(\mathbb{K}).$$

Siccome A è invertibile, si ha $\mathrm{rg}(A) = n$. Non è difficile verificare che è possibile trasformare $(A \mid \mathbb{I}_n)$ tramite una sequenza di operazioni elementari OE1, OE2, OE3, nella matrice

$$(\mathbb{I}_n \mid M).$$

Siccome le operazioni elementari trasformano un sistema di equazioni lineari in uno equivalente, segue che la soluzione di $A \cdot X = e_i$ coincide con la soluzione di $\mathbb{I}_n \cdot X = M^{(i)}$, che è proprio $M^{(i)}$, quindi $M = A^{-1}$.

6.4 Rango e sottomatrici

Definizione 6.4.1. Sia $A = (a_{ij}) \in M_{m,n}(\mathbb{K})$, e siano $p \in \{1, \dots, m\}$, $q \in \{1, \dots, n\}$. Siano inoltre $1 \leq i_1 < \cdots < i_p \leq m$, $1 \leq j_1 < \cdots < j_q \leq n$. Con

$$A(i_1, \dots, i_p \mid j_1, \dots, j_q)$$

denotiamo la matrice $p \times q$ a coefficienti in $\mathbb{K}$ il cui elemento di posto k, l è dato da

$$a_{i_k, j_l}, \ \forall k = 1, \dots, p, \forall l = 1, \dots, q.$$

Ogni matrice del tipo $A(i_1, \dots, i_p \mid j_1, \dots, j_q)$ si chiama sottomatrice $p \times q$ di A.

Proposizione 6.4.2. *Sia $A \in M_{m,n}(\mathbb{K})$, e sia B una sottomatrice $p \times q$ di A. Allora* $\mathrm{rg}(B) \leq \mathrm{rg}(A)$.

Dimostrazione. Omessa. □

Teorema 6.4.3. *Sia $A \in M_{m,n}(\mathbb{K})$. Allora*

$$\mathrm{rg}(A) = \max\{\mathrm{rg}(B) | B \text{ sottomatrice quadrata di } A\},$$

e anche

$$\mathrm{rg}(A) = \text{massimo degli ordini delle sottomatrici quadrate ed invertibili di } A.$$

Dimostrazione. Omessa. □