Matematica Discreta e Algebra Lineare

Appunti per il corso di Algebra e Geometria
Corso di Laurea in Informatica
Università dell'Insubria - Varese

Prof. Brunella Gerla

8 dicembre 2020

Indice

1 Insiemi

1.1 Prime definizioni

Un insieme è una collezione o una raccolta di oggetti. Questa definizione è piuttosto informale, ma andrà bene per lo scopo di questo corso. Definizioni più precise del concetto di insieme richiedono strumenti matematici molto elaborati. Sono esempi di insiemi:

1. l'insieme dei libri di una biblioteca,
2. l'insieme delle lettere della parola CASA,
3. l'insieme dei numeri primi,
4. l'insieme dei felini,
5. l'insieme delle lettere dell' alfabeto italiano.

Indicheremo gli insiemi con lettere latine maiuscole e gli oggetti da cui essi sono composti, chiamati **elementi**, con le lettere minuscole. Questa è una convenzione che ci permette di distinguere rapidamente se stiamo parlando di insiemi o di altri oggetti, ma come vedremo, è una convenzione che può essere abbandonata quando non si rivela utile.

Per indicare che l'elemento x appartiene all'insieme A si usa il simbolo $\in$. In tal caso si scrive

$$x \in A$$

e si legge "x appartiene ad A ". Per indicare, invece, che x non appartiene all'insieme A si scrive $x \notin A$, che si legge "x non appartiene ad A ".

In un insieme è importante solo quali elementi ci sono, non conta in che ordine sono scritti e non conta neanche quante volte si ripetono. Un insieme è caratterizzato dai suoi elementi (questo vuol dire che due insiemi che hanno gli stessi elementi sono uguali... questa frase può sembrare un po' strana, ma dovremo abituarci ad espressioni di questo tipo).

L'insieme privo di elementi si chiama **insieme vuoto** e si denota con $\{\}$ oppure con il simbolo $\emptyset$. Gli insiemi possono essere finiti o infiniti, a seconda del numero di elementi che contengono.

Gli insiemi si possono rappresentare in diversi modi:

1. La **notazione estensionale** consiste nell'elencare tutti e soli gli elementi dell'insieme (chiamata anche rappresentazione per **elencazione**). Si scrivono gli elementi dell'insieme tra parentesi graffe, separandoli con la virgola. Ad esempio
$$\{Mario, 3, \pi, *\}$$
oppure
$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}.$$
Questo tipo di notazione è molto utile per insiemi piccoli, con pochi elementi, ma diventa più difficile da utilizzare per insiemi più grandi o infiniti. D'altra parte, per alcuni insiemi infiniti si ricorre ugualmente alla notazione estensionale, anche se non è possibile materialmente elencarne tutti gli elementi. Ad esempio, l'insieme dei numeri naturali dispari si può rappresentare come
$$\{1, 3, 5, 7, \ldots\}.$$
Negli esempi precedenti, possiamo usare la rappresentazione estensionale per scrivere l'insieme delle lettere dalla parola CASA che sarà $\{C, A, S\}$ (ricordiamo che non c'è bisogno di ripetere la lettera A due volte), o per l'insieme delle lettere dell'alfabeto italiano
$$\{a, b, c, d, e, f, g, h, i, l, m, n, o, p, q, r, s, t, u, v, z\},$$
mentre è più difficile usare la notazione estensionale per rappresentare l'insieme dei felini (anche se per un biologo potrebbe non essere impossibile, si ottiene un insieme del tipo {gatti, tigri, leoni, etc..}).

2. La **notazione intensionale** descrive un insieme come la collezione di elementi che condividono una certa proprietà. Ad esempio per rappresentare l'insieme A di tutte le parole della lingua italiana scriviamo:
$$A = \{x : x \text{ è una parola della lingua italiana}\}$$
che si legge "A è l'insieme di tutti gli x tali che x è una parola della lingua italiana". Nota che al posto dei due punti si può trovare una linea verticale:
$$A = \{x \mid x \text{ è una parola della lingua italiana}\}.$$
Questa notazione consiste di due parti, nella prima scriviamo che forma hanno gli elementi, e se per esempio sono presi da qualche insieme più grande, nella seconda scriviamo quale proprietà devono avere tali elementi. Possiamo leggerla così: Un insieme è formato da quegli elementi x presi da un insieme più grande X che soddisfano una certà proprietà P cioè $\{x \in X : P(x)\}$. Ad esempio, se P è la proprietà di essere multiplo di 3, allora scriviamo $\{x \in \mathbb{N} : P(x)\}$ per indicare l'insieme dei numeri naturali che sono multipli di 3.

3. Possiamo rappresentare gli insiemi anche **graficamente**: si racchiudono gli elementi in una linea chiusa e le figure cosí ottenute sono chiamate **diagrammi di Eulero-Venn**. Nel caso dell'insieme $S = \{Mario, 3, \pi, *\}$, il diagramma di Eulero-Venn è come in Figura 6.4. Questa notazione è

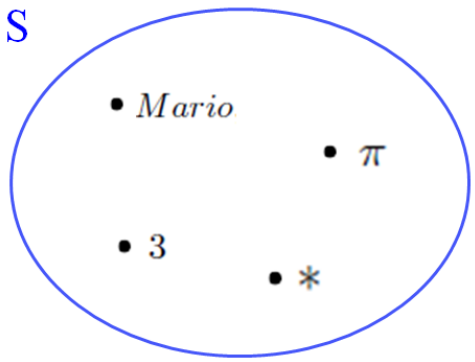


Figura 1.1: $S = \{Mario, 3, \pi, *\}$

utile per insiemi finiti e per alcune definizioni che vedremo più avanti.

In genere incontreremo sempre espressioni del tipo "Sia X un insieme" che vogliono dire che ci serve considerare un insieme X qualsiasi, del quale poi eventualmente andremo a specificare alcune proprietà. Uno degli scopi della matematica è quello di trovare proprietà comuni a diversi oggetti, quindi si cerca di ragionare in generale per poter trovare appunto proprietà generali.

Di particolare importanza sono alcuni **insiemi numerici** per i quali invece utilizzeremo come nome dei simboli speciali (anche questa chiaramente è una convenzione), tra cui

- $\mathbb{N} = \{0, 1, 2, \ldots\}$, l'insieme dei numeri naturali maggiori o uguali di zero;
- $\mathbb{N}^+ = \{1, 2, \ldots\}$, l'insieme dei numeri naturali maggiori strettamente di zero; e
- $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$, l'insieme dei numeri interi.

Esempio 1.1.1. Con le notazioni viste finora possiamo iniziare a scrivere alcuni esempi:

- $\{a, a, b\} = \{a, b\}$ perché non importa ripetere un elemento due volte, infatti gli insiemi $\{a, a, b\}$ e $\{a, b\}$ hanno gli stessi elementi;
- $\{a, b\} = \{b, a\}$ perché non importa l'ordine degli elementi;
- $\{1, 2, 3, 4\} = \{n \in \mathbb{N} \mid n \text{ è maggiore di } 0 \text{ e minore di } 5\}$;
- $2 \in \mathbb{N}$, $a \in \{a, b, c, d, e\}$, $a \notin \mathbb{N}$, $-4 \notin \mathbb{N}$.

Definizione 1.1.2. Un insieme A si dice **sottoinsieme** di un insieme B oppure **incluso** in B, se tutti gli elementi di A appartengono anche a B. Per indicare che A è un sottoinsieme di B si scrive $A \subseteq B$.

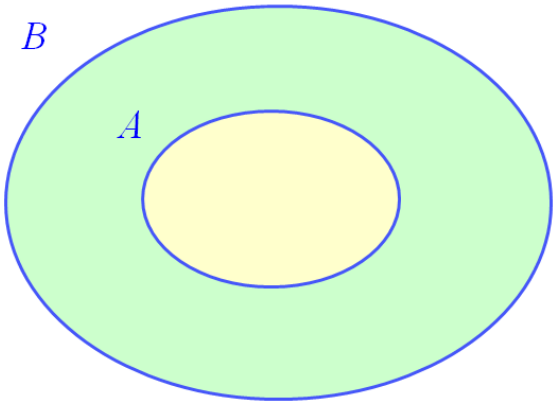


Figura 1.2: A è un sottoinsieme di B

Esempio 1.1.3. Se $X = \{a, b, c\}$ e $Y = \{1, a, 2, b, 3, c\}$, allora $X \subseteq Y$.

Per indicare, invece, che A non è un sottoinsieme di B si usa il simbolo $\not\subseteq$.

Esempio 1.1.4. Se $X = \{1, 5, b\}$ e $Y = \{1, b, c, d\}$, allora $X \not\subseteq Y$ perché $5 \in X$, ma $5 \notin Y$.

Dato un insieme A, l'insieme vuoto $\emptyset$ e l'insieme A stesso sono sottoinsiemi di A che si dicono **sottoinsiemi impropri**, mentre tutti gli altri sottoinsiemi di A si dicono **sottoinsiemi propri**.

Definizione 1.1.5. Un **singleton** o **singoletto** è un insieme con un solo elemento.

Per vedere se due insiemi sono uguali bisogna controllare che abbiano gli stessi elementi, eventualmente elencati con ordine diverso. Per esempio $\{1, 2, 3, 4, 5, 6, 7\}$ è uguale a $\{1, 3, 5, 7, 2, 4, 6\}$ perché gli elementi sono gli stessi. Può essere più difficile capire che due insiemi sono uguali quando sono descritti in modo diverso. In questo caso si può utlizzare il metodo della **doppia inclusione**: per provare che $A = B$ si prova che $A \subseteq B$ e che $B \subseteq A$. Per esempio consideriamo l'insieme $A = \{n \in \mathbb{N} \mid n - 1 > 0\}$ e $B = \{n \in \mathbb{N} \mid n^2 > 1\}$. Per provare che $A = B$ procediamo con la doppia inclusione: se prendo un elemento n in A, allora $n - 1 > 0$ e quindi $n > 1$ e quindi $n^2 > 1$, quindi $n \in B$. Abbiamo quindi provato che $A \subseteq B$. Viceversa, se $n \in B$ allora $n^2 > 1$ e quindi, dato che stiamo considerando numero interi, deve essere necessariamente $n > 1$ e quindi $n \in A$ e $B \subseteq A$. Avendo provato la doppia inclusione, si ha che $A = B$.

Definizione 1.1.6. L'**ordine** o la **cardinalità** di un insieme finito A è il numero di elementi di A e si indica con $|A|$.

Esempio 1.1.7. Se $X = \{1, 3, f, 5, 6\}$, allora $|X| = 5$.

Osservazione 1. La cardinalità dell'insieme vuoto è zero. La cardinalità di un singoletto è 1. Se X e Y sono insiemi finiti e $X \subseteq Y$ allora $|X| \leq |Y|$: si consideri per esempio $X = \{a, b, c\}$ e $Y = \{a, b, c, d, e\}$.

Nota che un insieme può avere elementi qualsiasi, in particolare può avere anche degli altri elementi come insiemi:

Esempio 1.1.8. Consideriamo l'insieme $A = \{a, 1, \{a\}, b, \{c\}\}$. Questo insieme ha 5 elementi che sono:

$$a \qquad 1 \qquad \{a\} \qquad b \qquad \{c\}.$$

In particolare due elementi di A sono a loro volta degli insiemi. Allora valgono le seguenti relazioni (utili per capire la differenza tra $\in$ e $\subseteq$):

- $a \in A$;
- $\{a\} \subseteq A$ perché $a \in A$;
- $\{a\} \in A$, cioè $\{a\}$ è anche un elemento di A;
- $b \in A$ quindi $\{b\} \subseteq A$ ma $\{b\} \notin A$.
- $c \notin A$, quindi $\{c\} \nsubseteq A$ ma $\{c\} \in A$.

Definizione 1.1.9. L' **insieme delle parti** $P(A)$ di un insieme A è l'insieme di tutti e soli i sottoinsiemi di A.

Per quanto detto in precedenza, si ha $\{\} \in P(A)$ e $A \in P(A)$ qualsiasi sia l'insieme A.

Esempio 1.1.10. Sia $A = \{1, 2, 3\}$. I sottoinsiemi di A sono:

- $\{\}$ con 0 elementi;
- $\{1\}$, $\{2\}$, $\{3\}$ con 1 elemento;
- $\{1, 2\}$, $\{2, 3\}$, $\{1, 3\}$ con 2 elementi;
- $\{1, 2, 3\} = A$ con 3 elementi.

Proposizione 1.1.11. *Se un insieme A ha n elementi allora ha 2^n sottoinsiemi. In altri termini: se $|A| = n$ allora $|P(A)| = 2^n$.*

Esempio 1.1.12. Se $A = \{1, \{2\}, 3, a\}$ allora $P(A)$ deve avere $2^4 = 16$ elementi. Elenchiamoli tutti:

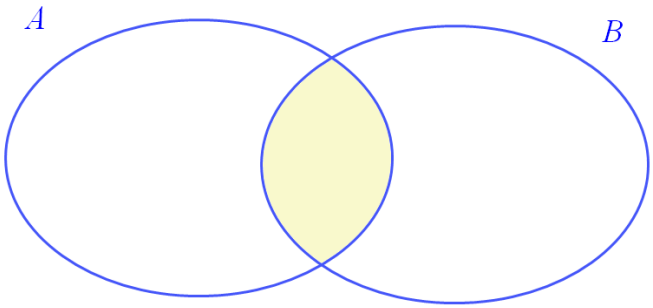
- $\{\}$
- $\{1\}$, $\{\{2\}\}$, $\{3\}$, $\{a\}$;
- $\{1, \{2\}\}$, $\{\{2\}, 3\}$, $\{1, 3\}$, $\{1, a\}$, $\{\{2\}, a\}$, $\{3, a\}$
- $\{\{2\}, 3, a\}$, $\{1, 3, a\}$, $\{1, \{2\}, a\}$, $\{1, \{2\}, 3\}$;
- $\{1, \{2\}, 3, a\} = A$.

Confronta con l'esempio precedente: non cambia molto, al posto di 2 bisogna scrivere $\{2\}$. Quanti e come saranno i sottoinsiemi dell'insieme $B = \{1, \{2, 3\}, 4\}$ (nota che B ha 3 elementi)?

1.2 Operazioni tra insiemi

Definizione 1.2.1. Dati due insiemi A e B, l' **insieme intersezione** di A e B è l'insieme degli elementi che appartengono contemporaneamente ad A e a B. In simboli

$$A \cap B = \{x : x \in A \text{ e } x \in B\}.$$



Esempio 1.2.2. Dati gli insiemi $X = \{n \in \mathbb{N} : \text{ n è pari }\}$ e $Y = \{n \in \mathbb{N} : \text{ n è un multiplo di 3 }\}$, allora

$$X \cap Y = \{6, 12, 18, 24, \ldots\}.$$

Osservazione 2. L'insieme intersezione di due insiemi è incluso negli insiemi stessi, in simboli: $A \cap B \subseteq A$ e $A \cap B \subseteq B$. Inoltre, se $A \subseteq B$, allora $A \cap B = A$.

Definizione 1.2.3. Due insiemi A e B che non hanno elementi in comune, ovvero tali che $A \cap B = \emptyset$, si dicono **disgiunti**.

Esempio 1.2.4. Se $X = \{a, b, c, d\}$ e $Y = \{b, c, d, e, f\}$ allora $X \cap Y = \{b, c, d\}$. Consideriamo i seguenti insiemi (si noti la particolare notazione usata):

- $X = \{n \in \mathbb{N} : n \text{ è pari }\}$;
- $Y = \{n \in \mathbb{N} : n \text{ è dispari }\}$;
- $Z = \{n \in \mathbb{N} : n \text{ è multiplo di } 4\ \}$;

allora X e Y sono disgiunti, infatti $X \cap Y = \emptyset$. Lo stesso vale per Y e Z.

Definizione 1.2.5. Dati due insiemi A e B, l' **insieme unione** di A e B è l'insieme degli elementi che appartengono ad A oppure a B. In simboli

$$A \cup B = \{x : x \in A \text{ oppure } x \in B\}.$$

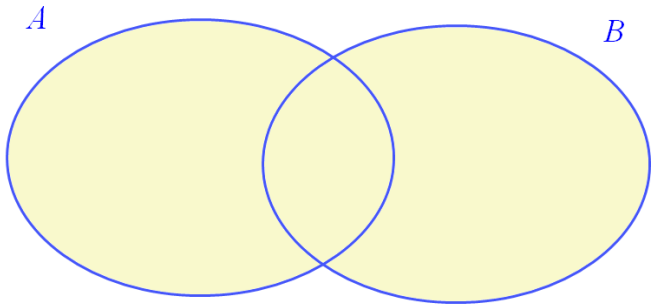


Figura 1.3: Unione

Esempio 1.2.6. Dati gli insiemi $X = \{a, e, i, o, u\}$ e $Y = \{a, b, c, d, e\}$, allora

$$X \cup Y = \{a, e, i, o, u, b, c, d\}.$$

Nota che non ripetiamo gli elementi che si trovano sia in X che in Y, basta scriverli una volta sola.

Possiamo contare gli elementi che si trovano nell'unione di due insiemi, conoscendo solo la cardinalità dei due insiemi di partenza? In genere non possiamo farlo se non sappiamo *quali* sono gli elementi dei due insiemi. Per esempio se considero due insiemi con 3 elementi non posso dire in generale quanti elementi ha la loro unione: se $X = \{a, b, c\}$ e $Y = \{b, c, d\}$ allora $X \cup Y = \{a, b, c, d\}$ e quindi $|X \cup Y| = 4$, ma se $Z = \{d, e, f\}$ allora $|X \cup Z| = 6$. Quindi il numero di elementi dell'unione non dipende solo dal numero di elementi degli insiemi che unisco, ma anche da quanti elementi i due insiemi hanno in comune. Vale infatti il seguente:

Principio di inclusione-esclusione: Se X e Y sono due insiemi finiti allora

$$|X \cup Y| = |X| + |Y| - |X \cap Y|.$$

Come vedremo questo principio è molto utile anche in alcuni casi di combinatoria.

Definizione 1.2.7. Dati due insiemi A e B, l' **insieme differenza** (o *complemento relativo*) fra A e B è l'insieme degli elementi di A che non appartengono a B. In simboli

$$A \setminus B = \{x \in A : x \notin B\}.$$

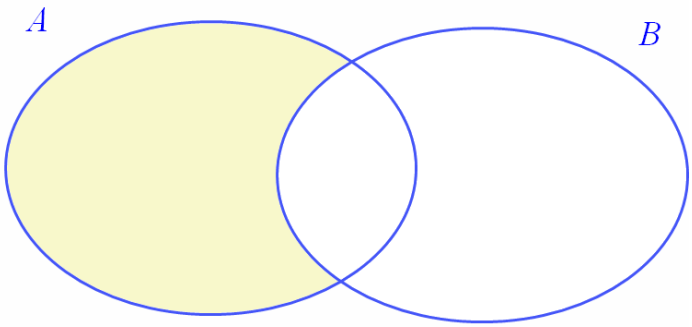


Figura 1.4: $A \setminus B$

Esempio 1.2.8. Dati gli insiemi $X = \{1, 2, 3, 4, 5\}$ e $Y = \{1, 3, 5\}$, allora $X \setminus Y = \{2, 4\}$.

Le operazioni viste finora possono essere definite tra i sottoinsiemi di un dato insieme U, cioè tra gli elementi di $\mathcal{P}(U)$, perché unione, intersezione e differenza di due sottoinsiemi di U è ancora un sottoinsieme di U. Se $A \subseteq U$ possiamo considerare l'insieme differenza $U \setminus A$, che in questo caso chiamiamo *complemento assoluto* di A e indichiamo con $\overline{A}$ (vedi Figura 1.5).

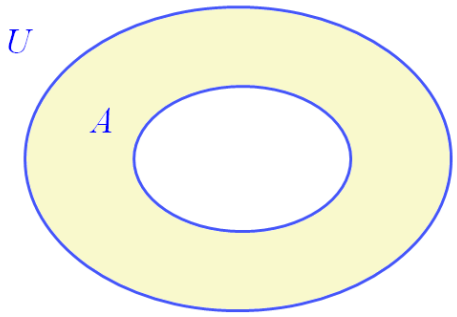


Figura 1.5: Complemento $\overline{A} = U \setminus A$

Esempio 1.2.9. Consideriamo l'insieme $\mathcal{P}(\mathbb{N})$ dei sottoinsiemi di $\mathbb{N}$. Sia $X \in \mathcal{P}(\mathbb{N})$ l'insieme dei numeri pari e $Y \in \mathcal{P}(\mathbb{N})$ l'insieme dei numeri dispari. Allora $X \setminus Y = X$, $Y \setminus X = Y$, $\overline{X}(= \mathbb{N} \setminus X) = Y$ e $\overline{Y} = X$. Se Z è l'insieme dei numeri multipli di 4 allora $X \setminus Z = \{n \in \mathbb{N} \mid n \text{ è pari e } n \text{ non è multiplo di } 4\}$.

Proprietà 1.2.10. *Tramite i diagrammi di Venn si possono controllare le seguenti uguaglianze che sono dette :*

- $\overline{A} \cup \overline{B} = \overline{A \cap B}$.
- $\overline{A} \cap \overline{B} = \overline{A \cup B}$.

Infatti, se un elemento x appartiene a $\overline{A} \cup \overline{B}$ allora vuol dire che o $x \in \overline{A}$ oppure $x \in \overline{B}$, quindi o $x \notin A$ oppure $x \notin B$, quindi x non appartiene all'intersezione $A \cap B$ e quindi $x \in \overline{A \cap B}$. In questo modo abbiamo mostrato che $\overline{A} \cup \overline{B} \subseteq \overline{A \cap B}$. Per mostrare l'altra inclusione, supponiamo che $x \in \overline{A \cap B}$, quindi x non appartiene a $A \cap B$, quindi o $x \notin A$ oppure $x \notin B$, quindi ancora $x \in \overline{A} \cup \overline{B}$. L'altra legge di De Morgan si dimostra in modo analogo.

Il concetto di insieme è fondamentale per la matematica. Tutti i concetti che vedremo in seguito (relazioni, funzioni, operazioni, strutture algebriche) sono tutti definiti a partire dalla definizione di insieme.

1.3 Prodotto Cartesiano

Abbiamo detto che in un insieme non è importante l'ordine con cui si elencano gli elementi. Quando invece vogliamo sottolineare l'ordine degli elementi possiamo usare altri concetti matematici: le coppie, quando abbiamo a che fare con due elementi, le triple quando dobbiamo considerarne tre, le quadruple, le quintuple e in genere le n-uple quando invece abbiamo n elementi (con n numero qualsiasi maggiore di 2).

L'insieme $\{a, \{a, b\}\}$ è chiamato **coppia** e viene di solito denotato con (a, b). Quindi la coppia (a, b) è diversa dalla coppia (b, a), dato che l'insieme $\{a, \{a, b\}\}$ è diverso dall'insieme $\{b, \{a, b\}\}$. Penseremo quindi in seguito ad una coppia (a, b) come una sequenza di due elementi che sono la **prima componente** a e la **seconda componente** b, e non useremo la definizione come insieme.

Definizione 1.3.1. Dati due insiemi A e B, il **prodotto cartesiano** di $A \times B$ è l'insieme di tutte le coppie (x, y) dove x è un elemento di A e y è un elemento di B. In simboli

$$A \times B = \{(x, y) : x \in A \text{ e } y \in B\}.$$

Esempio 1.3.2. Dati gli insiemi $X = \{a, b, c\}$ e $Y = \{1, 2\}$, allora

$$X \times Y = \{(a, 1), (a, 2), (b, 1), (b, 2), (c, 1), (c, 2)\}.$$

Possiamo contare gli elementi del prodotto cartesiano di due insiemi finiti: se voglio contare tutte le coppie che hanno prima componente in A e seconda componente in B allora inizio con il considerare tutte le coppie che hanno come prima componente il primo elemento di A e la cui seconda componente varia tra tutti gli elementi di B. In questo modo ottengo esattamente $|B|$ elementi. Poi passo a considerare come prima componente il secondo elemento di A e faccio

variare ancora la seconda componente tra tutti gli elementi di B, ottenendo in questo modo altri $|B|$ elementi. Se ripeto questo ragionamento per tutti gli elementi di A ottengo $|A| \cdot |B|$ elementi (si veda l'esempio precedente). Questo va sotto il nome di **Principio di moltiplicazione**: Se A e B sono insiemi finiti, allora

$$|A \times B| = |A| \cdot |B|.$$

Esempio 1.3.3. Siano $X = \{a, b, c\}$ e $Y = \{1\}$, allora

$$X \times Y = \{(a, 1), (b, 1), (c, 1)\}$$

e infatti $|X \times Y| = 3 \cdot 1 = 3$. Posso allora contare i sottoinsiemi di $X \times Y$ applicando il teorema visto in precendeza, ottenendo:

$$|P(X \times Y)| = 2^{|P(X \times Y)|} = 2^{|X| \cdot |Y|} = 2^3 = 8,$$

infatti

$$\begin{aligned} P(X \times Y) \;=\; & \{\{\}, \{(a, 1)\}, \{(b, 1)\}, \{(c, 1)\}, \\ & \{(a, 1), (b, 1)\}, \{(b, 1), (c, 1)\}, \{(a, 1), (c, 1)\}, X \times Y\}. \end{aligned}$$

1.4 Gli Insiemi e la Logica Matematica

Abbiamo visto che un insieme può anche essere definito con una **notazione intensionale**, descrivendolo come la collezione di elementi che condividono una certa proprietà. In questo paragrafo approfondiamo questo punto di vista: iniziamo con il sottolineare che non specificheremo formalmente cosa è una proprietà, ma utilizzeremo un po' di intuito per poter gestire i casi che esamineremo. In genere possiamo dire che una proprietà identifica alcuni elementi contenuti in un insieme più grande e ne scarta altri: per esempio essere un numero pari è una proprietà che identifica un sottoinsieme dei numeri naturali. Scriviamo

$$\{x \in X \mid P(x)\}$$

per indicare l'insieme di tutti gli elementi x di X che soddisfano la proprietà P (lo leggiamo anche *l'insieme degli elementi x di X tali che la proprietà P vale per x*). Ad esempio, se P è la proprietà di essere multiplo di 3, allora scriviamo $\{x \in \mathbb{N} \mid P(x)\}$ per indicare l'insieme dei numeri naturali che sono multipli di 3.

Se P è una proprietà e $x \in A$, allora $P(x)$ (che si legge *x soddisfa la proprietà P* oppure *vale P(x)*) è una frase che deve necessariamente essere vera oppure falsa: la chiameremo *proposizione* o *asserzione*. I valori Vero e Falso, che indichiamo con le lettere V e F, si dicono **valori di verità** della proposizione. Ad esempio,

se P è la propietà di essere un numero naturale multiplo di 4, allora $P(1)$ *(1 è un numero naturale multiplo di 4)* è una proposizione falsa e $P(8)$ *(8 è un numero naturale multiplo di 4)* è una proposizione vera. Altri esempi di proposizioni sono: *"2 è un numero pari"* (V), *"Parigi è la capitale dell'Italia"* (F) e *"3 è maggiore di 10"* (F). Le affermazioni *"Domani piove"* e *"L'enigmistica è divertente"*, invece non sono proposizioni in quanto esprimono una previsione e un giudizio, dunque non è possibile associargli un valore di verità in maniera oggettiva.

Con le proposizioni si possono eseguire delle operazioni, strettamente correlate alle operazioni insiemistiche, per ottenere proposizioni più complesse.

Gli operatori delle proposizioni sono i cosiddetti **connettivi logici**, tra cui i principali sono la negazione ($\neg$), la congiunzione ($\wedge$) e la disgiunzione ($\vee$). Se P e Q sono proprietà, allora $\neg P(x)$, $P(x) \wedge Q(x)$ e $P(x) \vee Q(x)$ sono nuove proposizioni i cui valori di verità dipendono da quelli di $P(x)$ e $Q(x)$ e sono descritti attraverso tabelle chiamate **tavole di verità**.

Negazione di una proposizione Sia P una proprietà, allora la negazione di $P(x)$, che si indica con $\neg P(x)$ e si legge "*not* $P(x)$", è la proposizione che è vera quando $P(x)$ è falsa ed è falsa quando $P(x)$ è vera.

Tavola di verità

$P(x)$	$\neg P(x)$
V	F
F	V

Il complemento di un insieme ha come proprietà caratteristica la negazione della proprietà caratteristica dell'insieme dato, dunque se $A = \{x \in X : P(x)\}$, allora

$$\overline{A} = \{x \in X : \neg P(x)\}.$$

Esempio 1.4.1. Se $x \in \mathbb{N}$, $P(x) =$ "x è dispari", allora $\overline{\{x \in \mathbb{N} \mid P(x)\}} = \{x \in \mathbb{N} :$ "x non è dispari"$\} = \{x \in \mathbb{N} :$ "x è pari"$\}$.

Congiunzione di due proposizioni Date le proprietà P e Q, la congiunzione di $P(X)$ e $Q(x)$, che si indica con $P(x) \wedge Q(x)$ e si legge "$P(x)$ *and* $Q(x)$", è la proposizione che è vera se $P(x)$ e $Q(x)$ sono contemporaneamente vere ed è falsa in ogni altro caso.

Tavola di verità

$P(x)$	$Q(x)$	$P(x) \wedge Q(x)$
V	V	V
V	F	F
F	V	F
F	F	F

L'insieme intersezione di due insiemi ha come proprietà caratteristica la congiunzione delle proprietà caratteristiche degli insiemi dati, dunque se $A = \{x \in X : P(x)\}$ e $B = \{x \in X : Q(x)\}$, allora

$$A \cap B = \{x \in X : P(x) \wedge Q(x)\}.$$

Esempio 1.4.2. Consideriamo le proprietà $P(x) =$"x è un numero pari"e $Q(x) =$"x è minore di 10". Allora $\{x \in \mathbb{N} \mid P(x)\} \cap \{x \in \mathbb{N} \mid Q(x)\} = \{x \in \mathbb{N} \mid$ "x è pari e minore di 10"$\} = \{0, 2, 4, 6, 8\}$.

Disgiunzione di due proposizioni Date le proprietà P e Q, la disgiunzione di $P(x)$ e $Q(x)$, che si indica con $P(x) \vee Q(x)$ e si legge "$P(x) \vee Q(x)$", è la proposizione che è vera se almeno una delle due proposizioni è vera ed è falsa se entrambe le proposizioni sono false.

La particella "o"del linguaggio ordinario corrisponde all'operatore $\vee$.

Tavola di verità

$P(x)$	$Q(x)$	$P(x) \vee Q(x)$
V	V	V
V	F	V
F	V	V
F	F	F

Osservazione 3. L'insieme unione di due insiemi ha come proprietà caratteristica la disgiunzione delle proprietà caratteristiche degli insiemi dati, dunque se $A = \{x \in X : P(x)\}$ e $B = \{x \in X : Q(x)\}$, allora

$$A \cup B = \{x \in X : P(x) \vee Q(x)\}.$$

Esempio 1.4.3. Se $N_1 = \{x \in \mathbb{N} :$ "x è multiplo di 5"$\}$ e $N_2 = \{x \in \mathbb{N} :$ "x è multiplo di 7"$\}$, allora $N_1 \cup N_2 = \{x \in \mathbb{N} :$ "x è multiplo di 5 o di 7"$\} = \{5, 7, 10, 14, 15, 20, 21, \ldots\}$.

Nella seguente tabella riassumiamo la corrispondenza tra operazioni logiche e operazioni insiemistiche.

Operazioni Logiche	**Operazioni Insiemistiche**
$\wedge$	$\cap$
$\vee$	$\cup$
$\neg$	complemento

Esempio 1.4.4. Sia A l'insieme degli studenti nella aula 2, $S(x)$ la proprietà di essere simpatico, $E(x)$ la proprietà di superare l'esame di algebra e geometria

al primo appello. Quindi l'insieme $\{x \in A \mid S(x)\}$ in questo contesto denota l'insieme degli studenti simpatici in aula 2 mentre $\{x \in A \mid E(x)\}$ è l'insieme degli studenti in aula 2 che superano l'esame al primo appello. Descrivere a parole i seguenti insiemi: $\{x \in A \mid \neg S(x)\}$, $\{x \in A \mid \neg E(x)\}$, $\{x \in A \mid S(x) \wedge \neg E(x)\}$, $\{x \in A \mid \neg S(x) \wedge \neg E(x)\}$, $\{x \in A \mid \neg S(x) \vee E(x)\}$.

Implicazione Date due proprietà P e Q, l'implicazione di $P(x)$ e $Q(x)$, che si indica con $P(x) \to Q(x)$ e si legge "*se* $P(x)$ *allora* $Q(x)$", è la proposizione che è falsa se $P(x)$ è vera e $Q(x)$ è falsa ed è vera in tutti gli altri casi.

Tavola di verità

$P(x)$	$Q(x)$	$P(x) \to Q(x)$
V	V	V
V	F	F
F	V	V
F	F	V

Osservazione 4. L'implicazione di proposizioni consente di definire l'inclusione di insiemi: dati gli insiemi $A = \{x \in X : P(x)\}$ e $B = \{x \in X : Q(x)\}$, allora

$$A \subseteq B \text{ se e solo se } P(x) \to Q(x) \text{ è vera per ogni } x \in X$$

Esempio 1.4.5. Siano $N_1 = \{x \in \mathbb{N} : P(x)\}$ e $N_2 = \{x \in \mathbb{N} : Q(x)\}$, dove $P(x)$= "x è maggiore di 4"e $Q(x)$="x è maggiore di 2".

Per ogni $n \in \mathbb{N}$, se n è maggiore di 4, allora n è maggiore di 2, dunque $N_1 \subseteq N_2$. D'altra parte $N_2 \nsubseteq N_1$, in quanto esistono numeri naturali x per cui la proposizione $Q(x) \to P(x)$ non è vera. Ad esempio, $Q(3) \to P(3)$ è falsa, poiché $Q(3)$ è vera e $P(3)$ è falsa.

Vedremo che spesso i risultati matematici sono del tipo "Se vale una certa proprietà P allora vale anche la proprietà Q". Questo tipo di espressione è in realtà una implicazione, $P \to Q$ (che si legge P implica Q). Per dimostrare una proprietà del genere si deve considerare come vera P, detta *ipotesi* e dalle informazioni contenute in P si deve ricavare Q con dei ragionamenti che si basano anche sulle varie definizioni matematiche coinvolte.

Contronominale. A partire dalla tavola di verità dell'implicazione, ci possiamo accorgere che dire che P implica Q equivale a dire che la negazione di Q implica la negazione di P. Vediamolo con un esempio: consideriamo l'aula dove facciamo lezione e l'affermazione *se una persona in aula ha meno di 20 anni allora è uno studente*. Se indico con V la proprietà *avere meno di 20 anni* e con S la proprietà *essere uno studente* allora l'espressione precedente si può formalizzare in questo modo:

Per ogni x in quest'aula, $V(x) \to S(x)$ (1)

Questa affermazione equivale a dire che

Per ogni x in quest'aula, Not $S(x) \to$ Not $V(x)$ (2)

cioè che se una persona in quest'aula non è uno studente allora non può avere meno di 20 anni. Le due espressioni (1) e (2) sono equivalenti, cioè dicono la stessa cosa. L'espressione (2) di chiama **contronominale** di (1). Nota che invece l'espressione

$$\text{Per ogni } x \text{ in quest'aula, } S(x) \to V(x)$$

non è equivalente alle altre due. Infatti questa espressione dice che ogni persona in quest'aula che è uno studente ha meno di venti anni, cosa che in genere non è vera.

Equivalenza. Altre volte gli enunciati hanno una forma del tipo

$$\text{vale P se e solo se vale Q.}$$

Questo tipo di affermazione corrisponde in realtà a due fatti: P implica Q e Q implica P. Si dice anche in questo caso che P e Q sono *equivalenti*. Per dimostrare questo tipo di risultati bisogna allora dimostrare le due implicazioni. Questo corrisponde al principio di doppia inclusione: per provare che due insiemi coincidono, si può provare che il primo è incluso nel secondo e che il secondo è incluso nel primo.

Esempio...

Quantificatori Siano X un insieme e P una proprietà. L'espressione $\exists x P(x)$ indica che esiste almeno un elemento x di X per cui $P(x)$ è vera.
Il simbolo $\exists$ si chiama **quantificatore esistenziale**.

L'espressione $\forall x P(x)$, invece, indica che $P(x)$ è vera per tutti gli x di X.
Il simbolo $\forall$ si chiama **quantificatore universale**.

Esempio 1.4.6. Se $X = \mathbb{N}$ e $P(x)$ è la proprietà di essere un numero pari, allora l'espressione $\exists x P(x)$ è vera, dato che è vero che esiste un numero pari, mentre l'espressione $\forall x P(x)$ è falsa perché non è vero che tutti i numeri sono pari.

Nelle dimostrazioni matematiche si ha a che fare sia con proprietà *universali* che devono essere provate per ogni elemento di un dato insieme, o anche con proprietà *esistenziali* per le quali si deve dimostrare l'esistenza di almeno un elemento che le soddisfa.

Facciamo un esempio. Se voglio controllare che tutti gli studenti in un'aula abbiano studiato allora devo fare una domanda ad ognuno di loro: mi basta però

trovare uno studente che non sa rispondere per poter dire che l'espressione "tutti gli studenti di quest'aula hanno studiato" non sarà più vera. In questo caso sarà invece vera l'espressione "esiste uno studente che non ha studiato". C'è quindi un collegamento tra i due quantificatori. D'altra parte, se voglio controllare che non esistano studenti antipatici allora devo controllare che tutti gli studenti siano simpatici.

In modo più formale possiamo scrivere nel seguente modo:

1. $\neg(\forall x P(x)) = \exists x \neg P(x)$;
2. $\neg(\exists x P(x)) = \forall x \neg P(x)$.

Ad esempio, l'affermazione "*non tutti i numeri naturali sono pari*" equivale all'affermazione "*esiste almeno un numero naturale che non è pari*"; invece "*non esiste un numero naturale minore di 0*" equivale a dire che "*tutti i numeri naturali sono maggiori o uguali di 0*".

Il punto (1) suggerisce che in matematica, per dimostrare che una proprietà P su un certo insieme X non è valida, basta esibire un **controesempio**, ovvero basta trovare un elemento $x \in X$ per cui $P(x)$ risulta falsa.

Esempio. Consideriamo l'espressione *Tutti gli studenti che superano l'esame di algebra e geometria al primo appello, superano anche l'esame di programmazione*. Come possiamo formalizzare questa espressione? Come possiamo provare se è vera oppure no? L'espressione contiene un quantificatore universale e una implicazione: *per ogni studente x, se x supera algebra e geoemtria allora x supera programmazione*. Per controllare che sia vera dobbiamo controllare che tutti gli studenti che superino algebra e geometria, superino anche programmazione. Quando questa espressione potrebbe essere falsa? Quando troviamo uno studente, che chiameremo Quintilio (sperando di non incontrare mai uno studente con questo nome), che superi l'esame di algebra e geometria ma non superi quello di programmazione. Non ci serve considerare studenti che non superano algebra e geometria, perché in questo caso non avremmo falsificato la nostra espressione che riguarda gli studenti che hanno superato tale esame. Se Quintilio supera algebra e geometria e non supera programmazione allora è il nostro controesempio e l'espressione è falsa. Se non ci sono studenti come Quintilio allora tutti gli studenti soddisfano l'implicazione e l'espressione è vera.

Per tornare ad un esempio più matematico: per dimostrare che un insieme A è contenuto in un insieme B devo controllare che tutti gli elementi di A appartengano a B. Quindi l'inclusione non sarà verificata se trovo un elemento di A che non appartiene a B. Per esempio, supponiamo di voler controllare se l'insieme dei numeri dispari maggiori di 1 è contenuto nell'insieme dei numeri primi. Consideriamo un numero dispari maggiore di 1, per esempio 3: 3 è anche un numero primo. Ci basta questo per poter affermare che vale l'inclusione? No,

perché dobbiamo controllare che questo valga per tutti i numeri dispari maggiori di 1. Consideriamo allora 5 che è dispari ed è ancora un numero primo. Anche 7 è un numero dispari che è anche un numero primo. Però 9 è un numero dispari che non è un numero primo, quindi non è vero che tutti i numeri dispari maggiori di 1 sono numeri primi. E' vero invece che esiste un numero dispari maggiore di 1 che non è un numero primo.

Per dimostrare che una proprietà è valida su un insieme X, bisogna provare che $P(x)$ è vera per ogni $x \in X$. Verificare che ciasun elemento di X soddifa la proprietà P risulta dispendioso se l'insieme X è molto grande e impossibile se X è infinito. Di conseguenza, bisogna ricorrere a una dimostrazione generale attraverso diversi metodi come il principio di induzione e la dimostrazione per assurdo.

1.5 Esercizi

1. Se A è un insieme di 4 elementi e B è un insieme di 6 elementi, quale delle seguenti affermazioni è sempre vera, qualsiasi siano gli elementi di A e B?
   - $A \cup B$ ha 10 elementi.
   - $A \cup B$ ha più elementi di $A \cap B$.
   - A e B sono disgiunti.

2. Sia $A = \{1, 3, 4, 6, 7, 8, 10, 13, 14, 21\}$ e $B = \{2, 4, 6, 8, 10, 12, 14, 16\}$. Descrivere gli elementi dei seguenti insiemi:
   - $A \cap B$
   - $A \cup B$
   - $A \setminus B$
   - $B \setminus A$

   Dire se le seguenti affermazioni sono vere:
   - $\{1, 2, 3, 4\} \subseteq A$
   - $\{1, 2, 3, 4\} \subseteq B$
   - $\{1, 2, 3, 4\} \subseteq A \cup B$
   - $\{12, 14, 16\} \subseteq B \setminus A$

3. Si considerino i seguenti insiemi: $R = \{a, b, \{a, b\}, c, \{c, d\}\}$, $S = \{a, b, c, d\}$ e $T = \{\{a, b\}, c, d\}$. Quanti elementi hanno R, S e T? Descrivere i seguenti insiemi:
   - $R \cap S$
   - $R \cup S$
   - $T \cap S$
   - $T \cup S$
   - $R \cap T$
   - $R \cup T$

4. Sia $A = \{a, \{1\}, 2, \{a, b\}\}$. Dire quali delle seguenti affermazioni è vera:
   - $a \in A$.
   - $a \subseteq A$
   - $\{a\} \in A$
   - $\{a\} \subseteq A$
   - $\{a, 2\} \in A$
   - $\{a, 2\} \subseteq A$
   - $\{a, b\} \in A$
   - $\{\{1\}\} \subseteq A$
   - $\{a, \{a, b\}\} \subseteq A$

5. Si considerino i seguenti insiemi:

   $A = \{\text{insieme dei gatti bianchi}\}$

   $B = \{\text{insieme dei gatti}\}$

   $C = \{\text{insieme dei cani}\}$

   $D = \{\text{insieme degli animali bianchi}\}$

   Quali delle seguenti affermazioni è vera:

- $A \subseteq B$
- $B \subseteq A$
- $D \cap B = A$
- A e C sono disgiunti
- B e D sono disgiunti
- C e D sono disgiunti

6. Si considerino i seguenti insiemi:

   $A = \{n \in \mathbb{N} \mid n \text{ è multiplo di } 4\}$

   $B = \{n \in \mathbb{N} \mid n \text{ è multiplo di } 5\}$

   $C = \{n \in \mathbb{N} \mid n \text{ è pari}\}$

   $D = \{0, 20, 25, 100\}$

   Quali delle seguenti affermazioni è vera:

   - $A \subseteq B$
   - $B \subseteq A$
   - $B \subseteq D$
   - $D \subseteq B$
   - $D \cap B = A$
   - A e C sono disgiunti
   - B e D sono disgiunti
   - $\overline{C}$ e D sono disgiunti
   - $D \subseteq A \cap B$
   - $B \cup D = B$

7. Scrivere tutti i sottoinsiemi di $X = \{a, \{a\}, b\}$, cioè $\mathcal{P}(X)$.

8. Sia $A = \{a, b, c\}$ e $B = \{a, b, c, d\}$. Scrivere $\mathcal{P}(A)$ e $\mathcal{P}(B)$ (insieme delle parti di A e insieme delle parti di B).

9. Se $S = \{a, b, c\}$ e $T = \{1, 2\}$ quali sono gli elementi di $S \times T$?

10. Scrivere gli elementi di $\mathcal{P}(\{a, b\} \times \{1, 2\})$.

11. Se $|A| = 4$, $|B| = 3$ e $|A \cap B| = 1$, quanti elementi hanno i seguenti insiemi?

    - $A \cup B$
    - $\mathcal{P}(A \cap B)$
    - $A \times B$
    - $A \times \mathcal{P}(A)$
    - $\mathcal{P}(A \times \mathcal{P}(A))$
    - $\mathcal{P}(A \times B)$
    - $\mathcal{P}(\mathcal{P}(B))$
    - $\mathcal{P}((A \cup B) \times B)$
    - $\mathcal{P}((A \cup B) \times (A \cap B))$

12. A quale delle seguenti espressioni è equivalente la frase *Non è vero che tutti gli studenti bravi superano l'esame di algebra e geometria al primo appello*:

    - Tutti gli studenti bravi non superano l'esame di algebra e geometria al primo appello.

- Non tutti gli studenti bravi sono bocciati al primo appello di algebra e geoemtria.
- Esiste uno studente bravo che non supera l'esame di algebra e geometria al primo appello.
- Esiste uno studente che non è bravo e supera l'esame di algebra di geometria al primo appello.

13. A quale delle seguenti espressioni è equivalente la frase *Non esiste un professore simpatico e bravo*:
    - O tutti i professori non sono simpatici oppure non sono bravi
    - Esiste un professore che è simpatico ma non è bravo
    - Esiste un professore che è bravo ma non è simpatico
    - Ogni professore non è contemporaneamente sia simpatico che bravo

14. Dimostrare in generale (quindi senza far riferimento a insiemi particolari o a esempi) che valgono le seguenti affermazioni, per qualsiasi insieme A e B:
    - $A \cap B \subseteq A \cup B$
    - Se $A \subseteq B$ allora $A \cap B = A$ e $A \cup B = B$
    - Se $A \nsubseteq B$ allora $A \cap B \neq A$
    - Se $S, T \in \mathcal{P}(A)$ allora $S \cap T \in \mathcal{P}(A)$
    - $A \setminus B \subseteq A$.

2 Relazioni e funzioni

2.1 Relazioni

Definizione 2.1.1. Dati gli insiemi A e B, una **relazione** fra A e B è un sottoinsieme del prodotto cartesiano $A \times B$. Una **relazione binaria** su A è un sottoinsieme di $A \times A$.

In una relazione ci sono solo alcune delle coppie del prodotto cartesiano. Ad esempio, dati gli insiemi $X = \{x : x \text{ è il nome di un abitante di Varese}\}$ e $Y = \{x : x \text{ è un numero telefonico}\}$, allora l'insieme $\mathcal{R}$ formato solo dalle coppie che hanno un nome di una persona come prima componente e il numero di telefono di quella persona come seconda componente è una relazione tra X e Y.

Esempio 2.1.2. Dati $A = \{a, b, c\}$ e $B = \{1, 2, 3\}$, l'insieme $\{(a, 1), (b, 1), (c, 1)\}$ è una relazione tra A e B.

Tra tutte le relazioni tra A e B possiamo considerare la relazione $\emptyset$ che chiameremo *relazione vuota*. Anche $A \times B$, cioè il prodotto cartesiano tra A e B, è una relazione che chiameremo *relazione totale*.

Proposizione 2.1.3. *Dati due insiemi finiti A e B, allora il numero di relazioni tra A e B è $|P(A \times B)| = 2^{n \cdot m}$, dove $|A| = n$ e $|B| = m$.*

Nel caso dell'Esempio 2.1.2, ci sono 2^9 relazioni tra A e B.
Notazione. Se $\mathcal{R}$ è una relazione tra gli insiemi A e B, cioè se $\mathcal{R} \subseteq A \times B$, allora spesso invece di scrivere che $(a, b) \in \mathcal{R}$ si scrive $a\mathcal{R}b$ e si legge *a è nella relazione $\mathcal{R}$ con b*.

Esempio 2.1.4. a) Dati $A = \{a, b, c\}$ e $B = \{1, 2, 3\}$, per indicare la relazione $\{(a, 1), (b, 1), (c, 1)\}$ possiamo anche scrivere $a\mathcal{R}1$, $b\mathcal{R}1$, $c\mathcal{R}1$.

b) L'insieme $\{(n, n) : n \in \mathbb{N}\}$ su $\mathbb{N}$ descrive la relazione di "uguaglianza" tra numeri naturali. Questa relazione si denota con $=$ e per dire che due elementi sono in questa relazione si scrive $n = m$.

c) La relazione di "minore o uguale" in $\mathbb{N}$ è definita dall'insieme $\{(n, m) \in \mathbb{N} \times \mathbb{N} : n \leq m\}$. Ad esempio, $1 \leq 5, 15 \leq 91$, ma non è vero che $3 \leq 2$.

d) La relazione di "essere multiplo " tra numeri naturali coincide con l'insieme $\{(n, m) \in \mathbb{N} \times \mathbb{N} : n \text{ è multiplo di } m\}$, dunque alcuni suoi elementi sono $(8, 2)$, $(15, 5)$ e $(100, 10)$.

Se A e B sono insiemi finiti, una relazione $\mathcal{R} \subseteq A \times B$ si può rappresentare disegnando una tabella a doppia entrata con le righe corrispondenti agli elementi dell' insieme A e le colonne corrispondenti agli elementi dell'insieme B e inserendo delle crocette nelle celle corrispondenti alle coppie che sono in relazione. Questa si chiama **matrice di adiacenza** della relazione.

Esempio 2.1.5. Siano gli insiemi $A = \{a, b\}$ e $B = \{1, 2, 3\}$. La relazione $\{(a, 1), (b, 2), (a, 3)\}$ tra A e B si può rappresentare nel modo seguente:

	1	2	3
a	$\times$		$\times$
b		$\times$	

Definizione 2.1.6. Data una relazione $\mathcal{R}$ tra A e B, definiamo la relazione **inversa** di $\mathcal{R}$ come la relazione $\mathcal{R}^{-1}$ tra B e A data da:

$$\mathcal{R}^{-1} = \{(b, a) \mid (a, b) \in \mathcal{R}\}.$$

Per esempio, se $\mathcal{R} = \{(a, 2), (b, 1), (a, 1), (b, 3)\}$ è una relazione tra $A = \{a, b\}$ e $B = \{1, 2, 3\}$ allora $\mathcal{R}^{-1} = \{(2, a), (1, b), (1, a), (3, b)\}$.

2.1.1 Relazioni binarie

Una relazione binaria su un insieme A è un sottoinsieme di $A \times A$.

Se l'insieme A è finito, una relazione binaria $\mathcal{R}$ su un insieme A si può rappresentare sia con la matrice di adiacenza, ma anche mediante il diagramma di Eulero-Venn di A, collegando con delle frecce gli elementi in relazione tra loro.

Esempio 2.1.7. Sia $A = \{a, b, c\}$. Il diagramma in Figura 2.1 rappresenta la relazione $\{(a, a), (a, b), (b, c), (c, a)\}$ su A.

Definizione 2.1.8. Sia $\mathcal{R}$ una relazione definita su A. $\mathcal{R}$ è **riflessiva** se ogni elemento di A è in relazione con se stesso, cioè $\forall x \in A,\ x\mathcal{R}x$.
Quindi una relazione NON è riflessiva se esiste un $x \in A$ tale che $x\ \not\mathcal{R}x$.

Nella rappresentazione con il diagramma di Venn, una relazione è riflessiva se ogni elemento è collegato a se stesso. Nella rappresentazione con la matrice di adiacenza, una relazione è riflessiva se sono segnate tutte le caselle sulla diagonale, corrispondenti alle coppie con prima e seconda componente uguali tra loro.

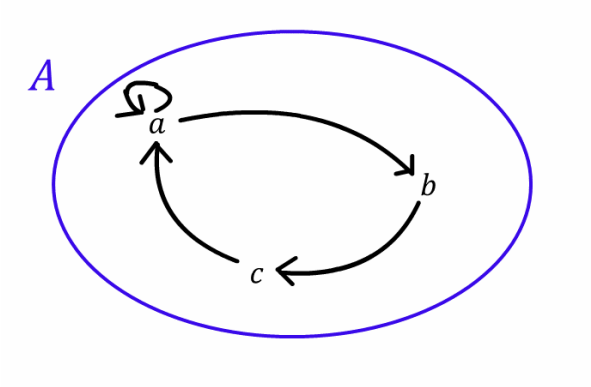


Figura 2.1: Relazione binaria

Esempio 2.1.9. Sia $A = \{a, b, c\}$. La relazione $\mathcal{R} = \{(a, a), (a, b), (b, b), (b, c), (c, c)\}$ è riflessiva, mentre non lo è $\mathcal{R}' = \{(a, a), (a, c), (b, c), (c, c)\}$, dato che non contiene la coppia (b, b). Le matrici di adiacenza delle due relazioni sono le seguenti:

$\mathcal{R}$	a	b	c
a	×	×	
b		×	×
c			×

$\mathcal{R}'$	a	b	c
a	×		×
b			×
c			×

Altri esempi di relazioni riflessive sono le relazioni numeriche descritte nell'esempio 2.1.4.

Definizione 2.1.10. Sia $\mathcal{R}$ una relazione definita su A. $\mathcal{R}$ è **simmetrica** se per ogni $x, y \in A$ se x è in relazione con y, allora y è in relazione con x, cioè:

$$\forall x, y \in A,\ x\mathcal{R}y \Rightarrow y\mathcal{R}x\,. \tag{2.1}$$

Come possiamo capire quando una relazione NON è simmetrica? Dobbiamo considerare la negazione della formula (2.1): quindi devono esistere x e y (dei controesempi) tali che non vale l'implicazione $x\mathcal{R}y \Rightarrow y\mathcal{R}x$. Ma quando non è valida una implicazione? Quando $x\mathcal{R}y$ ma $y\ \mathcal{R}x$. Quindi una relazione NON è simmetrica se esistono x e y tali che x è in relazione con y ma y non è in relazione con x.

Nella rappresentazione con il diagramma di Venn, una relazione è simmetrica se ogni volta che un elemento è collegato con un altro, allora ci deve essere anche un collegamento *di ritorno*, quindi tra due elementi o non ci sono collegamenti o ce ne sono due, uno in una direzione e uno nell'altra. Nella rappresentazione con la matrice di adiacenza, una relazione è simmetrica se le caselle segnate sono simmetriche rispetto alla diagonale che va dall'alto a sinistra al basso a destra.

Esempio 2.1.11. Dato l'insieme $A = \{1, 2, 3\}$, la relazione $\{(1, 2), (2, 1), (2, 3), (3, 2)\}$ è simmetrica mentre la relazione $\{(1, 2), (1, 3), (2, 3), (3, 2)\}$ non lo è. Le matrici

di adiacenza sono le seguenti:

$\mathcal{R}$	1	2	3
1		×	
2	×		×
3		×	

$\mathcal{R}$	1	2	3
1		×	×
2			×
3		×	

Come si può modificare la seconda relazione in modo che sia simmetrica?

La relazione uguaglianza è banalmente simmetrica, al contrario delle relazioni di minore o uguale e di divisibilità. Ad esempio, 3 è minore di 5, ma 5 non è minore di 3 e 6 divide 12, ma 12 non divide 6.

Definizione 2.1.12. Sia $\mathcal{R}$ una relazione definita su A. $\mathcal{R}$ è **transitiva** se, per ogni $x, y, z \in A$ se x è in relazione con y e y è in relazione con z, allora anche x è in relazione con z, cioè:

$$\forall x, y, z \in A,\ x\mathcal{R}y \wedge y\mathcal{R}z \Rightarrow x\mathcal{R}z\,.$$

Anche in questo caso cerchiamo di capire quando una relazione NON è transitiva: devono esistere x, y e z tali che l'implicazione $x\mathcal{R}y \wedge y\mathcal{R}z \Rightarrow x\mathcal{R}y$ non sia valida, cioè tali che pur essendo $x\mathcal{R}y$ e $y\mathcal{R}z$ non valga $x\mathcal{R}z$.

La proprietà transitiva non è facilmente controllabile con la matrice di adiacenza e con il diagramma di Venn, bisogna andare direttamente a verificare che valgano le relazioni come nella definizione.

Esempio 2.1.13. La relazione $\{(1,2)(2,2)(2,3),(1,3),(2,3)\}$ su $\{1,2,3\}$ è transitiva, mentre invece la relazione $\{(1,2)(2,2)(2,3),(1,3),(3,1),(2,3)\}$ non lo è perché 2 è in relazione con 3, 3 è in relazione con 1 ma 2 non è in relazione con 1.

L'insieme delle parole su un dato alfabeto

Introduciamo la definizione di stringa o parola su un alfabeto. Un **alfabeto** è un insieme A e una **stringa** o **parola** su A è una sequenza di elementi di A. Per esempio, se $A = \{a, b, c\}$, allora le sequenze $aabb$, aba e bb sono delle parole su A. Indichiamo con A^+ l'insieme di tutte le parole su A. La **lunghezza** di una parola u di A^+ è il numero di lettere che ricorrono in u e si indica con il simbolo $\#u$. Il numero di volte che una lettera x compare in una parola u si indica con $\#(x, u)$. Per esempio $\#(a, abca) = 2$ e $\#(b, abca) = 1$. Chiaramente $\#(a, u) \leq \#u$.

Definiamo ora una relazione $\mathcal{R}$ sull'insieme delle parole su un alfabeto A: siano $u, v \in A^+$,

$$u\mathcal{R}v \text{ se e solo se } \#u \leq \#v.$$

Si verifica facilmente che $\mathcal{R}$ è riflessiva (perché ogni parola è in relazione con se stessa, dato che ha la stessa lunghezza di se stessa), non è simmetrica (ad esempio, se $A = \{a\}$, allora $a\mathcal{R}aa$, ma non è vero che $aa\mathcal{R}a$), e infine è transitiva (perché se $\#u \leq \#v$ e $\#v \leq \#w$ allora sarà anche $\#u \leq \#w$, per la proprietà transitiva di $\leq$).

Una parola u è **prefisso** di v, se esiste un'altra parola w tale che $v = uw$. Ad esempio, se $A = \{a, b, c\}$, allora la stringa aa è prefisso della stringa $aababa$. Consideriamo una parola speciale di lunghezza 0 chiamata **parola vuota** e indicata con ϵ. Per ogni parola u possiamo scrivere $u = u\epsilon = \epsilon u$, quindi utilizzando la parola vuota possiamo dire che ogni parola è prefisso di se stessa (e anche che la parola vuota ϵ è prefisso di ogni altra parola).

Indichiamo con A^* l'insieme delle parole sull'alfabeto A a cui aggiungiamo anche la parola vuota, cioè

$$A^* = A^+ \cup \{\epsilon\}.$$

Definiamo un'altra relazione $\mathcal{R}_1$ su A^*: siano $u, v \in A^*$,

$$u\mathcal{R}_1 v \text{ se e solo se } u \text{ è prefisso di } v.$$

È facile verificare, anche in questo caso, che $\mathcal{R}_1$ è riflessiva (ogni parola è prefisso di se stessa), ed è transitiva (se u è un prefisso di v e v è un prefisso di w allora anche u è un prefisso di w), ma non è simmetrica (per esempio a è un prefisso di ab ma ab non è un prefisso di a).

Consideriamo $a \in A$ e $u \in A^+$ e indichiamo con $\#(a, u)$ il numero di volte in cui la lettera a occorre in u. Ad esempio, $\#(a, aab) = 2$ e $\#(a, bbc) = 0$.

Possiamo ora definire la relazione $\mathcal{R}_2$ su A^+: siano $u, v \in A^+$,allora

$$u\mathcal{R}_2 v \text{ se e solo se } \#(a, u) = \#(a, v).$$

$\mathcal{R}_2$, come $\mathcal{R}$ e $\mathcal{R}_1$ è riflessiva e transitiva, ma in più è anche simmetrica. Approfondiremo questo tipo di relazioni nella prossima sezione.

2.1.2 Relazioni d'equivalenza

Definizione 2.1.14. Una relazione $\mathcal{R}$ su A è una **relazione di equivalenza** se è riflessiva, simmetrica e transitiva.

La relazione di uguaglianza è una relazione di equivalenza, così come la relazione $\mathcal{R}_2$ sull'insieme delle parole, mentre le relazioni $\mathcal{R}$, $\mathcal{R}_1$ sull'insieme delle parole non lo sono.

Esempio 2.1.15. Sia $A = \{a, b, c\}$ e $\mathcal{R} = \{(a, a), (a, b), (b, a), (b, b), (c, c)\}$. La relazione $\mathcal{R}$ è una relazione d'equivalenza perché è riflessiva (infatti $(a, a), (b, b), (c, c) \in$

$\mathcal{R}$), simmetrica dato che:

$$\begin{array}{lll} (a,a) \in \mathcal{R} & \text{implica} & (a,a) \in \mathcal{R} \\ (a,b) \in \mathcal{R} & \text{implica} & (b,a) \in \mathcal{R} \\ (b,a) \in \mathcal{R} & \text{implica} & (a,b) \in \mathcal{R} \\ (b,b) \in \mathcal{R} & \text{implica} & (b,b) \in \mathcal{R} \\ (c,c) \in \mathcal{R} & \text{implica} & (c,c) \in \mathcal{R} \end{array}$$

e transitiva dato che:

$$\begin{array}{llll} (a,a) \in \mathcal{R} & \text{e} & (a,b) \in \mathcal{R} & \text{implica} \quad (a,b) \in \mathcal{R} \\ (a,b) \in \mathcal{R} & \text{e} & (b,a) \in \mathcal{R} & \text{implica} \quad (a,a) \in \mathcal{R} \\ (a,b) \in \mathcal{R} & \text{e} & (b,b) \in \mathcal{R} & \text{implica} \quad (a,b) \in \mathcal{R} \\ (b,a) \in \mathcal{R} & \text{e} & (a,a) \in \mathcal{R} & \text{implica} \quad (b,a) \in \mathcal{R} \\ (b,a) \in \mathcal{R} & \text{e} & (a,b) \in \mathcal{R} & \text{implica} \quad (b,b) \in \mathcal{R} \\ (b,b) \in \mathcal{R} & \text{e} & (b,a) \in \mathcal{R} & \text{implica} \quad (b,a) \in \mathcal{R} \end{array}$$

Nel seguito non andremo più a verificare la simmetria e la transitività per le coppie con prima e seconda componente uguale, perchè è banalmente verificata.

Esempio 2.1.16. La relazione $\{(1,1),(2,2),(3,3),(1,3),(3,1)\}$ definita su $\{1,2,3\}$. R è una relazione di equivalenza.

Esempio 2.1.17. Sia $\mathcal{R} = \{(n,m) \in \mathbb{N} \times \mathbb{N} : n+m \text{ è pari }\}$ e verifichiamo che $\mathcal{R}$ è una relazione d'equivalenza su $\mathbb{N}$. Osserviamo che $n \in \mathbb{N}$ è un numero pari se e solo se è un multiplo di 2 e cioè se esiste $k \in \mathbb{N}$ tale che $n = 2k$. A questo punto è facile provare che:

- $\mathcal{R}$ è riflessiva, dato che $n + n = 2n$, per ogni $n \in \mathbb{N}$;
- $\mathcal{R}$ è simmetrica, perchè se $n + m = 2i$, con $i \in \mathbb{N}$, allora anche $m + n = 2i$ (la somma di numeri naturali è commutativa).
- $\mathcal{R}$, infine, è transitiva: se $n + m = 2i$ e $m + l = 2j$, con $i, j \in \mathbb{N}$, allora $n + m + m + l = 2(i + j)$ e $n + l = 2(i + j) - 2m = 2(i + j - m)$, con $i + j - l \in \mathbb{N}$.

Esempio 2.1.18. Sia $X = \{a,b,c\}$ e $\mathcal{R}$ la relazione su $\mathcal{P}(X)$ uguale all' insieme delle coppie dei sottoinsiemi di X che hanno la stessa cardinalità: se $A, B \in \mathcal{P}(X)$, allora

$$A\mathcal{R}B \text{ se e solo se } |A| = |B|.$$

Si verifica facilmente che $\mathcal{R}$ è una relazione di equivalenza.

Esempio 2.1.19. Consideriamo la relazione di "essere multiplo " tra numeri naturali, cioè la relazione data dall'insieme $\{(n, m) \in \mathbb{N} \times \mathbb{N} : n \text{ è multiplo di } m\}$. Questa relazione è riflessiva, perché ogni numero è un multiplo di se stesso. Inoltre è transitiva, perché se n è un multiplo di m e m è un multiplo di h allora anche n è un multiplo di h. Ma non è simmetrica: infatti se n è un multiplo di m allora non è detto che m sia un multiplo di n, anzi questo vale solo nel particolare caso in cui $n = m$. Quindi la relazione di essere multiplo non è una relazione d'equivalenza.

Se $\mathcal{R}$ è una relazione d'equivalenza su un insieme A, posso raggruppare gli elementi di A tra di loro equivalenti. Consideriamo la relazione nell'Esempio 2.1.18: la relazione di avere la stessa cardinalità permette di raggruppare i sottoinsiemi di X nel seguente modo:

- Tutti i sottoinsiemi con 1 elemento sono equivalenti tra di loro: $\{a\}, \{b\}$ e $\{c\}$;
- Tutti i sottoinsiemi con 2 elementi sono eequivalenti tra di loro: $\{a, b\}$, $\{b, c\}$ e $\{a, c\}$;
- L'insieme vuoto $\{\}$ è equivalente solo a se stesso (è l'unico con 0 elementi);
- L'insieme X è equivalente solo a se stesso (è l'unico con 3 elementi).

Diamo allora la seguente definizione:

Definizione 2.1.20. Sia $\mathcal{R}$ una relazione di equivalenza sull'insieme A. La **classe di equivalenza** di $a \in A$ rispetto ad $\mathcal{R}$ è l'insieme degli elementi di A che sono in relazione con a. In simboli $[a]_{\mathcal{R}} = \{b \in A : a\mathcal{R}b\}$.

Definizione 2.1.21. L'**insieme quoziente** di un insieme A, rispetto a una relazione di equivalenza R di A, è l'insieme di tutte le classi di equivalenza di A rispetto a $\mathcal{R}$ e si indica con $A/\mathcal{R}$.

Esempio 2.1.22. Le classi di equivalenza della relazione

$$\mathcal{R} = \{(1,1), (2,2), (3,3), (4,4), (1,3), (3,1), (2,4), (4,2)\}$$

su $A = \{1, 2, 3, 4\}$ sono: $[1]_{\mathcal{R}} = \{1, 3\}$, $[2]_{\mathcal{R}} = \{2, 4\}$, $[3]_{\mathcal{R}} = \{1, 3\}$ e $[4]_{\mathcal{R}} = \{2, 4\}$. L'insieme quoziente $A/\mathcal{R}$ è $\{[1]_{\mathcal{R}}, [2]_{\mathcal{R}}\}$ dato che $[3]_{\mathcal{R}} = [1]_{\mathcal{R}}$ e $[4]_{\mathcal{R}} = [2]_{\mathcal{R}}$.

Esempio 2.1.23. Sia $\mathcal{P}(X) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}\}$ l'insieme delle parti di $X = \{a, b, c\}$ e $\mathcal{R}$ la seguente relazione: $A\mathcal{R}B$ se e solo se $|A| = |B|$. Le classi di equivalenza di $\mathcal{R}$ sono quattro: $[\{a\}]_{\mathcal{R}} = [\{b\}]_{\mathcal{R}} = [\{c\}]_{\mathcal{R}} = \{\{a\}, \{b\}, \{c\}\}$, $[\{a, b\}]_{\mathcal{R}} = \{\{a, b\}, \{b, c\}, \{a, c\}\}$, $[\emptyset]_{\mathcal{R}} = \{\emptyset\}$ e $[\{a, b, c\}]_{\mathcal{R}} = \{\{a, b, c\}\}$.

Esempio 2.1.24. Sia $\mathcal{R}$ la seguente relazione su $\mathbb{Z}$: $n\mathcal{R}m$ se e solo se $|n| = |m|$ (in questo caso con questa notazione si intende il valore assoluto), allora $\mathbb{Z}/\mathcal{R} = \{[n]_\mathcal{R} | n \in \mathbb{Z}\} = \{\{-n, n\} | n \in \mathbb{N}\}$.

Per capire le proprietà degli insiemi quozienti, diamo la seguente definizione:

Definizione 2.1.25. Si dice **partizione** di un insieme A una famiglia $\mathcal{F}$ di sottoinsiemi di A tale che

1. Ogni $X \in \mathcal{F}$ è diverso dall'insieme vuoto, $X \neq \emptyset$,
2. Gli elementi di $\mathcal{F}$ sono disgiunti, cioè per ogni $X, Y \in \mathcal{F}$, se $X \neq Y$ allora $X \cap Y = \emptyset$,
3. L'unione degli elementi di $\mathcal{F}$ è tutto l'insieme A, cioè $\bigcup_{X \in \mathcal{F}} X = A$.

Gli elementi di una partizione sono chiamati anche **blocchi** della partizione.

Esempio 2.1.26. Se $A = \{1, 2, 3, 4\}$, allora $\mathcal{F} = \{\{1, 2\}, \{3, 4\}\}$ è una partizione di A, in quanto tutti gli elementi di $\mathcal{F}$ sono diversi dall'insieme vuoto, $\{1, 2\} \cap \{3, 4\} = \emptyset$ e $\{1, 2\} \cup \{3, 4\} = \{1, 2, 3, 4\}$. L'insieme $\mathcal{F}' = \{\{1\}, \{2, 3\}\}$, invece, non è una partizione di A, infatti $\{1\} \cup \{2, 3\} \neq A$.

Teorema 2.1.27. *Sia $\mathcal{R}$ una relazione di equivalenza su A, allora $A/\mathcal{R}$ è una partizione di A. Viceversa, se $\mathcal{F}$ è una partizione di A allora la relazione $R_\mathcal{F}$ su A data da:*

$$x\mathcal{R}_\mathcal{F}y \text{ se e solo se } x \text{ e } y \text{ appartengono allo stesso blocco di } \mathcal{F}$$

è una relazione d'equivalenza tale che $A/\mathcal{R}_\mathcal{F} = \mathcal{F}$.

Dimostrazione. Per provare che $A/\mathcal{R}$ sia una partizione, dobbiamo prova che verifichi tutte le proprietà di una partizione:

1. Sia $a \in A$, allora $a \in [a]_\mathcal{R}$, poichè $\mathcal{R}$ è riflessiva, quindi $[a]_\mathcal{R} \neq \emptyset$.
2. Siano $a, b \in A$ e supponiamo che esista un elemento c che appartenga a $[a]_\mathcal{R} \cap [b]_\mathcal{R}$. Quindi $a\mathcal{R}c$ e $b\mathcal{R}c$ e per la proprietà simmetrica di $\mathcal{R}$, anche $c\mathcal{R}b$. Per la proprietà transitiva, da $a\mathcal{R}c$ e $c\mathcal{R}b$ segue che $a\mathcal{R}b$, quindi $[a]_\mathcal{R} = [b]_\mathcal{R}$. Allora possiamo dedurre che se $[a]_\mathcal{R} \neq [b]_\mathcal{R}$, cioè se $[a]_\mathcal{R}$ e $[b]_\mathcal{R}$ sono due elementi diversi di $A/\mathcal{R}$, allora non ci possono essere elementi nella loro intersezione e quindi $[a]_\mathcal{R} \cap [b]_\mathcal{R} = \emptyset$.
3. Per ogni $b \in A$ si ha $b \in [b]_\mathcal{R}$ per la proprietà riflessiva, quindi b appartiene anche all'unione di tutte le classi d'equivalenza, cioè $b \in \bigcup_{a \in A}[a]_\mathcal{R}$ e quindi $A \subseteq \bigcup_{a \in A}[a]_\mathcal{R}$. D'altra parte, se $b \in \bigcup_{a \in A}[a]_\mathcal{R}$, allora esiste $[a]_\mathcal{R} \in A/\mathcal{R}$ che contiene b, ma $[a]_\mathcal{R} \subseteq A$ quindi $b \in A$ e $\bigcup_{a \in A}[a]_\mathcal{R} \subseteq A$. Quindi, avendo dimostrato la doppia inclusione, si ha che $A = \bigcup_{a \in A}[a]_\mathcal{R}$.

Viceversa, per provare che $\mathcal{RF}$ sia una relazione d'equivalenza, dobbiamo provare che sia riflessiva, simmetrica e transitiva. Ma dato che ogni elemento appartiene allo stesso blocco di se stesso, la relazione è sicuramente riflessiva. Se x appartiene allo stesso blocco di y allora anche y appartiene allo stesso blocco di x e quindi la relazione è simmetrica. Per finire, se x e y appartengono allo stesso blocco, e y e z appartengono allo stesso blocco, allora anche x e z appartengono allo stesso blocco e quindi la relazione è transitiva.

Per provare che $A/\mathcal{R}_\mathcal{F} = \mathcal{F}$, consideriamo che per ogni $a \in A$

$$[a]_{\mathcal{R}_\mathcal{F}} = \{b \in A \mid \ a \text{ e } b \text{ appartengono allo stesso blocco}\}$$

quindi $[a]_{\mathcal{R}_\mathcal{F}}$ è composta da tutti gli elementi che appartengono ad uno stesso blocco e quindi coincide con un blocco della partizione. Inoltre se $B \in \mathcal{F}$ allora $B \neq \emptyset$ e quindi esiste un elemento $b \in B$ e $[b]_{\mathcal{R}_\mathcal{F}} = B$ perché $[b]_{\mathcal{R}_\mathcal{F}}$ è formata da tutti gli elementi che, essendo il relazione con b, appartengono allo stesso blocco di b. Quindi $F = A/\mathcal{R}_\mathcal{F}$.

Esempio 2.1.28. Consideriamo l'insieme A^4 delle parole di lunghezza 4 sull'alfabeto $A = \{a, b, c\}$ e la relazione $\mathcal{R}$ tale che due parole u e v di A^4 sono in relazione tra di loro se contengono lo stesso numero di lettere a. Per esempio le parole *aabc* e *bbaa* sono in relazione tra di loro perché contengono entrambe due lettere a mentre invece *abac* e *bcac* non lo sono. Quante classi d'equivalenza ci sono?

- $[bbcc]$ è la classe d'equivalenza che contiene tutte le parole che non hanno lettere a;
- $[abcc]$ è la classe d'equivalenza che contiene tutte le parole che hanno 1 lettera a;
- $[aacc]$ è la classe d'equivalenza che contiene tutte le parole che hanno 2 lettere a;
- $[aaac]$ è la classe d'equivalenza che contiene tutte le parole che hanno 3 lettere a;
- $[aaaa]$ è la classe d'equivalenza che contiene tutte le parole che hanno 4 lettere a e cioè contiene solo la parola *aaaa*.

Ci sono quindi 5 classi d'equivalenza, quindi la relazione $\mathcal{R}$ partiziona l'insieme A^4 in 5 blocchi.

Esempio 2.1.29. Consideriamo la seguente partizione dell'insieme $X = \{a, b, c, d, e\}$:

$$\mathcal{F} = \{\{a, b\}, \{c\}, \{d, e\}\}.$$

La relazione d'equivalenza associata ad $\mathcal{F}$ è la seguente:

$$\mathcal{R}_\mathcal{F} = \{(a, a), (b, b), (a, b), (b, a), (c, c), (d, d), (e, e), (d, e), (e, d)\}.$$

2.1.3 Relazioni d'ordine

Definizione 2.1.30. Sia $\mathcal{R}$ una relazione definita su A. $\mathcal{R}$ è **antisimmetrica** se per ogni $x, y \in A$ se x è in relazione con y e y è in relazione con x, allora $x = y$, cioè:

$$\forall x, y \in A,\ x\mathcal{R}y \text{ AND } y\mathcal{R}x \Rightarrow x = y\,. \tag{2.2}$$

Quindi una relazione è antisimmetrica se per due elementi diversi x e y non possono valere contemporaneamente $x\mathcal{R}y$ e $y\mathcal{R}x$.

Una relazione $\mathcal{R}$ NON è antisimmetrica quando esistono due elementi diversi tra di loro x e y tali che $x\mathcal{R}y$ e $y\mathcal{R}x$. Nel diagramma di Venn, questo corrisponde ad avere due elementi distinti che sono collegati in entrambe le direzioni.

Esempio 2.1.31. Se $A = \{a, b, c\}$ la relazione $R = \{(a, a), (b, b), (b, c), (a, b)\}$ è una relazione antisimmetrica, mentre la relazione $R_1 = \{(a, a), (b, b), (b, c), (a, b), (b, a)\}$ non è antisimmetrica: aR_1b e bR_1a ma $a \neq b$.

Una relazione R su A si dice una **relazione d'ordine** se è riflessiva, antisimmetrica e transitiva.

Esempio 2.1.32.

- La relazione di minore o uguale tra numeri è una relazione d'ordine.
- La relazione di essere multiplo tra numeri interi è una relazione d'ordine: è riflessiva perché ogni numero è multiplo di se stesso; è transitiva perché se n è un multiplo di m e m è un multiplo di h allora anche n è un multiplo di h; ed è antisimmetrica, perché se n è un multiplo di m e m è un multiplo di n allora l'unica possibilità è che sia $n = m$.
- La relazione di inclusione tra insiemi è una relazione d'ordine: ogni insieme è incluso in se stesso; se $A \subseteq B$ e $B \subseteq A$ allora $A = B$; se $A \subseteq B$ e $B \subseteq C$ allora $A \subseteq C$.

Per analogia con la relazione d'ordine usuale sui numeri, di solito per tutte le relazioni d'ordine si usa la stessa terminologia del $\leq$, quindi se $x\mathcal{R}y$ (con $\mathcal{R}$ relazione d'ordine) si dirà che x è *più piccolo* di y (rispetto a $\mathcal{R}$), e che analogamente y è *più grande* di x.

Definizione 2.1.33. Se R è una relazione d'ordine su A e per ogni $x, y \in A$ si ha che xRy oppure yRx, allora R si dice che è una relazione d'ordine totale su A (tutti gli elementi sono *confrontabili* tra di loro).

Per esempio la relazione d'ordine del minore o uguale è una relazione totale sull'insieme dei numeri interi, mentre la relazione di essere multiplo non lo è.

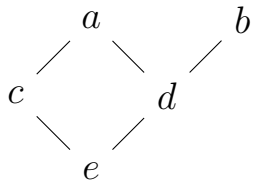
Un **insieme ordinato** $(S, \mathcal{R})$ è un insieme con una relazione d'ordine $\mathcal{R}$.

Esempio 2.1.34. Sull'insieme A^* delle parole sull'alfabeto $A = \{a, b, c\}$ si consideri la relazione $u\mathcal{R}v$ se e solo se $\#u \leq \#v$ (o, detto in altro modo, $\mathcal{R} = \{(u, v) \mid \#u \leq \#v\}$). La relazione $\mathcal{R}$ non è una relazione antisimmetrica, perché per esempio la parola $u = aabc$ è in relazione con $v = bacb$ dato che $\#u \leq \#v$, e anche $v\mathcal{R}u$ dato che $\#v \leq \#u$, ma $u \neq v$. Quindi non è una relazione d'ordine.

Diagrammi di Hasse

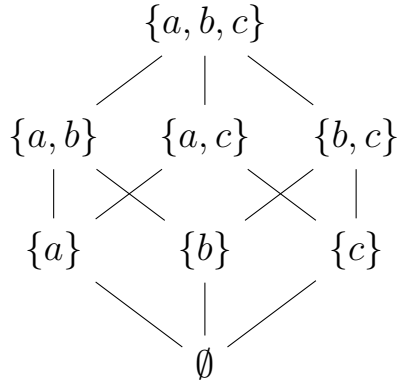
Le relazioni d'ordine sugli insiemi finiti possono essere rappresentate tramite i diagrammi di Hasse, che sono una modifica del diagramma di Venn dove vengono evidenziate solo alcune delle coppie in relazione. Nei diagrammi di Hasse infatti rappresentiamo gli elementi dell'insieme su cui è definita la relazione come punti del piano, la relazione d'ordine è rappresentata solo tra coppie di elementi di un certo tipo: si disegna un arco tra un elemento x e un elemento y solo se y *copre* x, cioè se xRy e non esiste nessun altro z diverso da x e y tale che $xRzRy$. In particolare non sono segnate le relazioni di ogni elemento con se stesso. Inoltre di solito si mettono più in basso gli elementi più piccoli (rispetto a $\mathcal{R}$). In altri termini, nel diagramma di Hasse si trascura di disegnare gli archi che testimoniano la riflessività e la transitività.

Esempio 2.1.35. La relazione $\mathcal{R} = \{(a, a), (b, b), (c, c), (d, d), (e, e), (c, a), (e, c), (e, a), (d, a), (d, b), (e, d), (e, b)\}$ è una relazione d'ordine su $\{a, b, c, d, e\}$ ed ha il seguente diagramma di Hasse:



Come sarebbe il diagramma se si disegnassero tutte le coppie in relazione?

Esempio 2.1.36. La relazione di inclusione su $\mathcal{P}(\{a, b\})$ ha il seguente diagramma di Hasse:



Definizione 2.1.37. In un insieme ordinato $(S, \mathcal{R})$ diciamo che un elemento $x \in S$ è il MINIMO se per ogni $y \in S$ si ha $x\mathcal{R}y$. Invece x è il MASSIMO se per ogni $y \in S$, $y\mathcal{R}x$.

Non sempre minimo e massimo esistono, ma se esistono allora sono unici.

Nell'esempio 2.1.35 l'elemento e è il minimo, perché ogni altro elemento è più grande. Non c'è un massimo perché tra a e b non c'è un più grande. Nell'esempio 2.1.36 il minimo è $\emptyset$ e il massimo è $\{a, b, c\}$.

Definizione 2.1.38. In un insieme ordinato $(S, \mathcal{R})$ diciamo che un elemento $x \in S$ è un MINIMALE se non esiste $y \in S$ tale che $y\mathcal{R}x$, cioè non esistono elementi più piccoli di x. Invece x è un MASSIMALE se non esiste $y \in S$ tale che $x\mathcal{R}y$, cioè non esistono elementi più grandi di x.

Nell'esempio 2.1.35 gli elementi a e b sono massimali.

Proposizione 2.1.39. *Se un insieme ordinato $(S, \mathcal{R})$ ha un unico elemento massimale M allora M è un massimo per S. Se ha un unico elemento minimale m allora m è un minimo m per S.*

Definizione 2.1.40. Se $(S, \mathcal{R})$ è un insieme ordinato e X è un sottoinsieme di S, l'*estremo inferiore* di X in S è il massimo tra gli elementi di S che sono più piccoli di tutti gli elementi di X, cioè

$$\inf X = \max\{y \in S \mid y\mathcal{R}x \text{ per ogni } x \in X\}\,.$$

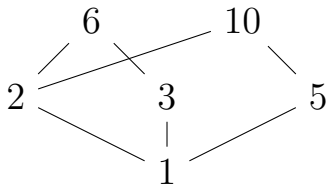
L'estremo inferiore potrebbe non esistere.

Analogamente, l'*estremo superiore* di X in S è il minimo tra gli elementi di S che sono più grandi di tutti gli elementi di X, cioè

$$\sup X = \min\{y \in S \mid x\mathcal{R}y \text{ per ogni } x \in X\}\,.$$

L'estremo superiore potrebbe non esistere.

Esempio 2.1.41. Consideriamo l'insieme $S = \{1, 2, 3, 5, 6, 10\}$ con la relazione di divisibilità, cioè $n\mathcal{R}m$ se m è un multiplo di n. Il diagramma di Hasse di questo insieme ordinato è



S ha un minimo che è 1 e due elementi massimali che sono 6 e 10. Consideriamo il sottoinsieme $X = \{2, 3, 5\}$. Si ha $\inf X = 1$ mentre $\sup X$ non esiste. Infatti

$$\{y \in S \mid y\mathcal{R}x \text{ per ogni } x \in X\} = \{1\}$$

e

$$\{y \in S \mid x\mathcal{R}y \text{ per ogni } x \in X\} = \emptyset\,.$$

2.2 Funzioni

Definizione 2.2.1. Una relazione $f \subseteq A \times B$ è una **funzione** dall'insieme A all'insieme B se per ogni $a \in A$ esiste un unico $b \in B$ per cui $(a, b) \in f$ (in simboli $f(a) = b$). L'elemento b è detto **immagine** di a e l'elemento a **controimmagine** di b.

Per indicare che f è una funzione di A in B si scrive

$$f : A \to B.$$

Per dire quali sono le coppie in relazione tramite la funzione f, scriveremo $f(a) = b$ oppure anche $f : a \mapsto b$. Talvolta, soprattutto quando si ha a che fare con insiemi infiniti, scriveremo

$$f : a \in A \mapsto f(a) \in B\,.$$

L'insieme A si chiama **dominio** (o **campo di esistenza**) di f e l'insieme B **codominio** di f.

Esempio 2.2.2. La relazione $f = \{(a, 2), (b, 1), (c, 2)\}$ è una funzione tra $\{a, b, c\}$ e $\{1, 2\}$. Scriviamo $f : \{a, b, c\} \to \{1, 2\}$ e $f(a) = 2$, $f(b) = 1$, $f(c) = 2$, oppure anche

$$\begin{aligned} f : \ & a \mapsto 2 \\ & b \mapsto 1 \\ & c \mapsto 2 \end{aligned}$$

La relazione $\{(n, 3n) \mid n \in \mathbb{N}\}$ è una funzione che ha $\mathbb{N}$ come dominio e $3\mathbb{N}$ come codominio. Si può anche scrivere

$$f : n \in \mathbb{N} \mapsto 3n \in 3\mathbb{N}\,.$$

Possiamo rappresentare una funzione con i diagrammi di Venn, considerando i diagrammi di dominio e codominio e poi collegando con una freccia gli elementi del dominio che sono in relazione con quelli del codominio. La definizione di funzione assicura che da ogni elemento del dominio parta una ed una sola freccia.

Esempio 2.2.3.

- La relazione $\{(a, 2), (b, 1), (c, 2)\}$ tra $A = \{a, b, c\}$ e $B = \{1, 2\}$ è una funzione perché ogni elemento di A si trova come prima componente di una sola coppia (vedi Figura 2.2). La relazione $\{(a, 1), (a, 2), (b, 1), (c, 1)\}$ invece non è una funzione perché l'elemento $a \in A$ si trova come prima componente di due coppie. Neanche la relazione $\{(a, 1), (b, 2)\}$ è una funzione perché non contiene nessuna coppia che abbia c come prima componente.

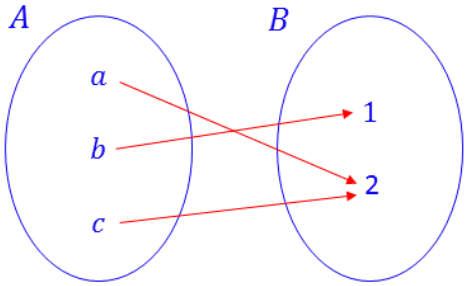


Figura 2.2: Funzione $f : \{a, b, c\} \to \{1, 2\}$

- La funzione $f : A \to A$ tale che $f(a) = a$ per ogni $a \in A$, si chiama funzione **identica** di A (o **identità**) e si denota anche con id_A. Corrisponde alla relazione di uguaglianza $\{(a, a) \mid a \in A\}$.
- Fissato un elemento $c \in A$, la funzione $f_c : A \to A$ tale che $f_c(a) = c$ per ogni $a \in A$, si chiama funzione **costante**. Corrisponde alla relazione $\{(a, c) \mid a \in A\}$.

Definizione 2.2.4. Se $f : A \to B$ e $C \subseteq A$, l'**immagine** di C tramite f è l'insieme $f(C) = \{f(c) \mid c \in C\} \subseteq B$. Se invece $D \subseteq B$, la **controimmagine** di D tramite f è l'insieme $f^{-1}(D) = \{a \in A \mid f(a) = d \text{ per qualche } d \in D\}$.

Per esempio, se $f : \{a, b, c, d, e\} \to \{1, 2, 3, 4\}$ è definita da $f(a) = 2$, $f(b) = 4$, $f(c) = 1$, $f(d) = 2$ e $f(e) = 1$, allora l'immagine di A è $f(A) = \{1, 2, 4\}$, la controimmagine di $\{1, 2\}$ è $f^{-1}(\{1, 2\}) = \{a, c, d, e\}$. Nota che la controimmagine del codominio è sempre tutto il dominio.

Definizione 2.2.5. Una funzione $f : A \to B$ si dice

- ~~**iniettiva**~~ se $\forall x, y \in A, x \neq y \Rightarrow f(x) \neq f(y)$; in altre parole non possono esserci frecce che partono da due elementi diversi del dominio e arrivano nello stesso elemento del codominio.
- **suriettiva** se $\forall y \in B, \exists x \in A : f(x) = y$; in altre parole in tutti gli elementi del codominio deve arrivare una freccia. In questo caso l'immagine di A coincide con B.
- **biettiva** se è iniettiva e suriettiva.

Esempio 2.2.6. La funzione $f : A \to B$ in Figura 2.2 è suriettiva, ma non iniettiva, dato che $f(a) = f(c) = 2$ e $f(b) = 1$.

Esempio 2.2.7. La funzione $g : B \to A$ in Figura 2.3 è iniettiva, ma non suriettiva, infatti $g(1) = b$ e $g(2) = a$ e c non ha controimmagine.

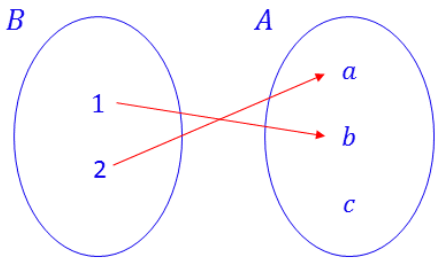


Figura 2.3: Funzione g iniettiva

Utilizziamo il simbolo B^A per denotare l' insieme di tutte le possibili funzioni dall'insieme A all' insieme B. Osserviamo che se $|A| < |B|$, allora non esistono funzioni suriettive in B^A, invece nel caso in cui $|A| > |B|$, B^A non contiene funzioni iniettive.

Definizione 2.2.8. Due insiemi A e B si dicono **equipotenti** se esiste una funzione biettiva tra A e B. Due insiemi equipotenti finiti hanno lo stesso numero di elementi.

Per esempio, gli insiemi $A = \{a, b, c\}$ e $B = \{1, \{a\}, 2\}$ sono equipotenti, perché esiste una funzione biettiva tra A e B, per esempio $f : A \to B$ tale che $f(a) = 1$, $f(b) = 2$, $f(c) = \{a\}$. Nota che non tutte le funzioni tra A e B sono biettive, per esempio la funzione $g(a) = 1$, $g(b) = 1$, $g(c) = 1$ non lo è.

Proposizione 2.2.9. *Se X e Y sono due insiemi finiti, allora valgono i seguenti risultati:*

- *Se $|X| > |Y|$ non esistono funzioni iniettive tra X e Y;*
- *Se $|X| < |Y|$ non esistono funzioni suriettive tra X e Y;*
- *Se $|X| \neq |Y|$ non esistono funzioni biettive tra X e Y.*
- *Se $|X| = |Y|$ e f è una funzione iniettiva tra A e B, allora f è anche suriettiva (e quindi biettiva).*
- *Se $|X| = |Y|$ e f è una funzione suriettiva tra A e B, allora f è anche iniettiva (e quindi biettiva).*

Nota però che se $|X| < |Y|$ possono esistere funzioni iniettive tra X e Y, ma non è detto che tutte le funzioni lo siano. Per esempio, se $X = \{a, b\}$ e $Y = \{1, 2, 3, \}$, la funzione f definita da $f(a) = 1$ e $f(b) = 1$ non è una funzione iniettiva, anche se $|X| < |Y|$. Analogamente se $|X| > |Y|$ possono esistere funzioni suriettive tra X e Y ma non è detto che tutte le funzioni lo siano (per esercizio scrivere una funzione non suriettiva tra $\{1, 2, 3\}$ e $\{a, b\}$). E se $|X| = |Y|$ non è detto che tutte le funzioni tra X e Y siano biettive.

Proposizione 2.2.10. *Se X e Y sono insiemi finiti, allora esistono $|Y|^{|X|}$ funzioni da X a Y.*

Esempio 2.2.11. Se $A = \{a, b\}$, $B = \{1, 2\}$ allora ci sono $2^2 = 4$ funzioni tra A e B che sono le seguenti:

$a \mapsto 1$ $b \mapsto 1$	$a \mapsto 2$ $b \mapsto 2$	$a \mapsto 1$ $b \mapsto 2$	$a \mapsto 2$ $b \mapsto 1$

Quante e quali sono le funzioni tra $\{a, b, c\}$ e $\{1, 2\}$? E quelle tra $\{1, 2\}$ e $\{a, b, c\}$?

Esempio 2.2.12. Siano $A = \{a, b\}$ e $B = \{1\}$, allora esiste un'unica funzione f da A a B, poichè $|B|^{|A|} = 1^2 = 1$, vedi Figura 2.4.

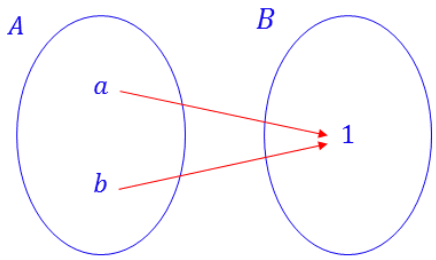


Figura 2.4: Funzione da $\{a, b\}$ a $\{1\}$

Esempio 2.2.13. Il numero di funzioni da $B = \{1\}$ ad $A = \{a, b\}$ è $2^1 = 2$ e non ci sono funzioni suriettive dato che $|B| < |A|$, vedi Figura 2.5.

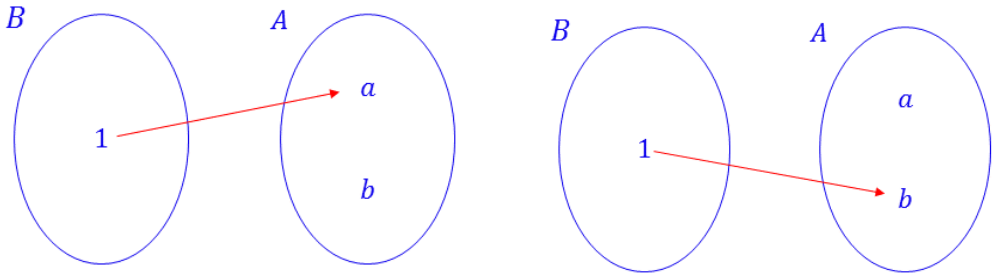


Figura 2.5: Funzioni da $\{1\}$ a $\{a, b\}$

Se una funzione f ha come codominio un insieme che è anche dominio di una funzione g, allora posso considerare di applicare le due funzioni una dietro l'altra, ottenendo ancora una funzione che avrà il dominio di f e il codominio di g, nel seguente modo:

Definizione 2.2.14. Date le funzioni $f : A \to B$ e $g : B \to C$, la **composizione** di f e g è la funzione

$$g \circ f : A \to C$$

tale che $(g \circ f)(a) = g(f(a))$, per ogni $a \in A$.

Esempio 2.2.15. Date le funzioni $f : A \to B$ e $g : B \to C$ come in Figura 2.6 e la loro composta $F = g \circ f$, allora $F(a) = g(f(a)) = h$, $F(b) = g(f(b)) = l$ e $F(c) = g(f(c)) = h$.

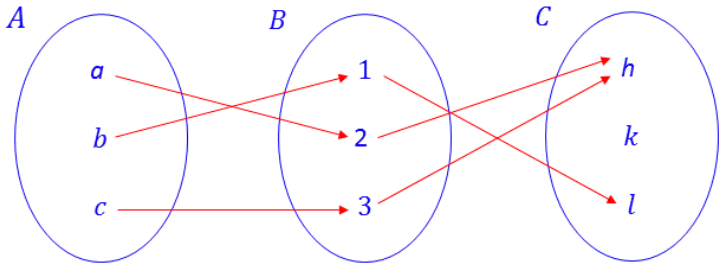


Figura 2.6: Composizione di funzioni

Proposizione 2.2.16. *Sia $f : A \to B$, allora $f \circ id_A = f$ e $id_A \circ f = f$.*

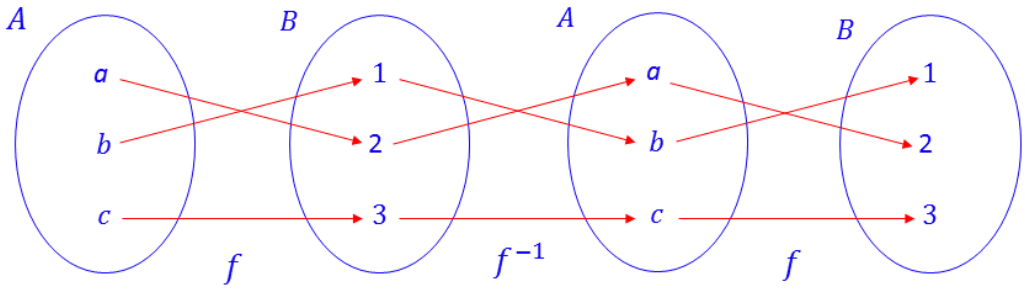


Figura 2.7: Composizione e inversa

Dato che una funzione è una relazione, dalla definizione 2.1.6 possiamo definire per ogni funzione f la sua *relazione inversa* che però in genere non sarà una funzione. Per esempio, se $f : \{a, b, c\} \to \{1, 2\}$ è la funzione data da $f(a) = 1$, $f(b) = 1$ e $f(c) = 2$, allora la relazione inversa di f è data da $f^{-1} = \{(1, a), (1, b), (2, c)\}$ che non è una funzione perché ci sono due coppie che hanno 1 come prima componente. Se però la f è biettiva, allora la sua relazione inversa è una funzione:

Definizione 2.2.17. Sia $f : A \to B$ una funzione biettiva, la funzione **inversa** di f è la funzione f^{-1} tale che per ogni $b \in B$, $f^{-1}(b)$ è l'unico elemento di A che ha b come immagine. Quindi per ogni $a \in A$ e $b \in B$ si ha $f^{-1}(f(a)) = a$ e $f(f^{-1}(b)) = b$, che possiamo anche scrivere come $f \circ f^{-1} = id_B$ e $f^{-1} \circ f = id_A$.

Esempio 2.2.18. Se f è la funzione da $A = \{a, b, c\}$ a $B = \{1, 2, 3\}$ tale che $f(a) = 2, f(b) = 1$, e $f(c) = 3$, allora $f^{-1}(1) = b, f^{-1}(2) = a$ e $f^{-1}(3) = c$ (vedi Figura 2.7).

Esercizio 2.2.19. La funzione $f : x \in \mathbb{N} \mapsto 2x \in 2\mathbb{N}$ è biettiva.
– f è iniettiva: dati $x, y \in \mathbb{N}$, se $x \neq y$, allora $2x \neq 2y$;
– f è suriettiva: dato $z \in 2\mathbb{N}$, allora esiste $h \in \mathbb{N}$ tale che $z = 2h = f(h)$.
f è iniettiva e suriettiva, quindi è anche biettiva. La funzione inversa $f^{-1} : 2\mathbb{N} \to \mathbb{N}$ associa ad ogni numero pari $2n$ il numero n.

Supponiamo che sia $g : 2n \in 2\mathbb{N} \mapsto n + 1 \in \mathbb{N}^+$. Allora la funzione composta $g \circ f$ è tale che $(g \circ f)(n) = g(f(n)) = g(2n) = n + 1$. Nota che g è iniettiva e suriettiva e anche la funzione $f \circ g$ è biettiva.

2.3 Esercizi

1. Sia $A = \{a, b, c\}$. Dire delle seguenti relazioni se sono riflessive, simmetriche, antisimmetriche e transitive:
   - $\mathcal{R}_1 = \{(a, a), (a, b), (b, b)\}$
   - $\mathcal{R}_2 = \{(a, a), (a, b), (b, b), (b, a), (c, c), (c, a)\}$
   - $\mathcal{R}_3 = \{(a, a), (b, b), (c, c)\}$
   - $\mathcal{R}_4 = \{(a, a), (a, b), (b, c), (a, c)\}$
   - $\mathcal{R}_5 = \{(a, a), (a, b), (b, a), (b, b), (b, c), (a, c)\}$
   - $\mathcal{R}_6 = \{(a, a), (b, b), (c, c), (a, c), (c, a)\}$

2. Sia $A = \{a, b, c, d\}$ e consideriamo l'insieme A^3 delle parole di lunghezza 3 sull'alfabeto A. Dimostrare che la relazione $\mathcal{R} = \{(u, v) \in A^3 \times A^3 \mid \#(a, u) + \#(b, u) = \#(a, v) + \#(b, v)\}$ è una relazione d'equivalenza su A^3 e scrivere le classi d'equivalenza (quante ne sono?).

3. Sull'insieme $\mathbb{Z}$ dei numeri interi si consideri la relazione $\mathcal{R}_5$ definita nel seguente modo:

   $$n\mathcal{R}_5 m \text{ se e solo se } n - m \text{ è un multiplo di 5.}$$

   Scrivere alcune coppie di numeri che sono in relazione tra di loro e alcune che invece non sono in relazione. Provare che la relazione $\mathcal{R}_5$ è una relazione d'equivalenza, determinare le classi di equivalenza e l'insieme quoziente.

4. Dire se i seguenti sottoinsiemi di $\mathcal{P}(X)$ sono partizioni di $X = \{a, b, c, d, e\}$:
   - $\{\{c, d\}, \{a, b, c\}, \{e\}\}$
   - $\{\{a\}, \{b\}, \{c, d, e\}\}$
   - $\{\{c, d\}, \{a, b\}, \{e\}\}$
   - $\{\{c\}, \{d\}, \{e\}, \{a\}, \{b\}\}$
   - $\{\{a, d\}, \{c, b, e\}\}$
   - $\{\{b, e\}, \{b, c\}, \{b, d, a\}\}$

5. Scrivere un insieme A e una relazione $\mathcal{R}$ su A tale che ci siano 5 classi d'equivalenza in $A/\mathcal{R}$, 3 delle quali con 2 elementi ciascuna e le altre due con 3 elementi ciascuna.

6. Si consideri l'insieme $S = \{2, 4, 5, 7, 10, 14, 23, 24, 26, 27\}$ con la relazione di essere multiplo. Dire se esistono minimi e massimi, elementi massimali e minimali. Se $X = \{2, 4, 5, 7\}$ esistono l'estremo inferiore e superiore di X in S?

7. Si consideri l'insieme A^* delle parole sull'alfabeto $A = \{a, b, c\}$ e la relazione $\mathcal{R} = \{(u, v) \mid u \text{ è un prefisso di } v\}$ su A^*. Provare che la relazione $\mathcal{R}$ è una relazione d'ordine su A^*. Se $B = \{a, b, ab, aa, abc, aab, bac\}$ allora disegnare il diagramma di Hasse di B, dire se B ha minimo e massimo, quali sono gli elementi massimali e minimali di B, quali sono (se esistono) l'estremo inferiore e l'estremo superiore di B in A^*.

8. Si consideri la relazione di inclusione definita su $\{\{1\}, \{2\}, \{1, 2\}, \{1, 2, 3\}, \{1, 2, 3, 4\}, \{1, 2, 3, 5\}\}$. Si disegni il diagramma di Hasse e si dica se ci sono massimo e minimo, insiemi massimali e minimali.

9. Dire se le seguenti relazioni tra $A = \{a, b, c, d\}$ e $B = \{1, 2, 3, 4\}$ sono funzioni oppure no, e in caso siano funzioni determinare se sono iniettive e/o suriettive:

   1) $\{(a, 1), (b, 2), (c, 3), (d, 4)\}$
   2) $\{(a, 1), (b, 2), (c, 3)\}$
   3) $\{(a, 1), (b, 2), (c, 3), (c, 3), (d, 4)\}$
   4) $\{(a, 2), (b, 2), (c, 2), (c, 3), (d, 2)\}$
   5) $\{(a, 2), (b, 2), (c, 2), (d, 2)\}$
   6) $\{(a, 4), (b, 3), (c, 2), (d, 1)\}$
   7) $\{(a, 1), (b, 2), (c, 1), (d, 2)\}$
   8) $\{(a, 1), (b, 2), (a, 3), (b, 4)\}$
   9) $\{(a, 1), (a, 2), (a, 3), (a, 4)\}$
   10) $\{(c, 1), (b, 2), (d, 3), (a, 4)\}$

10. La relazione $\mathcal{R} = \{(x, y) \in \mathbb{N} \times \mathbb{Z} \mid x + y = 3\}$ è una funzione? E' iniettiva e/o suriettiva? E la relazione $\{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x = y^2\}$?

11. Nella funzione $f : x \in \mathbb{Z} \to x^2 \in \mathbb{Z}$ determinare l'immagine e la controimmagine dei seguenti insiemi:

    - $\{1, 2, 3, 4\}$
    - $\{2, 5, 7, 9, 10\}$
    - $\mathbb{N}$
    - $\mathbb{Z}$
    - $\{h \in \mathbb{Z} \mid h \leq 0\}$
    - $\{4, 9, 25\}$

    La funzione f è iniettiva e/o suriettiva?

12. Si considerino le funzioni $f : \{a, b, c\} \to \{1, 2, 3\}$, $g : \{1, 2, 3\} \to \{\bullet, \star, \diamond\}$ e $h : \{a, b, c\} \to \{\bullet, \star, \diamond\}$ definite da:

$f:\ a \mapsto 2$	$g:\ 1 \mapsto \star$	$h:\ a \mapsto \star$
$\quad b \mapsto 1$	$\quad 2 \mapsto \diamond$	$\quad b \mapsto \star$
$\quad c \mapsto 3$	$\quad 3 \mapsto \diamond$	$\quad c \mapsto \diamond$

    Dire se f e g sono iniettive e/o suriettive, calcolare $g \circ f$, f^{-1}, $h \circ f^{-1}$ e dire se sono iniettive e/o suriettive.

13. Sia $A = \{a, b, c\}$ e $B = \{1, 2, 3\}$. Quante funzioni ci sono tra $\mathcal{P}(A)$ e B? E tra A e $\mathcal{P}(A \times B)$? Scrivere tutte le funzioni tra A e B.

14. Sia $A = \{a, b, c\}$ e si consideri l'insieme A^* di tutte le parole su A, compresa la parola vuota ϵ. La funzione

$$f : u \in A^* \to \#u \in \mathbb{N}$$

è iniettiva e/o suriettiva? Sia $g : n \in \mathbb{N} \to n^2 \in \mathbb{N}$ e si dica se la funzione composta $g \circ f : A^* \to \mathbb{N}$ è iniettiva e/o suriettiva. Calcolare l'immagine tramite $g \circ f$ dell'insieme $\{aa, ab, abc, cba\}$.

15. Se $f : A \to B$ è una funzione, si consideri la relazione su A data da $\mathcal{R}_f = \{(a_1, a_2) \mid f(a_1) = f(a_2)\}$. Dimostrare che R_f è una relazione d'equivalenza su A.

3 I numeri interi

L'insieme dei numeri interi $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ è l'unione dei numeri naturali $\mathbb{N}$ e dei *numeri interi negativi* $\{\ldots, -3, -2, -1\}$. In $\mathbb{Z}$ sono definite le operazioni di somma $+$ e di prodotto $\cdot$ che godono della proprietà commutativa e della proprietà associativa: per ogni $n, m, l \in \mathbb{Z}$

$n + m = m + n$ e $m \cdot n = n \cdot m$ (proprietà commutativa);

$n + (m + l) = (n + m) + l$ e $n \cdot (m \cdot l) = (n \cdot m) \cdot l$ (proprietà associativa).

3.1 Divisibilità

Definizione 3.1.1. Siano $a, b \in \mathbb{Z}$. Si dice che b **divide** a se esiste $c \in \mathbb{Z}$ tale che

$$a = b \cdot c.$$

Per esempio, 2 divide 12, perchè $12 = 2 \cdot 6$, mentre 5 non divide 9 dato che non esiste un numero intero n tale che $9 = 5 \cdot n$. Ogni intero divide 0, poichè $0 = n \cdot 0$, per ogni $n \in \mathbb{Z}$; inoltre 1 divide ogni numero intero e ogni numero divide se stesso, in quanto $n = 1 \cdot n$, per ogni $n \in \mathbb{Z}$.

Se b divide a, si dice anche che b è un **divisore** di a oppure che a è **divisibile** per b e che a è un **multiplo** di b. In tal caso si scrive $b \,|\, a$.

Definizione 3.1.2. Un intero positivo p, diverso da 1, si dice **primo** se i suoi unici divisori positivi sono 1 e p.

Esempi di numeri primi sono 2,3,5,7,11,13,17 ....

Teorema 3.1.3. *I numeri primi sono infiniti.*

Teorema 3.1.4 (Teorema della Divisione)**.** *Siano $a, b \in \mathbb{Z}$ con $b \neq 0$, allora esistono e sono univocamente determinati $q \in \mathbb{Z}$ e $r \in \mathbb{N}$, tali che*

$$a = qb + r, \quad con \;\; 0 \leq r < |b|.$$

*Gli interi q ed r sono detti rispettivamente **quoziente** e **resto** della divisione. Il resto r si denota anche con $rest(a, b)$.*

Ad esempio se $a = 13$ e $b = 2$, allora $q = 6$ e $r = 1$ dato che $13 = 6 \cdot 2 + 1$. Chiaramente $rest(a, b) = 0$ se e solo se b divide a.

Definizione 3.1.5. Dati $a, b \in \mathbb{Z}$, il **massimo comune divisore** di a e b si denota con $MCD(a, b)$ ed è quel numero intero positivo d tale che

1. d è un divisore di a e b,
2. se t è un divisore di a e di b, allora t è anche un divisore di d.

Esempio 3.1.6. Il massimo comun divisore di 12 e 4 è 4, in quanto gli interi 1, 2 e 4 sono i divisori comuni di 12 e 4, quindi verificano la condizione 1 della definizione 3.1.5, inoltre 4 è multiplo di 1 e 2 e dunque è il solo che verifica anche la condizione 2.

Definizione 3.1.7. Siano $a, b \in \mathbb{Z}$, a e b si dicono **coprimi** se $MCD(a, b) = 1$.

Ad esempio 3 e 2 sono coprimi, anche 24 e 49 sono coprimi, mentre 24 e 14 non lo sono perché $MCD(24, 14) = 2$.

Proposizione 3.1.8. *Siano $a, b \in \mathbb{Z}$, si verifica che*

1. $MCD(a, b) = MCD(b, a)$,
2. *se a è un multiplo di b, allora* $MCD(a, b) = b$,
3. $MCD(a, b) = MCD(a, -b) = MCD(-a, b) = MCD(-a, -b)$.

Algoritmo di Euclide.

Tale algoritmo consente di calcolare il massimo comun divisore di due interi a e b eseguendo divisioni successive. Possiamo supporre, senza perdere di generalità che $a \geq b > 0$, dal momento che $MCD(a, b) = MCD(|a|, |b|)$.

Il primo passo dell'algoritmo consiste nell'eseguire la divisione tra a e b:

$$a = b \cdot q_1 + r_1, \quad \text{con} \quad r_1 < b.$$

A questo punto se $r_1 = 0$, allora $MCD(a, b) = b$. Nel caso contrario, invece, si esegue la divisione tra b e r_1:

$$b = r_1 \cdot q_2 + r_2, \quad \text{con} \quad r_2 < r_1.$$

Analogamente a quanto fatto nel passo precedente, se $r_2 = 0$, allora $MCD(a, b) = r_1$, altrimenti si esegue la divisione tra r_1 e r_2:

$$r_1 = r_2 \cdot q_3 + r_3, \quad \text{con} \quad r_2 < r_3.$$

Tale procedimento si itera fino ad arrivare al passo n, dove

$$r_{n-2} = r_{n-1} \cdot q_n + r_n \quad \text{e} \quad r_n = 0,$$

allora $MCD(a, b)$ coincide con r_{n-1}, ovvero con l'ultimo resto non nullo delle divisioni successive.

Esempio 3.1.9. Per determinare il massimo comun divisore di 32 e 15 con l'algoritmo di Euclide si eseguono le seguenti divisioni successive:

i) $32 = 2 \cdot 15 + 2$

ii) $15 = 7 \cdot 2 + 1$;

iii) $2 = 2 \cdot 1 + 0$

L'ultimo resto non nullo è 1, quindi $MCD(32, 15) = 1$.

Teorema 3.1.10 (Teorema di Bézout)**.** *Siano $a, b \in \mathbb{Z}$ e $d = MCD(a, b)$, allora esistono $n, m \in \mathbb{Z}$ tali che*

$$d = n \cdot a + m \cdot b.$$

In tal caso si dice che d è una ***combinazione lineare*** *di a e b con coefficienti n e m.*

Per calcolare $d = MCD(a, b)$ come combinazione lineare di a e b si possono usare le divisioni successive dell'algoritmo precedente. Infatti basta ricavare i resti dalle divisioni successive e andare a sostituirli man mano nelle eguaglianze precedenti. Può essere utile a questo proposito, sostituire le lettere a e b al posto dei rispettivi numeri in modo da gestire il calcolo letterale, senza farsi confondere dai calcoli aritmetici.

Esempio 3.1.11. Nel caso dell'esempio 3.1.9, 1 è combinazione lineare di 15 e 32:

$$1 = 5 \cdot 15 - 7 \cdot 32.$$

Infatti riscrivendo le divisioni i) e ii) con a al posto di 32 e b al posto di 15 si ottiene

i) $a = 2 \cdot b + 2$

ii) $b = 7 \cdot 2 + 1$;

iii) $2 = 2 \cdot 1 + 0$

Quindi da i) si ha $2 = a - 2 \cdot b$ e da ii) $1 = b - 7 \cdot 2$; sostituendo si ottiene $1 = b - 7 \cdot 2 = b - 7 \cdot (a - 2 \cdot b) = b - 7 \cdot a + 14 \cdot b = 15 \cdot b - 7 \cdot a$.

3.2 Classi di resto

Definizione 3.2.1. Dati $a, b \in \mathbb{Z}$ e $m \in \mathbb{N}$, si dice che a è **congruo** b **modulo** m se a e b divisi per m danno lo stesso resto.

Ci sono diverse notazioni per indicare che a è congruo b modulo m: $a(m\mathbb{Z})b$, $a \equiv_m b$, $a \equiv b(mod\ m)$ oppure $a \equiv b(m)$.

La relazione così introdotta in $\mathbb{Z}$ si dice **congruenza modulo m** e si denota con $m\mathbb{Z}$.

Proposizione 3.2.2. *Per ogni intero $m > 1$, $m\mathbb{Z}$ è una relazione di equivalenza in $\mathbb{Z}$.*

Indichiamo con $[a]_m$ la classe di equivalenza di a rispetto $m\mathbb{Z}$, dunque

$$[a]_m = \{b \in \mathbb{Z} \mid a(m\mathbb{Z})b\} = \{b \in \mathbb{Z} \mid rest(a, m) = rest(b, m)\}.$$

Dato che il resto della divisione per m può essere uguale a $0, \ldots, m-1$, vale il seguente risultato:

Proposizione 3.2.3. *Dato l'intero $m > 1$, allora esistono esattamente m classi di equivalenza rispetto alla relazione $m\mathbb{Z}$ (si chiamano **classi di resto**) e sono $[0]_m, [1]_m, \ldots, [m-1]_m$. In particolare*

$$[h]_m = \{km + h \mid k \in \mathbb{Z}\}.$$

I rappresentanti delle classi di equivalenza sono quindi tutti i possibili resti delle divisioni per m.

Esempio 3.2.4. Dato che $rest(4, 3) = rest(1, 3) = 1$, $4 \equiv 1(3)$, inoltre le classi di equivalenza modulo 3 sono $[0]_3 = \{0, 3, 6, 9, \ldots\}$, $[1]_3 = \{1, 4, 7, 10, \ldots\}$ e $[2]_3 = \{2, 5, 8, 11, \ldots\}$.

L'insieme quoziente $\mathbb{Z} \setminus m\mathbb{Z}$ si denota con $\mathbb{Z}_m$ ed è chiamato **insieme degli interi modulo m**. Per esempio, $\mathbb{Z}_4 = \{[0]_4, [1]_4, [2]_4, [3]_4\}$.

Proposizione 3.2.5. *Dati $a, b, m \in \mathbb{Z}$ con $m > 1$, $a \equiv b(m)$ se e solo se $a - b$ è un multiplo di m.*

Una conseguenza della Proposizione 3.2.5 è che le classi di equivalenza si possono ridefinire in questo modo: dati $a, m \in \mathbb{Z}$, con $m > 1$

$$[a]_m = \{b \in \mathbb{Z} \mid a - b = hm, \text{ con } h \in \mathbb{Z}\}.$$

Dati $a, b, m \in \mathbb{Z}$, con $m > 1$, in $\mathbb{Z}_m$ sono definite le operazioni di somma e prodotto:

- $[a]_m + [b]_m = [a+b]_m$, e
- $[a]_m \cdot [b]_m = [a \cdot b]_m$.

Proposizione 3.2.6. *Dati $a, b, m \in \mathbb{Z}$, con $m > 1$, se $a \equiv b(m)$, allora, per ogni $t \in \mathbb{Z}$, $a + t \equiv b + t(m)$ e $a \cdot t \equiv b \cdot t(m)$.*

Esempio 3.2.7. Riportiamo le tavole della somma e del prodotto in $\mathbb{Z}_2 = \{[0]_2, [1]_2\}$, $\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$ e $\mathbb{Z}_4 = \{[0]_4, [1]_4, [2]_4, [3]_4\}$.

$+$	$[0]_2$	$[1]_2$
$[0]_2$	$[0]_2$	$[1]_2$
$[1]_2$	$[1]_2$	$[0]_2$

$\cdot$	$[0]_2$	$[1]_2$
$[0]_2$	$[0]_2$	$[0]_2$
$[1]_2$	$[0]_2$	$[1]_2$

$+$	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_3$	$[0]_3$	$[1]_3$	$[2]_3$
$[1]_3$	$[1]_3$	$[2]_3$	$[0]_3$
$[2]_3$	$[2]_3$	$[0]_3$	$[1]_3$

$\cdot$	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_3$	$[0]_3$	$[0]_3$	$[0]_3$
$[1]_3$	$[0]_3$	$[1]_3$	$[2]_3$
$[2]_3$	$[0]_3$	$[2]_3$	$[1]_3$

$+$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[1]_4$	$[1]_4$	$[2]_4$	$[3]_4$	$[0]_4$
$[2]_4$	$[2]_4$	$[3]_4$	$[0]_4$	$[1]_4$
$[3]_4$	$[3]_4$	$[0]_4$	$[1]_4$	$[2]_4$

$\cdot$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[0]_4$	$[0]_4$	$[0]_4$
$[1]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[2]_4$	$[0]_4$	$[2]_4$	$[0]_4$	$[2]_4$
$[3]_4$	$[0]_4$	$[3]_4$	$[2]_4$	$[1]_4$

Definizione 3.2.8. Dato un intero $m > 1$, la classe $[a]_m$ è **invertibile** se esiste $[b]_m$ tale che $[a]_m \cdot [b]_m = [1]_m$. Si dice che $[b]_m$ è l' **inverso** di $[a]_m$.

Osserviamo che $[1]_m$ è sempre invertibile dato che $[1]_m \cdot [1]_m = [1]_m$ e invece $[0]_m$ non è mai invertibile.

Esempio 3.2.9. Dalle tavole del prodotto possiamo individuare gli elementi invertibili e i rispettivi inversi, ad esempio $[2]_4$ non è invertibile, invece $[3]_4$ è invertibile e il suo inverso è $[3]_4$.

Proposizione 3.2.10. *Dato l'intero $m > 1$, $[a]_m$ è invertibile se e solo se $MCD(a, m) = 1$, ovvero a ed m sono coprimi.*

Esempio 3.2.11. La classe $[2]_4$ non è invertibile, in quanto $MCD(2, 4) = 2$, invece $MCD(3, 4) = 1$, per cui $[3]_4$ è invertibile.

Definiamo ora la funzione di Eulero φ che consente di determinare il numero di elementi invertibili in $\mathbb{Z}_m$.

Definizione 3.2.12. Dato un intero $m > 1$,

$$\varphi(m) = |\{n \in \mathbb{N} \mid MCD(n, m) = 1, \text{ con } 1 \leq n < m\}|.$$

Per ogni $m > 1$ in $\mathbb{Z}_m$ ci sono esattamente $\varphi(m)$ elementi invertibili.

Esempio 3.2.13. Calcoliamo il numero di elementi invertibili in $\mathbb{Z}_m$ per $m = 1, 2, 3,$ e 4: $\varphi(2) = 1$, $\varphi(3) = |\{1, 2\}| = 2$, $\varphi(4) = |\{1, 3\}| = 2$ e $\varphi(5) = |\{1, 2, 3, 4\}| = 4$.

Proposizione 3.2.14. *Sia p un numero primo, allora*

1. $\varphi(p^n) = p^n - p^{n-1}$, *per ogni* $n \geq 1$, *e*
2. *se* $MCD(a, b) = 1$, *allora* $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

Esempio 3.2.15. La scomposizione in fattori primi di 120 è $2^3 \cdot 3 \cdot 5$, dunque $\varphi(120) = \varphi(2^3) \cdot \varphi(3) \cdot \varphi(5) = (2^3 - 2^2) \cdot 2 \cdot 4 = 4 \cdot 2 \cdot 4 = 32$. Concludiamo che in $\mathbb{Z}_{120}$ ci sono 32 elementi invertibili.

Esempio 3.2.16. In $\mathbb{Z}_{300}$ ci sono 80 elementi invertibili: $\varphi(300) = \varphi(2^2 \cdot 3 \cdot 5^2) = \varphi(2^2) \cdot \varphi(3) \cdot \varphi(5^2) = (2^2 - 2^1) \cdot (3 - 1) \cdot (5^2 - 5^1) = 2 \cdot 2 \cdot 20 = 80$.

Equazioni congruenziali lineari

Definizione 3.2.17. Un' **equazione congruenziale lineare** (**congruenza lineare**) è un'espressione del tipo

$$a \cdot x \equiv b (mod\ m)$$

dove $a, b, m \in \mathbb{Z}$ e x è l'incognita dell'equazione.

Ad esempio, $2x \equiv 1 (mod\ 3)$ è un'equazione congruenziale.

Teorema 3.2.18. *Siano $a, b, m \in \mathbb{Z}$, con $MCD(a, m) = 1$. L'insieme delle soluzioni della congruenza lineare $ax \equiv b (mod\ m)$ è*

$$\{sb + mh \mid h \in \mathbb{Z}\},$$

dove $s, t \in \mathbb{Z}$ e $1 = as + mt$ (teorema di Bézout).

Esempio 3.2.19. Data la congruenza lineare $2x \equiv 1 (mod\ 3)$, dove $MCD(2, 3) = 1$, attraverso le divisioni successive $3 = 1 \cdot 2 + 1$, $2 = 2 \cdot 1 + 0$, scriviamo 1 come combinazione lineare di 2 e 3: $1 = 2(-1) + 3(1)$, allora tutte le soluzioni della congruenza sono del tipo $-1 + 3h$, con $h \in \mathbb{Z}$.

Il seguente teorema generalizza il teorema 3.2.18 al caso in cui il massimo comun divisore tra a e m è diverso da 1.

Teorema 3.2.20. *Siano $a, b, m \in \mathbb{Z}$, con $MCD(a, 1)$. L'equazione congruenziale $ax \equiv b(mod\ m)$ ammette soluzione se e solo se $d \setminus b$. In tal caso l'insieme delle soluzioni è*

$$\left\{\frac{s}{d}b + \frac{m}{d}h \mid h \in \mathbb{Z}\right\},$$

dove $s, t \in \mathbb{Z}$ e $d = as + mt$ (teorema di Bézout). La soluzione $x_0 = \frac{s}{d}b$ è detta ***soluzione particolare*** *della congruenza lineare.*

Esempio 3.2.21. Per dimostrare che $56x \equiv 12(mod\ 30)$ ammette soluzione, calcoliamo $MCD(56, 30)$. Le divisioni successive $56 = 1 \cdot 30 + 26$, $30 = 1 \cdot 26 + 4$ e $4 = 2 \cdot 2 + 0$, per cui $MCD(56, 30) = 2$. La congruenza ammette soluzione dato che $2/12$. Scriviamo 2 come combinazione lineare di 56 e 30: $2 = (56 - 30) - 6(2 \cdot 30 - 56) = 7 \cdot 56 - 13 \cdot 30$. Dunque, $\left\{\frac{7}{2}12 + \frac{30}{2}h, n \in \mathbb{Z}\right\} = \{42 + 15h, h \in \mathbb{Z}\}$ è l'insieme delle soluzioni di $56x \equiv 12(mod\ 30)$.

3.3 Il principio di Induzione

Il principio di induzione è un potente strumento di dimostrazione, al quale si ricorre ogni qual volta si debba dimostrare che una proprietà vale per ogni numero intero naturale oppure a partire da un certo $n_0 \in \mathbb{N}$.

Il principio di induzione si basa su una proprietà fondamentale dei numeri naturali, e cioè che possono essere costruiti a partire dallo 0 e dalla funzione di successore. Proviamo a vedere un esempio e poi enunceremo il principio in generale.

Supponiamo di voler calcolare le seguenti somme:

$$\begin{aligned} 1 + 2 \\ 1 + 2 + 3 \\ 1 + 2 + 3 + 4 \\ 1 + 2 + 3 + 4 + 5 \\ 1 + 2 + 3 + 4 + 5 + 6 \end{aligned}$$

Invece di rifare ogni volta la somma, possiamo pensare che $1 + 2 + 3$ è uguale a $1 + 2$ più 3, per calcolare $1 + 2 + 3 + 4$ possiamo sommare 4 al risultato ottenuto

precedentemente, e così via. Quindi

$$\begin{aligned} 1+2 &= 3 \\ 1+2+3 &= 3+3=6 \\ 1+2+3+4 &= 6+4=10 \\ 1+2+3+4+5 &= 10+5=15 \\ 1+2+3+4+5+6 &= 15+6=21. \end{aligned}$$

Generalizziamo questo discorso. Se invece di fermarci alle somme fino a 6 vogliamo calcolare le somme fino ad un numero n che non specifichiamo (ma che potrà in seguito essere sostituito con un numero qualsiasi) allora possiamo scrivere in questo modo: chiamiamo s_n la somma dei numeri fino a n, cioè:

$$s_n = 1+2+3+4+...+n$$

dove mettiamo i puntini per dire che non sappiamo quanti addendi ci saranno perché dipendono da n. Quindi $s_1 = 1$, $s_2 = 1+2$, $s_3 = 1+2+3$ e così via. Dalle osservazioni precedenti (e dalla definizione di somma) abbiamo che

$$s_{n+1} = s_n + (n+1).$$

Questo tipo di uguaglianza si dice *ricorsiva* perché per esprimere il valore di s_{n+1} dobbiamo usare un'altra s. Se voglio conoscere per esempio a quanto è uguale s_{23} dovrò calcolare s_{22}, e per calcolare quest'ultima dovrò calcolare s_{21} e così via, fino ad arrivare a s_1 che è uguale a 1.

Esiste una forma più concisa, non ricorsiva, per calcolare s_n? Trovarla non è semplicissimo, anche se ci sono dei metodi (vedi...), ma possiamo fare un'altra cosa: io vi dico che $s_n = n(n+1)/2$ e vi chiedo di controllare che questa affermazione è corretta. Chiedo cioè di controllare che per ogni numero naturale $n \geq 1$ vale la seguente uguaglianza:

$$s_n = \frac{n(n+1)}{2}. \tag{3.1}$$

Ancora una volta, per valori piccoli di n possiamo controllare direttamente: se $n = 1$ allora la parte destra dell'equazione è uguale a 1 e quella sinistra è uguale a $1 \cdot 2/2 = 1$, quindi l'uguaglianza vale. Per $n = 2$ a sinistra ho $1+2 = 3$ e a destra ho $2 \cdot 3/2 = 3$. Per $n = 3$ a sinistra ho $1+2+3 = 6$ e a destra ho $3 \cdot 4/2 = 6$. Ma come faccio a provarlo per OGNI numero naturale n? Posso ragionare in questo modo: supponiamo di aver dimostrato che l'uguaglianza valga fino ad un certo numero m, cioè che $s_m = m(m+1)/2$. Che cosa succede per $m+1$? Posso ragionare così:

$$\begin{aligned} s_{m+1} &= s_m + (m+1) = \tfrac{m(m+1)}{2} + (m+1) = \\ &= \tfrac{m(m+1)+2(m+1)}{2} = \tfrac{(m+1)(m+2)}{2}. \end{aligned} \tag{3.2}$$

Ho visto quindi che se suppongo vero il risultato per $n = m$ allora riesco a provarlo per $n = m + 1$ cioè per il successore di m: infatti l'espressione (3.2) equivale proprio a (3.1) quando si pone $n = m + 1$. Quindi, riassumendo, la proprietà che $s_n = n(n + 1)/2$ è vera per $n = 1$. Quindi per quanto detto prima è vera anche per $n = 2$ che è il successore di 1, quindi è vera per $n = 3$ che è il successore di 2, e così via, la proprietà sarà vera per qualsiasi numero naturale.

Quanto detto finora con questo esempio è in realtà una proprietà molto importante dei numeri naturali che si chiama *principio di induzione*:

Definizione 3.3.1. Sia $P(n)$ una proprietà che dipende dalla variabile naturale n. Dato $n_0 \in \mathbb{N}$, se si verificano le seguenti condizioni:

1. $P(n_0)$ è vera, e

2. per un generico $m \geq n_0$, supponendo che $P(m)$ sia vera (tale condizione è chiamata **ipotesi d'induzione**), allora si dimostra che $P(m + 1)$ è vera,

allora $P(n)$ è vera per ogni $n \geq n_0$.

Il punto 1 è generalmente chiamato **base d'induzione**, il punto 2 **passo d'induzione**. Nel punto 2, quando si parla di un generico m si intende che m è un numero qualsiasi, quindi il passo di induzione consiste nel fare una dimostrazione della proprietà per $m + 1$, sfruttando la conoscenza che il risultato valga per un qualunque m.

Notazione. Il principio di induzione viene spesso (ma non solo) utilizzato per dimostrare quanto valgono delle somme. Utilizzeremo allora una notazione più compatta. La somma di più elementi che dipendono da un parametro può essere scritta con il simbolo di sommatoria. Per esempio

$$\sum_{i=1}^{n} i = 1 + 2 + \ldots + n$$

che si legge *la somma di i per i che varia da* 1 *a n*. Nel simbolo di sommatoria si scrive in basso il valore da cui si parte, in alto il valore a cui si arriva, e dopo il simbolo di sommatoria si scrive l'espressione che si deve sommare. Tale espressione deve contenere la variabile (che chiamiamo *vincolata* o anche *muta*) presente in basso nel simbolo, cioè la variabile che varia nella somma. La n presente nell'espressione è sempre una variabile, ma viene chiamata variabile *libera* (non è vincolata a prendere dei valori quando si fa la somma). Per esempio se scrivo

$$\sum_{i=2}^{n} i^2$$

vuol dire che devo sommare i numeri i^2 per tutti i valori di i che variano da 2 a n, cioè

$$\sum_{i=2}^{n} i^2 = 2^2 + 3^2 + 4^2 + \ldots + n^2.$$

Se istanzio il valore della variabile libera, ponendo per esempio $n = 4$ allora ho

$$\sum_{i=2}^{4} i^2 = 2^2 + 3^2 + 4^2 = 4 + 9 + 16 = 29.$$

I nomi delle variabili vincolate non sono importanti, basta che ci sia coerenza. Per esempio

$$\sum_{i=1}^{n} i^3 = \sum_{k=1}^{n} k^3 (\text{ ma non posso scrivere } \sum_{i=1}^{n} k^3).$$

Invece i nomi delle variabili libere possono far cambiare il valore dell'espressione: se $n \neq m$ allora

$$\sum_{i=1}^{n} i^3 \neq \sum_{i=1}^{m} i^3. \tag{3.3}$$

(Provare per esempio con $n = 3$ e $m = 4$ a calcolare le due sommatorie in (3.3).) Come espressione più generale possibile di una sommatoria, posso considerare una espressione numerica a_i che dipende da i e scrivere

$$\sum_{i=1}^{n} a_i = a_1 + a_2 + \ldots + a_n.$$

Negli esempi precedenti abbiamo considerato prima $a_i = i$, poi $a_i = i^2$ e poi ancora $a_i = i^3$. Se per esempio $a_i = (i + 3)/2$ allora

$$\sum_{i=1}^{n} a_i = (1 + 3)/2 + (2 + 3)/2 + (3 + 3)/2 + \ldots + (n + 3)/2.$$

Nota che (e questo sarà molto importante nelle dimostrazioni per induzione):

$$\sum_{i=1}^{n} a_i = \left(\sum_{i=1}^{n-1} a_i \right) + a_n.$$

Esempio 3.3.2. Dimostriamo che

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

per ogni $n \geq 1$.

In questo caso la proprietà $P(n)$ è l'uguaglianza $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ che dipende da n, mentre la variabile i è la variabile vincolata il cui valore si esaurisce all'interno della somma.
- Base d'induzione: per $n = 1$, si ha $1 = \frac{1 \cdot 2}{2}$, dunque $P(1)$ è vera.
- Passo d'induzione: dato $t \in \mathbb{N}$, se assumiamo che $P(t)$ sia vera, ossia

$$\sum_{i=1}^{t} i = \frac{t(t+1)}{2},$$

allora

$$\sum_{i=1}^{t+1} i = \sum_{i=1}^{t} i + (t+1) = \frac{t(t+1)}{2} + (t+1) = \frac{t(t+1) + 2(t+1)}{2} = \frac{(t+1)(t+2)}{2},$$

dunque $P(t+1)$ è vera.

Esempio 3.3.3. Dimostriamo che

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

per ogni $n \geq 1$.
- Base d'induzione: per $n = 1$ si ha $1^2 = \frac{1 \cdot 2 \cdot 3}{6}$, dunque $P(1)$ è vera.
- Passo d'induzione: dato $t \in \mathbb{N}$, se assumiamo che $P(t)$ sia vera, ossia

$$\sum_{i=1}^{t} i^2 = \frac{t(t+1)(2t+1)}{6},$$

allora

$$\sum_{i=1}^{t+1} i^2 = \sum_{i=1}^{t} i^2 + (t+1)^2 = \frac{t(t+1)(2t+1) + 6(t+1)^2}{6} =$$

$$\frac{(t+1)[t(2t+1) + 6(t+1)]}{6} = \frac{(t+1)(2t^2 + 7t + 6)}{6} = \frac{(t+1)(t+2)(2t+3)}{6},$$

dunque $P(t+1)$ è vera.

Un altro simbolo molto utile, simile a quello di sommatoria, è il simbolo di **produttoria**: con

$$\prod_{k=1}^{n} a_k$$

si intende il prodotto $a_1 \cdot \ldots \cdot a_n$.

Esempio 3.3.4. Mostrare che per $n \geq 2$ si ha:

$$\prod_{k=2}^{n}\left(1-\frac{1}{k}\right)=\frac{1}{n}.$$

- Base di induzione: per $n = 2$ si ha $(1 - 1/2) = 1/2$ e quindi la proprietà vale.
- Passo di induzione: assumiamo che la proprietà valga per t e dimostriamola per $t + 1$. L'ipotesi di induzione quindi è

$$\prod_{k=2}^{t}\left(1-\frac{1}{k}\right)=\frac{1}{t}$$

e voglio dimostrare

$$\prod_{k=2}^{t+1}\left(1-\frac{1}{k}\right)=\frac{1}{t+1}.$$

Valgono i seguenti passaggi:

$$\prod_{k=2}^{t+1}\left(1-\frac{1}{k}\right)=\prod_{k=2}^{t}\left(1-\frac{1}{k}\right)\cdot\left(1-\frac{1}{t+1}\right)=$$

(per ipotesi di induzione)

$$\frac{1}{t}\cdot\left(1-\frac{1}{t+1}\right)=\frac{1}{t+1}.$$

Le dimostrazioni per induzione non si usano solo per le sommatorie o le produttorie:

Esempio 3.3.5. Dimostriamo che $n(n + 1)$ è un numero pari, per ogni $n \in \mathbb{N}$.
- Base d'induzione: $P(1)$ è vera, in quanto $1(1 + 1) = 2$.
- Passo d'induzione: dato $t \in \mathbb{N}$, assumiamo che $P(t)$ sia vera, ossia che $t(t+1)$ è pari. Di conseguenza anche $(t+1)(t+2)$ è pari, perché è uguale a $t(t+1)+2(t+1)$ che è la somma di due numeri pari, dunque $P(t + 1)$ è vera.

Esempio 3.3.6. Usando il principio di induzione, dimostriamo che per ogni $n \geq 1$ il numero $7^n - 1$ è un multiplo di 6.
- Base di induzione: per $n = 1$ si ha $7^1 - 1 = 6$ che è un multiplo di 6.
- Passo di induzione: supponiamo che il risultato sia vero per n e dimostriamolo per $n + 1$. Supponiamo quindi che $7^n - 1$ sia un multiplo di 6, cioè esiste $a \in \mathbb{Z}$ tale che $7^n - 1 = 6a$ e quindi $7^n = 6a + 1$. Allora $7^{n+1} - 1 = 7 \cdot 7^n - 1 = 7(6a + 1) - 1 = 42a + 6 = 6(7a - 1)$ e quindi è un multiplo di 6.

Attraverso il principio di induzione dimostriamo il seguente teorema:

Teorema 3.3.7. *Sia X un insieme tale che $|X| = n$, allora $|\mathcal{P}(X)| = 2^n$.*

Dimostrazione: $P(0)$ è vera, dato che se X è l'insieme vuoto, allora $\mathcal{P}(X) = \{\emptyset\}$, e quindi $|\mathcal{P}(X)| = 1 = 2^0$ (base d'induzione). Dato $t \in \mathbb{N}$, supponiamo che $P(t)$ è vera, ovvero che ogni insieme di cardinalità t ha 2^t sottoinsiemi (ipotesi d'induzione). Consideriamo ora un insieme $X = \{x_1, \ldots, x_t, x_{t+1}\}$ con $t+1$ elementi e sia $Y = \{x_1, \ldots, x_t\}$. Osserviamo che un sottoinsieme di X può contenere o meno l'elemento x_{t+1} quindi o è un sottoinsieme di Y oppure si ottiene aggiungendo x_{t+1} ad un sottoinsieme di Y. Quindi:

$$\mathcal{P}(X) = \mathcal{P}(Y) \cup \{S \cup \{x_{t+1}\} | S \in \mathcal{P}(Y)\},$$

dunque, dato che per ipotesi di induzione $|\mathcal{P}(Y)| = 2^t$, si ha $|\mathcal{P}(X)| = |\mathcal{P}(Y)| + |\{S \cup \{x_{t+1}\} | S \in \mathcal{P}(Y)\}| = 2^t + 2^t = 2^{t+1}$ (passo d'induzione).

Seconda forma del principio di induzione

Il principio di induzione si può anche enunciare in una seconda forma che utilizzeremo per alcune dimostrazioni più avanti. La differenza sta nel fatto che il passo di induzione non va da m a $m+1$, ma va da tutti i valori più piccoli di m ad m.

Definizione 3.3.8. Sia $P(n)$ una proprietà che dipende dalla variabile naturale n. Dato $n_0 \in \mathbb{N}$, se si verificano le seguenti condizioni:

1. $P(n_0)$ è vera, e
2. supponendo che $P(m)$ sia vera per ogni $t < m$, allora si dimostra che $P(m)$ è vera,

allora $P(n)$ è vera per ogni $n \geq n_0$.

Utilizzando la seconda forma del principio di induzione dimostriamo il seguente teorema:

Teorema 3.3.9. *Ogni intero positivo maggiore di 1 è prodotto di numeri primi (in modo unico).*

Dimostrazione: Sia n un intero positivo maggiore di 1. Come base di induzione consideriamo $n = 2$ che è un numero primo e quindi è banalmente un prodotto (di un solo fattore) di numeri primi.

Sia ora $n > 2$ e come ipotesi di induzione supponiamo il risultato vero per ogni numero minore di n (seconda forma del principio di induzione). Se n è un numero primo, il risultato banalmente è valido. Se invece n non è primo, allora n ha un divisore diverso da 1 e da n, quindi si può scrivere

$$n = a \cdot b$$

con a e b entrambi maggiori di 1 e minori di n. Quindi posso applicare l'ipotesi di induzione ad a e b che saranno prodotto di numei primi: $a = p_1 \cdot \ldots \cdot p_n$ e $b = q_1 \cdot \ldots \cdot q_m$ e quindi:

$$n = p_1 \cdot \ldots \cdot p_n \cdot q_1 \cdot \ldots \cdot q_m$$

e abbiamo mostrato che n è prodotto di numeri primi. QED. (manca la dimostrazione dell'unicita')

Teorema 3.3.10. *I numeri primi sono infiniti.*

Dimostrazione: Supponiamo per assurdo che l'insieme dei numeri primi sia finito, per esempio sia

$$P = \{p_1, \ldots, p_n\}$$

e consideriamo il numero

$$m = (p_1 \cdot \ldots \cdot p_n) + 1.$$

Il numero m sicuramente non appartiene all'insieme P, quindi non è un numero primo. Allora per il teorema fondamentale dell'aritmetica esistono dei numeri primi $q_1, \ldots, q_t \in P$ tali che

$$m = q_1 \cdot \ldots \cdot q_t.$$

Dato che i numeri $q_1, \ldots, q_t$ appartengono a P allora coincidono con qualche p_i, supponiamo per esempio che $q_1 = p_1$. Dall'equazione precedente abbiamo:

$$\begin{aligned}
(p_1 \cdot \ldots \cdot p_n) + 1 &= q_1 \cdot \ldots \cdot q_t \\
(p_1 \cdot \ldots \cdot p_n) + 1 &= p_1 q_2 \cdot \ldots \cdot q_t \\
1 &= p_1 \cdot \ldots \cdot q_t - p_1 \cdot \ldots \cdot p_n \\
1 &= p_1(p_2 \cdot \ldots \cdot q_t - p_2 \cdot \ldots \cdot p_n)
\end{aligned}$$

ma questo porta ad un assurdo, dato che il numero p_1 non può dividere 1. QED

3.4 Elementi di combinatoria

Quando abbiamo parlato di contare gli elementi di un insieme abbiamo formulato le seguenti regole, che valgono qualsiasi siano gli insiemi finiti X e Y:

$|X \cup Y| = |X| + |Y| - |X \cap Y|$ (principio di inclusione/esclusione)
$|X \times Y| = |X| \cdot |Y|$ (principio di moltiplicazione)
$|\mathcal{P}(X)| = 2^{|X|}$.

Usando queste proprietà, possiamo risolvere alcuni problemi di combinatoria.

Esempio 3.4.1. Quanti sono i numeri compresi tra 1 e 100 che sono divisibili o per 2 o per 5? Chiamiamo A l'insieme dei numeri divisibili per 2 e B l'insieme dei numeri divisibili per 5. Quindi

$$A \cap B = \{n \mid 1 \leq n \leq 100 \text{ e } n \text{ è divisibile per 2 e per 5}\}.$$

Considerando che $|A| = 50$, $|B| = 20$ e $|A \cap B| = 10$, si ha

$$|A \cup B| = 50 - 20 + 10 = 60$$

quindi ci sono 60 numeri compresi tra 1 e 100 che sono divisibili per 2 o per 5.

Esempio 3.4.2. In un bar ogni bibita costa 5 euro. Ci sono 21 clienti, ognuno dei quali ordina una o due bibite diverse. In tutto vengono ordinate 12 aranciate e 15 chinotti. Quanti scontrini da 10 euro verranno emessi? Sia A l'insieme dei clienti che prende l'aranciata e B l'insieme dei clienti che prende il chinotto. Quindi si ha $|A| = 12$ e $|B| = 15$, mentre $|A \cup B| = 21$ perchè $A \cup B$ è l'insieme delle persone che hanno preso o un aranciata o un chinotto (o entrambi). Quindi quante sono le persone che hanno preso esattamente due bibite? Saranno

$$|A \cap B| = |A| + |B| - |A \cup B| = 12 + 15 - 21 = 6.$$

Il principio di moltiplicazione ci serve invece per contare le sequenze di elementi, in cui si distinguono due sequenze di oggetti che hanno un ordine diverso tra di loro. Un tipico esempio è quello delle parole che si possono scrivere su un alfabeto: Se per esempio $A = \{a, b, c\}$ potrò scrivere $3 \cdot 3 = 9$ parole di lunghezza due, perchè sono tante quante gli elementi del prodotto cartesiano $A \times A$. Le parole di lunghezza 4 saranno invece 3^4.

Esempio 3.4.3. Quanti numeri di tre cifre si possono scrivere con le cifre da 0 a 9? Dato che ci sono 10 cifre disponibili, i numeri formati da tre di queste cifre sono $10 \cdot 10 \cdot 10 = 1000$ (non dovrebbe essere sorprendente...)

Esempio 3.4.4. Se un ristorante offre un menu completo formato da un primo, un secondo e un dolce e permette di scegliere tra 3 primi, 4 secondi e 3 dolci, quanti menu diversi tra di loro si possono chiedere? Sono $3 \cdot 4 \cdot 3$.

Anche per contare le funzioni tra due insiemi finiti S e T usiamo il principio di moltiplicazione: ogni funzione corrisponde ad una sequenza di $|S|$ elementi di $|T|$, quindi in totale ci saranno $|T|^{|S|}$ possibili funzioni.

Per esprimere concetti più complessi possiamo introdurre delle definizioni che ci aiutano nei calcoli, ma sono comunque costruite a partire dal principio di moltiplicazione.

Definizione 3.4.5. Per ogni numero $n \in \mathbb{N}$, il **fattoriale di** n, denotato con $n!$ è un numero definito come segue: $0! = 1$ e $n! = n(n-1)!$, cioè

$$n! = n(n-1) \cdot (n-2) \cdot \ldots \cdot 2 \cdot 1\,.$$

Proviamo a rispondere a questa domanda: quante parole di 2 lettere distinte tra di loro posso scrivere usando un alfabeto di 4 lettere? La prima lettera la posso scegliere tra 4 diverse possibilità, ma la seconda la dovrò scegliere tra 3 possibili lettere, perché una sarà stata già usata in precedenza. In tutto avrò $4 \cdot 3$ possibili parole.

Definizione 3.4.6. Una **disposizione semplice** di k elementi scelti tra n, è una sequenza formata da k simboli diversi tra di loro, presi tra tutti i possibili n. Il numero di disposizioni semplici si denota con $d_{n,k}$ ed è dato dalla seguente formula:

$$d_{n,k} = \frac{n!}{(n-k)!}$$

(nota che deve essere $k \leq n$).

Una **permutazione** di n elementi è una disposizione semplice di n elementi scelti tra n (cioè come nel caso precedente ma con $k = n$). In questo caso si ha

$$d_{n,n} = n!$$

cioè ci sono $n!$ possibili permutazioni di n elementi.

Proposizione 3.4.7. *Dati gli insiemi A e B tali che $|A| = k$, $|B| = n$ e $k \leq n$, il numero di funzioni iniettive di A in B è*

$$d_{n,k} = \frac{n!}{(n-k)!}.$$

Esempio 3.4.8. Siano $X = \{1, 2, 3\}$ e $Y = \{a, b, c, d, e\}$, allora il numero di funzioni iniettive di X in Y è

$$\frac{5!}{(5-3)!} = \frac{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{2 \cdot 1} = 60.$$

Si noti che per avere funzioni iniettive tra A e B deve essere $|A| \leq |B|$.

Se $|A| = |B|$ allora tutte le funzioni iniettive sono anche suriettive e quindi biettive, e di funzioni biettive che ne sono $d_{|A|,|A|}$. Nel caso particolare in cui $A = B$ le funzioni biettive vengono anche dette permutazioni, coerentemente con quanto detto in precedenza.

Esempio 3.4.9. Sia $X = \{a, b, c\}$, allora il numero di permutazioni di X è $3! = 3 \cdot 2 \cdot 1 = 6$:

1. $f_1(a) = a, f_1(b) = b, f_1(c) = c$;
2. $f_2(a) = a, f_2(b) = c, f_2(c) = b$;
3. $f_3(a) = b, f_3(b) = a, f_3(c) = c$;
4. $f_4(a) = c, f_4(b) = b, f_4(c) = a$;
5. $f_5(a) = c, f_5(b) = a, f_5(c) = b$;
6. $f_6(a) = b, f_6(b) = c, f_6(c) = a$.

Definizione 3.4.10. Una **disposizione con ripetizione** di k elementi scelti tra n è una sequenza formata da k simboli (anche con ripetizioni) scelti tra gli n. Il numero di disposizioni con ripetizione si indica con $d'_{n,k}$ ed è dato dalla seguente formula:

$$d'_{n,k} = n^k \,.$$

Esempio 3.4.11. In una cesta ci sono 5 biglie colorate di colore rosso, bianco, giallo, verde e blu. Ci sono tre bambine: Anna, Bianca e Carla. In quanti modi si possono distribuire le biglie in modo che ogni bambina ne abbia una? Dobbiamo contare le disposizioni semplici (perché una volta che ho dato una biglia ad una bambina non posso darla ad un altra) di 3 oggetti presi tra 5 possibili, quindi il numero è $d_{5,3} = (5!)/(2!) = 5 \cdot 4 \cdot 3 = 60$.

Nelle disposizioni siamo interessati a distinguere sequenze che hanno ordine diverso degli elementi, così come la parola *aba* è diversa dalla parola *baa*. Proviamo a contare adesso gli insiemi invece delle sequenze.

Definizione 3.4.12. Il **coefficiente binomiale** di n su k (con $0 \leq k \leq n$) si indica con $\binom{n}{k}$ ed è dato dalla seguente formula

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Si ha che $\binom{n}{k} = d_{n,k}/h!$. In particolare, per $k = 0$ si ha $\binom{n}{0} = 1$ e per $k = n$ si ha $\binom{n}{n} = 1$.

Il nome "coefficiente binomiale" deriva dal fatto che i numeri introdotti nella precedente definizione sono i coefficienti delle potenze dei binomi. Infatti vale il seguente risultato:

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i \,.$$

I coefficienti binomiali possono essere rappresentati e calcolati (per piccoli numeri) utilizzando il cosiddetto *triangolo di Tartaglia* in cui alla riga i sono elencati

i valori di $\binom{i}{j}$ per $j = 0, \ldots, i$. Da questa rappresentazione grafica si nota che ogni coefficiente binomiale è la somma dei due coefficienti che sono sopra di lui. Questo corrisponde alla proprietà che $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$:

$n = 0$							1							
$n = 1$						1		1						
$n = 2$					1		2		1					
$n = 3$				1		3		3		1				
$n = 4$			1		4		6		4		1			
$n = 5$		1		5		10		10		5		1		
$n = 6$	1		6		15		20		15		6		1	
$n = 7$	1	7		21		35		35		21		7		1

Tabella 3.1: Triangolo di Tartaglia

Definizione 3.4.13. Una **combinazione semplice** di k elementi presi da n è un sottoinsieme di k elementi di un insieme con n elementi. Il numero di combinazioni semplici si denota con $c_{n,k}$ ed è dato dalla seguente formula:

$$c_{n,k} = \binom{n}{k}$$

Le combinazioni semplici contano quanti sottoinsiemi con un fissato numero di elementi ci sono. Quindi deve essere

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n$$

perché se sommo quanti sottoinsiemi ci sono di k elementi, per k che varia da 0 a n, trovo il numero totale di sottoinsiemi che è appunto 2^n.

Esempio 3.4.14. Quanti sottoinsiemi di 3 elementi ha $\{a, b, c, d, e, f\}$? Bisogna calcolare

$$\binom{6}{3} = \frac{6!}{3!3!} = \frac{6 \cdot 5 \cdot 4}{3 \cdot 2} = 20\,.$$

Esempio 3.4.15. Se X è un insieme di 5 elementi esistono:

- $\binom{5}{0} = 1$ sottoinsieme di X di cardinalità 0;
- $\binom{5}{1} = 5$ sottoinsiemi di X di cardinalità 1;
- $\binom{5}{2} = 10$ sottoinsiemi di X di cardinalità 2;
- $\binom{5}{3} = 10$ sottoinsiemi di X di cardinalità 3;

- $\binom{5}{4} = 5$ sottoinsiemi di X di cardinalità 4;

- $\binom{5}{5} = 1$ sottoinsieme di X di cardinalità 5.

Esempio 3.4.16. In quanti modi si possono giocare due numeri al lotto? In questo caso non importa con che ordine si giocano, bisogna considerare i sottoinsiemi di due elementi dell'insieme dei 90 numeri del lotto, quindi:

$$\binom{90}{2} = \frac{90!}{2!88!} = \frac{90 \cdot 89}{2} = 45 \cdot 89 = 4005\,.$$

Esempio 3.4.17. Supponiamo che per formare un'equipe medica ci voglia un anestesista, due medici e tre infermieri. Se in un ospedale sono presenti 4 anestesisti, 8 medici e 7 infermieri quante diverse equipe mediche si potranno formare? Per rispondere a questa domanda dobbiamo mettere insieme i concetti visti finora: in ogni equipe ci vuole un anestesista, un insieme di due medici e un insieme di tre di infermieri. Quanti insiemi di due medici posso formare a partire dagli 8 medici che ci sono in ospedale (non importa l'ordine con cui scelgo i medici)?. Ci sono $\binom{8}{2} = \frac{8!}{2 \cdot 6!} = 28$ possibili insiemi formati da due medici dell'ospedale. Riguardo agli infermieri, ragionando in maniera simile si può dire che ci sono $\binom{7}{3} = \frac{7!}{3!4!} = 35$ possibili insiemi di tre infermieri. In totale le possibili equipe saranno:

$$4 \text{ anestesisti } \times 28 \text{ team di medici } \times 35 \text{ team di infermieri} = 3920.$$

Per chiudere il quadro ci manca la seguente definizione

Definizione 3.4.18. Una **combinazione con ripetizione** di k elementi presi da n è un insieme di k elementi che può contenere anche delle ripetizioni (non è quindi un vero insieme...) presi da un insieme di n elementi. Il numero di combinazioni con ripetizione è dato da:

$$c'_{n,k} = \binom{n+k-1}{k}\,.$$

Esempio 3.4.19. Se al mercato ci sono pere, mele, kiwi e banane e voglio comprare due frutti (anche uguali tra loro) allora ho ($n = 4$, $k = 2$)

$$c'_{4,2} = \binom{n+k-1}{k} = \binom{5}{2} = \frac{5!}{2!3!} = 10$$

possibili scelte.

Ricapitolando, se $k \leq n$:

	senza ripetizione	**con ripetizione**
con ordine	disposizioni semplici $d_{n,k} = \frac{n!}{(n-k)!}$	disposizioni con ripetizione (seque $d'_{n,k} = n^k$
senza ordine	combinazioni semplici (sottoinsiemi) $c_{n,k} = \binom{n}{k}$	combinazioni con ripetizione $c'_{n,k} = \binom{n+k-1}{k}$

Inoltre:

- I sottoinsiemi di k elementi di un insieme con n elementi sono $\binom{n}{k}$;
- Le funzioni iniettive tra S e T sono $d_{|T|,|S|} = \frac{|T|!}{(|T|-|S|)!}$ (se $|S| \leq |T|$);
- Le funzioni biettive di S in T sono $|T|! = |S|!$ (se $|S| = |T|$).

3.5 Esercizi

1. Provare per induzione le seguenti proprietà:
   - per $n \geq 1$:
   $$\sum_{k=1}^{n} k^3 = \frac{n^2(n+1)^2}{4}$$
   - per $n \geq 2$:
   $$\sum_{k=2}^{n} (2k-3) = (n-1)^2$$
   - per $n \geq 2$:
   $$\sum_{k=2}^{n} k \cdot 2^k = (n-1) \cdot 2^{n+1}$$
   - per $n \geq 1$:
   $$\sum_{k=0}^{n-1} 2k+1 = n^2$$
   - per $n \geq 1$:
   $$5^n - 1 \text{ è un multiplo di } 4$$
2. Usare l'algoritmo di Euclide per trovare il Massimo Comun Divisore d delle seguenti coppie di numeri (a, b) e scrivere d come combinazione lineare di a e b:
   - $MCD(15, 32)$
   - $MCD(42, 12)$
   - $MCD(42, 15)$
   - $MCD(36, 84)$
   - $MCD(72, 124)$
   - $MCD(72, 100)$
3. Scrivere le tavole di addizione e moltiplicazione di $\mathbb{Z}_4$, $\mathbb{Z}_5$ e $\mathbb{Z}_6$ e dire quali elementi sono invertibili (rispetto alla moltiplicazione) nelle tre tavole.
4. Dimostrare che se $x \equiv y (mod\, n)$ e $z \in \mathbb{Z}$ allora $x + z \equiv y + z (mod\, n)$.
5. Se $A = \{1, 2, 3, 4, 5\}$ e $B = \{a, b, c, d, e, f, g, h\}$ quante funzioni ci sono tra A e B? E quante funzioni iniettive? Quanti sottoinsiemi di 3 elementi ha l'insieme B?
6. Se una gelateria offre 14 gusti di gelato, quanti possibili coni con due gusti si possono fare, considerando che nello scegliere due gusti non importa l'ordine con cui si scelgono (cioccolata e nocciola è uguale a nocciola e cioccolata)?

4 Strutture algebriche

Lo studio delle strutture algebriche ha come obiettivo di caratterizzare le proprietà delle operazioni: a partire dalle ben note proprietà delle operazioni tra numeri, si generalizza lo studio ad altri contesti più astratti.

4.1 Operazioni

Dato un insieme non vuoto A, si dice **operazione binaria** (o semplicemente **operazione**), oppure **legge di composizione interna** su A una funzione dal prodotto cartesiano $A \times A$ in A

$$* : A \times A \mapsto A.$$

L'immagine della coppia (a, b) tramite $*$ si indica con $a * b$.

Un insieme su cui sono definite una o più operazioni si dice **struttura algebrica**. Su uno stesso insieme si possono definire diverse operazioni, così come per esempio sull'insieme dei numeri interi definiamo la somma, il prodotto etc.

Definizione 4.1.1. Data una struttura algebrica $(A, *)$:

- l'operazione $*$ si dice **commutativa** se e solo se $a * b = b * a$, per ogni a, b in A;
- l'operazione $*$ si dice **associativa** se e solo se $a * (b * c) = (a * b) * c$, per ogni a, b, c in A;
- un elemento $e \in A$ si dice **elemento neutro** di A rispetto all' operazione $*$ se per ogni $a \in A$, $a * e = e * a = a$;
- se A ha elemento neutro, allora un elemento $a \in A$ si dice **invertibile** o **simmetrizzabile** se esiste $b \in A$ tale che $a * b = e = b * a$. L'elemento b è chiamato **inverso** o **simmetrico** di a.

Elementi neutri e elementi inversi (o simmetrizzabili) sono relativi all'operazione che si sta considerando. Operazioni diverse definite sullo stesso insieme possono avere in genere elementi neutri diversi. L'elemento neutro potrebbe non esistere, ma se esiste è unico.

Esempio 4.1.2. L'addizione tra numeri naturali

$$+ : \mathbb{N}_0 \times \mathbb{N}_0 \mapsto \mathbb{N}_0$$

è commutativa e associativa, 0 è l'elemento neutro ed è, inoltre, l'unico elemento invertibile di $(\mathbb{N}_0, +)$; invece, data la struttura $(\mathbb{Z}, +)$, ogni elemento di $\mathbb{Z}$ è simmetrizzabile rispetto all'addizione, dato che il simmetrico di ogni n è il numero $-n$ poiché $n + (-n) = 0$.

Esempio 4.1.3. La moltiplicazione tra numeri interi

$$\cdot : \mathbb{Z} \times \mathbb{Z} \mapsto \mathbb{Z}$$

è commutativa e associativa, 1 è l'elemento neutro e gli unici elementi invertibili sono 1 e -1, in quanto $1 \cdot 1 = 1$ e $-1 \cdot -1 = 1$.

Esempio 4.1.4. L'operazione di sottrazione su $\mathbb{Z}$ non è commutativa, perché se $n, m \in \mathbb{Z}$ si ha $n - m \neq m - n$. Non è neanche associativa, perché $(n - m) - h \neq n - (m - h)$. Anche la divisione è un'operazione su $\mathbb{Q}$ che non è commutativa né associativa.

Dato che in genere un'operazione $*$ è una funzione che ad ogni coppia di un insieme A associa un elemento di A, se l'insieme A è finito possiamo rappresentarla con una tabella in cui le righe e le colonne sono etichettate con gli elementi di A e nella casella della tabella corrispondente alla riga a e alla colonna b si inserisce l'elemento $a * b$. La proprietà commutativa dell'operazione corrisponde alla simmetria della tabella rispetto alla diagonale data dalle coppie del tipo (x, x). L'elemento neutro invece può essere individuato in una tabella andando a cercare una riga e una colonna in cui si ripetono gli elementi nello stesso ordine in cui sono elencati come etichette delle colonne o delle righe. Infine gli elementi invertibili o simmetrizzabili sono quegli elementi che hanno l'elemento neutro nella riga e nella colonna che gli corrisponde.

Esempio 4.1.5. Sia $A = \{a, b, c, d\}$ e consideriamo l'operazione $*$ data dalla seguente tabella:

$*$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

La tabella rappresenta la seguente operazione su A:

- $a * a = a$
- $b * a = b$
- $c * a = c$
- $d * a = d$
- $a * b = b$
- $b * b = c$
- $c * b = d$
- $d * b = b$
- $a * c = c$
- $b * c = d$
- $c * c = a$
- $d * c = a$
- $a * d = d$
- $b * d = a$
- $c * d = b$
- $d * d = c$

Questa operazione è commutativa e associativa: la commutatività è facilmente controllabile dalla tabella, ma non l'associatività. L'elemento a è l'elemento neutro, e tutti gli elementi sono invertibili.

4.2 Strutture algebriche

Definizione 4.2.1. Sia $(A, *)$ una struttura algebrica, allora

- $(A, *)$ è un **semigruppo** se $*$ è associativa;
- $(A, *)$ è un **monoide** se è un semigruppo ed esiste l'elemento neutro;
- $(A, *)$ è un **gruppo** se è un monoide e ogni elemento di A è invertibile.

Esempio 4.2.2. $(\mathbb{N}_0, +)$ è un semigruppo, $(\mathbb{N}, +)$ è un monoide e $(\mathbb{Z}, +)$ è un gruppo.

Esempio 4.2.3. L'insieme dei numeri razionali $\mathbb{Q}$ non è un gruppo con l'operazione di moltiplicazione. Infatti l'elemento 0 non è invertibile perché per qualsiasi $x \in \mathbb{Q}$ si ha $0 * x = 0$ mentre l'elemento neutro della moltiplicazione è 1. Però $(\mathbb{Q} \setminus \{0\}, \cdot)$ è un gruppo. Analogamente, anche $(\mathbb{R}, \cdot)$ non è un gruppo.

Esempio 4.2.4. Consideriamo l'insieme delle parole A^+ su un alfabeto A. Possiamo definire su A^+ un'operazione $\circ$ detta **concatenazione** tale che $u \circ v = uv$ è la parola ottenuta scrivendo una dopo l'altra le parole u e v. Per esempio, se $u = abc$ e $v = aabbc$ allora $u \circ v = abcaabbc$. L'operazione di concatenazione non è commutativa, perché $uv \neq vu$, ma è associativa. Quindi la struttura $(A^+, \circ)$ è un semigruppo, ma non un monoide dato che non esiste l'elemento neutro. La struttura $(A^+ \cup \{\varepsilon\}, \circ)$, dove il simbolo ε è la parola vuota (la parola di lunghezza 0 tale che $\forall u \in A^+, \varepsilon \circ u = u \circ \varepsilon = u$), invece è un monoide. D'altra parte $(A^+ \cup \{\varepsilon\}, \circ)$ non è un gruppo, poichè nessuno degli elementi di $A^+ \cup \{\varepsilon\}$ è invertibile rispetto all' operazione $\circ$.

Esempio 4.2.5. Consideriamo l'insieme $5\mathbb{N} = \{5n \mid n \in \mathbb{N}\}$ dei multipli di 5. Su $5\mathbb{N}$ definiamo l'operazione

$$n *_5 m = \frac{nm}{5}.$$

Questa operazione è commutativa e associativa. Inoltre l'elemento neutro è 5 perché $n *_5 5 = \frac{5n}{5} = n$ e l'unico elemento invertibile è 5 perché $5 *_5 5 = 5$ e l'unico altro caso in cui $n *_5 m = \frac{nm}{5} = 5$ è quando $n = 1$ e $m = 25$ ma $1 \notin 5\mathbb{N}$. Quindi $(\mathbb{Z}, *_5)$ è un monoide.

Esempio 4.2.6. Se $A = \{1, 2, 3\}$ con A^A denotiamo l'insieme delle funzioni di A in A. Consideriamo l'operazione $\circ$ di composizione di funzioni, allora

1. $\circ$ non è commutativa: per esempio, siano $f, g \in A^A$ tali che $f(a) = b, f(b) = c, f(c) = c$ e $g(a) = a, g(b) = a, g(c) = c$, allora $(f \cdot g)(a) = f(g(a)) = f(a) = b$ e $(g \cdot f)(a) = g(f(a)) = g(b) = a$, quindi $g \circ f \neq f \circ g$;

2. $\circ$ è associativa;

3. la funzione identità id_A è l'elemento neutro rispetto a $\cdot$;

4. $f \in A^A$ è biettiva se e soltanto se è invertibile rispetto all' operazione $\circ$.

Sia P_A l'insieme delle funzioni biettive (dette anche permutazioni) di A. La struttura $(P_A, \circ)$ è un gruppo (perché ogni funzione biettiva è invertibile) detto **gruppo delle permutazioni** di A.

Definizione 4.2.7. Un gruppo $(G, *)$ si dice **commutativo** (o **abeliano**) se l' operazione $*$ è commutativa.

Dagli esempi precedenti, possiamo stabilire che $(\mathbb{Z}, +)$ è un gruppo commutativo, mentre $(P_A, \circ)$ non lo è. Quali sono altri gruppi commutativi che si possono considerare sugli insiemi numerici?

Esempio 4.2.8. Sia A un insieme e consideriamo l'insieme $\mathcal{P}(A)$ dei sottoinsiemi di A. Su $\mathcal{P}(A)$ possiamo definire due operazioni, l'unione $\cup$ e l'intersezione $\cap$: sono entrambe commutative perché per ogni sottoinsieme X, Y di A si ha che $X \cup Y = Y \cup X$ e $X \cap Y = Y \cap X$. Sono associative perché $(X \cup Y) \cup Z = X \cup (Y \cup Z)$ e analogamente per l'intersezione. Inoltre l'elemento neutro di $\cup$ è $\emptyset$ dato che per ogni $X \in \mathcal{P}(A)$ si ha che $X \cup \emptyset = X$, mentre l'elemento neutro di $\cap$ è A dato che $X \cap A = X$. L'unico elemento invertibile rispetto a $\cup$ è $\emptyset$ dato che per avere $X \cup Y = \emptyset$ l'unica possibilità è appunto che sia $X = Y = \emptyset$. Analogamente, l'unico elemento invertibile rispetto a $\cap$ è A. Quindi le due strutture $(\mathcal{P}(A), \cup)$ e $(\mathcal{P}, \cap)$ sono dei monoidi.

Esempio 4.2.9. Consideriamo l'insieme $\mathbb{Z}_m$ delle classi di resto modulo m con l'operazione di moltiplicazione $(\mathbb{Z}_m, \cdot)$. Il prodotto è commutativo e associativo, l'elemento neutro è $[1]_m$. Dal capitolo precedente, sappiamo che un elemento $[a]_m$ di $\mathbb{Z}_m$ è invertibile rispetto al prodotto se $MCD(a, m) = 1$. In particolare se m è un numero primo, allora tutte le classi $[a]_m$ con $a \neq 0$ sono invertibili.

Le operazioni numeriche che abbiamo considerato finora, cioè somma e prodotto, sono in relazione l'una con l'altra, per esempio soddisfano la proprietà distributiva: per ogni n, m, h si ha che $n(m+h) = nm + nh$. Per generalizzare questa situazione consideriamo adesso strutture algebriche con due operazioni.

Definizione 4.2.10. Una struttura algebrica $(A, *_1, *_2)$ è un **anello** se

1. $(A, *_1)$ è un gruppo commutativo;
2. $(A, *_2)$ è un semigruppo;
3. vale la proprietà distributiva di $*_2$ su $*_1$, ovvero per ogni $x, y, z \in A$

$$\begin{aligned} x *_2 (y *_1 z) &= (x *_2 y) *_1 (x *_2 z) \\ (y *_1 z) *_2 x &= (y *_2 x) *_1 (z *_2 x). \end{aligned}$$

(la proprietà distributiva la scriviamo in due modi diversi perché in genere l'operazione $*_2$ non è commutativa.)

Esempio 4.2.11. $(\mathbb{Z}, +, \cdot)$ è un anello, infatti $(\mathbb{Z}, +)$ è un gruppo, $(\mathbb{Z}, \cdot)$ è un semigruppo e vale la proprietà distributiva di $\cdot$ su $+$. Anche $(\mathbb{R}, +, \cdot)$ e $(\mathbb{Q}, +, \cdot)$ sono anelli, mentre $(\mathbb{N}, +, \cdot)$ non lo è perché $(\mathbb{N}, +)$ non è un gruppo.

Esempio 4.2.12. Un esempio molto importante di anello, che però non approfondiremo in questi appunti, è l'anello dei polinomi. Consideriamo l'insieme di tutti i polinomi, di qualsiasi grado, nella variabile x che abbiano come coefficienti i numeri interi. Questo insieme lo denotiamo con $\mathbb{Z}[x]$ e lo chiamiamo anello dei polinomi a coefficienti interi. Possiamo definire su $\mathbb{Z}[x]$ le operazioni di somma e prodotto tra polinomi, e con queste operazioni la struttura è un anello. Anche l'insieme $\mathbb{R}[x]$ dei polinomi a coefficienti reali con le operazioni di somma e prodotto è un anello.

Definizione 4.2.13. Una struttura algebrica $(A, *_1, *_2)$ è un **campo** se

1. $(A, *_1)$ è un gruppo commutativo;
2. $(A \setminus \{0\}, *_2)$ è un gruppo;
3. vale la proprietà distributiva di $*_2$ su $*_1$.

Esempio 4.2.14. $(\mathbb{R}, +, \cdot)$ è un campo, poichè $(\mathbb{R}, +)$ è un gruppo commutativo, $(\mathbb{R} \setminus \{0\}, \cdot)$ è un gruppo e vale la proprietà distributiva di $\cdot$ su $+$. Anche $(\mathbb{Q}, +, \cdot)$ è un campo, mentre $(\mathbb{Z}, +, \cdot)$ non lo è perché $(\mathbb{Z} \setminus \{0\}, \cdot)$ non è un gruppo.

Per ogni numero primo p, l'insieme $\mathbb{Z}_p$ degli interi modulo p è un campo con le operazioni di somma e prodotto, perché $(\mathbb{Z}_p \setminus \{[0]_p\}, \cdot)$ è un gruppo.

Un altro campo molto importante è il campo dei numeri complessi, che non approfondiremo in questi appunti.

4.3 Sottostrutture e omomorfismi

Nelle prossime pagine proviamo a generalizzare nel contesto delle strutture algebriche alcune nozioni insiemistiche come i sottoinsiemi e le funzioni.

Definizione 4.3.1. Sia $(A, *)$ una struttura algebrica. Un sottoinsieme H di A è detto **stabile** rispetto all'operazione $*$ se per ogni $x, y \in H$ si ha che $x * y \in H$.

Esempio 4.3.2. Abbiamo in realtà già visto un esempio di insieme stabile rispetto ad una operazione: quando abbiamo considerato l'insieme $\mathbb{Q}$ dei numeri razionali e abbiamo detto che non è un gruppo. Se considero il sottoinsieme $\mathbb{Q} \setminus \{0\}$ ottenuto togliendo l'elemento 0 da $\mathbb{Q}$, ho un sottoinsieme che è stabile rispetto al prodotto, perché il prodotto di due numeri diversi da zero è sempre diverso da zero. In particolare $\mathbb{Q} \setminus \{0\}$ è un gruppo.

Esempio 4.3.3. Data la struttura $(\mathbb{N}, +)$, l'insieme $2\mathbb{N} \subseteq \mathbb{N}$ è stabile, in quanto la somma di due numeri pari è sempre pari: se $x, y \in 2\mathbb{N}$, allora $x = 2a$ e $y = 2b$, con $a, b \in \mathbb{N}$, dunque $x + y = 2a + 2b = 2(a + b) \in 2\mathbb{N}$. L'insieme D dei numeri naturali dispari invece non è stabile, dato che la somma di due numeri dispari è un numero pari: se $x, y \in D$, allora $x = 2a+1$ e $y = 2b+1$, con $a, b \in \mathbb{N}$, dunque $x + y = 2a + 2b + 2 = 2(a + b + 1) \notin D$.

Esempio 4.3.4. Consideriamo l'insieme delle parole A^* sull'alfabeto $A = \{a, b, c\}$. L'operazione di concatenazione rende questo insieme un monoide. Sia $S = \{u \in A^* \mid u \text{ inizia con la lettera } a\}$, cioè S è il sottoinsieme di A^* formato da tutte le parole che iniziano con la lettera a. L'insieme S è stabile rispetto all'operazione di concatenazione, dato che se considero due parole di S, la parola che ottengo concatenando queste due è ancora una parola di S perché inizierà con la lettera a. Invece l'insieme delle parole di lunghezza 3 non è un sottoinsieme stabile di A^* perché concatenando due parole di lunghezza tre non si ottiene ancora una parola di lunghezza 3.

Teorema 4.3.5. *Dato un monoide $(A, *)$, l'insieme*

$$U(A) = \{a \in A \mid a \text{ è invertibile } \}$$

è stabile rispetto all'operazione $*$ ed è un gruppo.

Dimostrazione. Chiamiamo e l'elemento neutro di A. Se $a, b \in U(A)$, allora esistono $a', b' \in U(A)$ tali che

$$a * a' = e \quad \text{e} \quad b * b' = e.$$

L'inverso di $a * b$ è $b' * a'$:

$$(b' * a') * (a * b) = b * (a' * a) * b' = b * e * b' = b * b' = e,$$

dunque $a * b \in U(A)$. Quindi $U(A)$ è un monoide cha ha elemento neutro perché l'elemento neutro è sempre invertibile, inoltre ogni suo elemento è invertibile per definizione, quindi $U(A)$ è un gruppo. □

Esempio 4.3.6. La struttura $(\mathbb{Q}, \cdot)$ è un monoide, e solo 0 non è invertibile, quindi $U(\mathbb{Q}) = \mathbb{Q} \setminus \{0\}$ e $(\mathbb{Q} \setminus \{0\}, \cdot)$ è un gruppo.

Esempio 4.3.7. Se p è un numero primo l'unico elemento non invertibile di $\mathbb{Z}_p$ è $[0]_p$, quindi $(\mathbb{Z}_p, +, \cdot)$ è un campo, dato che $(\mathbb{Z}_p \setminus \{[0]_p\}, \cdot)$ è un gruppo.

Definizione 4.3.8. Sia $(G, \cdot)$ un gruppo e denotiamo con 1_G l'elemento neutro di G e, per ogni $g \in G$, con g' l'inverso di g. Un sottoinsieme H di G è un **sottogruppo** di G se:

- è stabile rispetto a $\cdot$;
- $1_G \in H$;
- se $h \in H$ allora $h' \in H$, cioè H contiene l'inverso dei propri elementi.

Esempio 4.3.9. L'insieme dei numeri pari è un sottogruppo di $(\mathbb{N}, +)$. Infatti abbiamo già visto che è stabile rispetto al prodotto. Inoltre 0 è un numero pari, e la negazione di un numero pari è un numero pari.

Esempio 4.3.10. L'insieme $\mathbb{Z} \setminus \{0\}$ dei numeri interi diverso da 0 è un sottoinsieme di $\mathbb{Q} \setminus \{0\}$ ed è stabile rispetto al prodotto. Ma non è un sottogruppo perché non contiene l'inverso dei suoi elementi (a parte 1).

Proposizione 4.3.11. *Sia $(G, \cdot)$ un gruppo e $H \subseteq G$. H è un sottogruppo se e solo se per ogni $h, k \in H$ si ha $h \cdot k' \in H$.*

Dimostrazione. Dobbiamo dimostrare due cose: che se H è un sottogruppo allora soddisfa la proprietà scritta nell'enunciato e viceversa, cioè se H soddisfa la proprietà descritta nell'enunciato allora è un sottogruppo.

Iniziamo supponendo che H sia un sottogruppo. Allora se $h, k \in H$ vuol dire che anche l'inverso k' appartiene a H e quindi, poiché in particolare H è stabile, si ha $h \cdot k' \in H$.

Viceversa, supponiamo per ipotesi che per ogni $h, k \in H$ si ha $h \cdot k' \in H$, dobbiamo mostrare le tre condizioni della definizione 4.3.8. Iniziamo dalla seconda: se considero $h = k$ allora l'ipotesi mi assicura che $h \cdot h' \in H$ e cioè $1_G \in H$. Allora posso considerare $h = 1_G$ e per ogni $k \in H$ avrò $1_G \cdot k' \in H$ e quindi $k' \in H$, così anche la terza condizione è verificata. Per mostrare la prima, notiamo che $(k')' = k$ cioè l'inverso dell'inverso è l'elemento di partenza. Quindi se $h, k \in H$, per quanto detto prima anche $k' \in H$ e per la nostra ipotesi $h \cdot (k')' = h \cdot k \in H$: quindi H è un sottogruppo di G. □

Estendiamo alle strutture algebriche il concetto di funzione.

Definizione 4.3.12. Date due strutture algebriche $(A, *)$ e $(B, \odot)$, una funzione $f : A \to B$ si chiama **omomorfismo** se per ogni $x, y \in A$:

$$f(x * y) = f(x) \odot f(y).$$

In altre parole un omomorfismo è una funzione che *trasforma* l'operazione del dominio nell'operazione del codominio.

Esempio 4.3.13. La funzione

$$f : n \in \mathbb{N} \mapsto 2^n \in \mathbb{N}$$

è un omomorfismo tra $(\mathbb{N}, +)$ e $(\mathbb{N}, \cdot)$, poichè

$$f(n + m) = 2^{n+m} = 2^n \cdot 2^m = f(n) \cdot f(m),$$

per ogni $n, m \in \mathbb{N}$.

Esempio 4.3.14. La funzione

$$f : a \in A^* \mapsto \#a \in \mathbb{N}$$

è un omomorfismo tra $(A^*, \circ)$ e $(\mathbb{N}, +)$, infatti per ogni parola $u, v \in A^*$ si ha:

$$f(a \circ b) = \#ab = \#a + \#b = f(a) + f(b).$$

Esempio 4.3.15. Per ogni $n \in \mathbb{N}$ sia $\ell(n)$ il numero di lettere che compongono la parola che descrive il numero n: per esempio $\ell(1) = 3$ dato che nella parola "*uno*" ci sono tre lettere, mentre $\ell(5) = 6$ perché nella parola "*cinque*" ci sono sei lettere. La funzione $\ell : \mathbb{N} \to \mathbb{N}$ che assegna ad ogni n il numero $\ell(n)$ non è un omomorfismo di $(\mathbb{N}, +)$ in $(\mathbb{N}, +)$. Infatti per esempio

$$\ell(3 + 5) = \ell(8) = 4$$

mentre

$$\ell(3) = 3 \text{ e } \ell(5) = 6, \text{ quindi } \ell(3) + \ell(5) = 9\,.$$

Esempio 4.3.16. Consideriamo la struttura nell'Esempio 4.1.5 e la funzione $f : A \to A$ definita da:

$$f(a) = b \quad f(b) = c \quad f(c) = a \quad f(d) = d$$

La funzione f non è un omomorfismo perché per esempio $f(a) * f(b) = b * c = d$ ma $f(a * b) = f(b) = c$.

Definizione 4.3.17. Un **isomorfismo** è un omomorfismo biettivo, inoltre due strutture algebriche sono **isomorfe** se esiste un isomorfismo tra loro.

Esempio 4.3.18. Consideriamo la strutture $(A, *)$ dell'esempio 4.1.5. La funzione

$$\begin{aligned} f \ : \ & A \to \mathbb{Z}_4 \\ & a \mapsto [0]_4 \\ & b \mapsto [1]_4 \\ & c \mapsto [2]_4 \\ & d \mapsto [3]_4 \end{aligned}$$

è un isomorfismo tra $(A, *)$ e $(\mathbb{Z}_4, +)$. Infatti è una funzione biettiva e valgono le proprietà degli omomorfismi, come si può notare confrontando le tabelle delle due operazioni:

$*$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

$+$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[1]_4$	$[1]_4$	$[2]_4$	$[3]_4$	$[0]_4$
$[2]_4$	$[2]_4$	$[3]_4$	$[0]_4$	$[1]_4$
$[3]_4$	$[3]_4$	$[0]_4$	$[1]_4$	$[2]_4$

Esempio 4.3.19. La funzione che ad ogni parola su A^* associa la sua lunghezza non è un isomorfismo di $(A^*, \circ)$ in $(\mathbb{N}, +)$ perché non è biettiva.

Le operazioni di due strutture isomorfe soddisfano le stesse proprietà, sono praticamente la stessa operazione se non fosse che gli elementi hanno nomi diversi. Si dice anche che l'algebra è lo studio delle strutture algebriche *a meno di isomorfismi*: questo vuol dire che l'algebra è interessata alle proprietà algebriche indipendentemente dal nome degli elementi.

4.4 Esercizi

- Sull'insieme $A = \{a, b, c\}$ si considerino le operazioni date dalle seguenti tabelle:

$*_1$	a	b	c
a	b	a	c
b	a	b	c
c	c	c	a

$*_2$	a	b	c
a	a	b	c
b	b	a	a
c	c	a	a

  Tali operazioni sono commutative? Hanno un elemento neutro? E elementi invertibili?

- Sull'insieme $B = \{0, 1\}$ si consideri l'operazione di AND data dalla seguente tabella:

	0	1
0	0	0
1	0	1

  L'operazione è commutativa e/o associativa? Esiste l'elemento neutro? Gli elementi sono invertibili? Dimostrare che la funzione $f : B \to \mathbb{Z}_2$ tale che $f(0) = [0]_2$ e $f(1) = [1]_2$ è un isomorfismo di (B, AND) in $(\mathbb{Z}_2, \cdot)$.

- Si consideri l'insieme $\mathbb{Z} \times \mathbb{Z}$ e l'operazione

$$(n, m) * (h, k) = (n + h, mk).$$

  L'operazione $*$ ha un elemento neutro? Ci sono elementi invertibili?

- L'insieme $\{2^n \mid n \in \mathbb{N}\}$ è un sottoinsieme stabile di $(\mathbb{Z}, \cdot)$?

- Si consideri il sottoinsieme $H = \{[0]_4, [2]_4\}$ di $\mathbb{Z}_4$. H è stabile rispetto a $+$? E rispetto al prodotto? Mostrare che $(H, +)$ è un sottogruppo di $(\mathbb{Z}_4, +)$. Sia f la funzione da H a $\mathbb{Z}_2$ tale che $f([0]_4) = [0]_2$ e $f([2]_4) = [1]_2$. Dimostrare che f è un isomorfismo di $(H, +)$ in $(\mathbb{Z}_2, +)$.

- Dire delle seguenti funzioni se sono omomorfismi:

$$\begin{aligned}
f_1 &: n \in (\mathbb{Z}, +) \to n \in (\mathbb{Z}, \cdot) \\
f_2 &: n \in (\mathbb{Z}, +) \to n + 1 \in (\mathbb{Z}, +) \\
f_3 &: [n]_4 \in (\mathbb{Z}_4, +) \to [2n]_8 \in (\mathbb{Z}_8, +) \\
f_4 &: [n]_4 \in (\mathbb{Z}_4, \cdot) \to [2n]_8 \in (\mathbb{Z}_8, \cdot) \\
f_5 &: [n]_2 \in (\mathbb{Z}_2, +) \to 2n \in (\mathbb{Z}, +)
\end{aligned}$$

- Sia A^* il monoide delle parole sull'alfabeto $\{a, b, c\}$ con l'operazione di concatenazione. Si consideri l'insieme $B = \{a, b\}$ e il monoide delle parole B^* su B. L'insieme B^* è un sottoinsieme di A^*. Si dimostri che B^* è stabile in A^* rispetto all'operazione di concatenazione. La funzione $f : u \in B^* \mapsto uc \in A^*$ (cioè tale che $f(u)$ è la parola uc ottenuta concatenando u e c) è un omomorfismo di B^* in A^*?

- Sia $A = \{a, b, c\}$ e A^* il monoide delle parole su A. Per ogni $u \in A^*$, con $\#(a, u)$ denotiamo il numero di lettere a presenti in u. La funzione

$$f : u \in A^* \mapsto \#(u, a) \in \mathbb{N}$$

  è un omomorfismo di $(A^*, \circ)$ in $(\mathbb{N}, +)$? E' biettiva?

- (difficile) Sia $X = \{1, 2, 3\}$ e P_X l'insieme di tutte le permutazioni di X, cioè delle funzioni biettive di X in X. Quanti elementi ha P_X? Per ogni funzione $f \in P_X$ sia $fix(f) = \{x \in X \mid f(x) = x\}$. Si consideri l'operazione $\circ$ di composizione di funzioni. La funzione

$$fix : f \in P_X \mapsto fix(f) \in \mathcal{P}(X)$$

  è un omomorfismo di $(P_X, \circ)$ in $(\mathcal{P}(X), \cap)$? E' una funzione biettiva?

5 Matrici

5.1 Prime definizioni

Una matrice $m \times n$ a valori reali è una tabella con m righe e n colonne costituite da numeri reali. L'insieme delle matrici $m \times n$ si indica con $\mathcal{M}_{m,n}$.

Esempio 5.1.1. Il seguente è un esempio di una matrice con 2 righe e 3 colonne:

$$\begin{pmatrix} 2 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \in \mathcal{M}_{2,3}$$

Definizione 5.1.2. Una matrice in cui il numero di righe è uguale al numero di colonne si chiama **matrice quadrata**, l'insieme delle matrici quadrate con n righe e colonne si indica con $\mathcal{M}_n$. Se $A \in \mathcal{M}_n$ allora n è **l'ordine** della matrice A.

Esempio 5.1.3. Il seguente è un esempio di matrice 3×3 quadrata di ordine 3

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & \pi \end{pmatrix} \in \mathcal{M}_3$$

(nota che gli elementi che compaiono in una matrice possono essere numeri reali qualsiasi).

Notazione. Per scrivere una matrice in forma generica uso la seguente notazione: se $A \in \mathcal{M}_{m,n}$ allora si scrive

$$A = (a_{ij}) = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \dots & a_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & a_{m3} & \dots & a_{mn} \end{pmatrix}$$

cioè gli elementi di A sono del tipo a_{ij} dove i è l'indice della riga e j è l'indice della colonna. Gli elementi a_{ii} formano la *diagonale* della matrice.

Esempio 5.1.4. Se $m = 3$ e $m = 2$ allora $A \in \mathcal{M}_{3,2}$

$$A = (a_{ij}) = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \\ a_{31} & a_{32} \end{pmatrix}$$

dove $i = 1, 2, 3$ e $j = 1, 2$.

Esempio 5.1.5. Se

$$A = \begin{pmatrix} 3 & 1 \\ 2 & 0 \\ 0 & 3 \end{pmatrix} \in \mathcal{M}_{3,2}$$

allora $a_{11} = 3$, $a_{12} = 1$, $a_{21} = 2$, $a_{22} = 0$, $a_{31} = 0$, $a_{32} = 3$

Definizione 5.1.6. Se $A \in \mathcal{M}_{1,m}$, cioè se A ha una riga e n colonne, A si dice **vettore riga**

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n}. \end{pmatrix}$$

Se $A \in \mathcal{M}_{m,1}$, cioè se A ha m righe e una colonne, A si dice **vettore colonna**

$$A = \begin{pmatrix} a_{11} \\ a_{21} \\ a_{31} \\ \vdots \\ a_{m,1} \end{pmatrix}$$

Definizione 5.1.7. Sia $A \in \mathcal{M}_{m,n}$. La **trasposta di** A è una matrice $A^T \in \mathcal{M}_{n,m}$ ottenuta da A scambiando le righe con le colonne, cioè se $A = (a_{ij})$ allora $A^T = (a_{ji})$.

Esempio 5.1.8.

$$A = \begin{pmatrix} 1 & 0 & 1 & 2 \\ 3 & 1 & 1 & 1 \\ 0 & -1 & 3 & -4 \end{pmatrix} \in \mathcal{M}_{3,4}$$

$$A^T = \begin{pmatrix} 1 & 3 & 0 \\ 0 & 1 & -1 \\ 1 & 1 & 3 \\ 2 & 1 & -4 \end{pmatrix} \in \mathcal{M}_{4,3}$$

Se $A \in \mathcal{M}_{1,n}$ è un vettore riga allora $A^T \in \mathcal{M}_{n,1}$ è un vettore colonna (e viceversa)

Definizione 5.1.9. Una matrice $A \in \mathcal{M}_{m,n}$ si dice *nulla* se tutti i suoi elementi sono uguali a 0. In ogni $\mathcal{M}_{m,n}$ c'è una matrice nulla che indichiamo con $O_{m,n}$. La *matrice identica* di ordine n è la matrice quadrata $I_n = (\delta_{ij}) \in \mathcal{M}_n$ dove $\delta_{ii} = 1$ e $\delta_{ij} = 0$ per ogni $i \neq j$. Cioè I_n è la matrice quadrata di ordine n che ha tutti gli elementi uguali a 0 tranne quelli sulla diagonale che sono uguali a 1.

Esempio 5.1.10. La matrice

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

è una matrice nulla. Se $n = 2$

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Se $n = 3$

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

5.2 Operazioni tra matrici

Definizione 5.2.1 (Somma di matrici)**.** Se $A, B \in \mathcal{M}_{m,n}$ e $A = (a_{ij})$ e $B = (b_{ij})$, allora $A+B = (a_{ij}+b_{ij}) \in \mathcal{M}_{m,n}$, cioè la somma di due matrici A e B è la matrice che ha come elementi la somma degli elementi di A e di B.

Esempio 5.2.2.

$$A = \begin{pmatrix} 1 & 2 \\ 0 & -3 \end{pmatrix} \qquad B = \begin{pmatrix} 0 & 1 \\ -2 & 1 \end{pmatrix}$$

$$A + B = \begin{pmatrix} 1+0 & 2+1 \\ 0-2 & -3+1 \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ -2 & -2 \end{pmatrix}$$

Nota che la somma di due matrici si definisce solo quando le due matrici hanno lo stesso numero di righe e di colonnne.

Proprietà. Posso considerare la struttura algebrica $(\mathcal{M}_{m,n}, +)$ che ha le seguenti proprietà:

- La somma è associativa e commutativa.
- L'elemento neutro è la *matrice nulla* $O_{m,n} \in \mathcal{M}_{m,n}$

  $A + O_{m,n} = (a_{ij} + 0) = (a_{ij}) = A$
- Una matrice $A \in \mathcal{M}_{m,n}$ è simmetrizzabile se esiste A' tale che

  $A + A' = 0 \Rightarrow (a_{ij} + a'_{ij}) = (z_{ij}) \Rightarrow a_{ij} + a'_{ij} = 0 \Rightarrow a'_{ij} = -a_{ij}\ \forall i, j \Rightarrow A' = (-a_{ij})$

  quindi tutte le matrici (a_{ij}) sono simmetrizzabili e il simmetrico è la matrice $(-a_{ij})$.

Perciò la struttura algebrica $(\mathcal{M}_{m,n}, +)$ è un gruppo.

Definizione 5.2.3. Se $A \in \mathcal{M}_{m,n}$ e $B \in \mathcal{M}_{n,k}$ allora il **prodotto righe per colonne** di A e B è la matrice $C = A \cdot B = (c_{ij}) \in \mathcal{M}_{m,k}$ dove per ogni $i = 1, \ldots, m$ e $j = 1, \ldots, k$:

$$c_{ij} = \sum_{h=1}^{n} (a_{ih} \cdot b_{hj}). \tag{5.1}$$

Nota che per poter definire il prodotto righe per colonne, il numero di colonne di A deve essere uguale al numero di righe di B.

Esempio 5.2.4. Consideriamo il caso $m = n = k = 2$

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \qquad B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \qquad A \cdot B = C = \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix}$$

$$c_{11} = \sum_{h=1}^{2} (a_{1h} \cdot b_{h1}) = (a_{11} \cdot b_{11}) + (a_{12} \cdot b_{21})$$

$$c_{12} = \sum_{h=1}^{2} (a_{1h} \cdot b_{h2}) = (a_{11} \cdot b_{12}) + (a_{12} \cdot b_{22})$$

$$c_{21} = \sum_{h=1}^{2} (a_{2h} \cdot b_{h1}) = (a_{21} \cdot b_{11}) + (a_{22} \cdot b_{21})$$

$$c_{22} = \sum_{h=1}^{2} (a_{2h} \cdot b_{h2}) = (a_{21} \cdot b_{12}) + (a_{22} \cdot b_{22})$$

Quindi per esempio:

$$A = \begin{pmatrix} 2 & 0 \\ 1 & 2 \end{pmatrix} \qquad B = \begin{pmatrix} 3 & 1 \\ 1 & 2 \end{pmatrix} \qquad C = A \cdot B = \begin{pmatrix} 6 & 2 \\ 5 & 5 \end{pmatrix}$$

Esempio 5.2.5. Se $A \in \mathcal{M}_{2,3}$ e $B \in \mathcal{M}_{3,1}$ allora $A \cdot B \in \mathcal{M}_{2,1}$

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \qquad B = \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix}$$

$$A \cdot B = C = \begin{pmatrix} 1 \cdot 0 + 0 \cdot 1 + 1 \cdot 2 \\ 0 \cdot 0 + 1 \cdot 1 + 1 \cdot 2 \end{pmatrix} = \begin{pmatrix} 2 \\ 3 \end{pmatrix}$$

$$c_{11} = \sum_{h=1}^{3} (a_{1h} + b_{h1}) \qquad c_{21} = \sum_{h=1}^{3} (a_{2h} + b_{h1})$$

Proprietà. Ci chiediamo adesso che proprietà ha la struttura algebrica $(\mathcal{M}_n, \cdot)$.

- Il prodotto righe per colonne NON è commutativo.

  Esempio 5.2.6.

$$B = \begin{pmatrix} 3 & 1 \\ 1 & 2 \end{pmatrix} \qquad A = \begin{pmatrix} 2 & 0 \\ 1 & 2 \end{pmatrix}$$

$$A \cdot B = \begin{pmatrix} 6 & 2 \\ 5 & 5 \end{pmatrix} \qquad B \cdot A = \begin{pmatrix} 7 & 2 \\ 4 & 4 \end{pmatrix} \qquad \Rightarrow A \cdot B \neq B \cdot A$$

- Il prodotto righe per colonne è associativo.

- Se considero matrici quadrate con $n = m$, allora l'elemento neutro per il prodotto righe per colonne è la matrice identica. Se $A \in \mathcal{M}_n$,

$$A \cdot I_n = A = I_n \cdot A$$

  Per esempio per $n = 2$ e $A = (a_{ij})$ allora $A \cdot I_2 = (c_{ij}) \in \mathcal{M}_2$ con
  $c_{11} = (a_{11} \cdot \delta_{11}) + (a_{12} \cdot \delta_{21}) = a_{11}$
  $c_{12} = (a_{11} \cdot \delta_{12}) + (a_{12} \cdot \delta_{22}) = a_{12}$
  $c_{21} = (a_{21} \cdot \delta_{11}) + (a_{22} \cdot \delta_{21}) = a_{21}$
  $c_{22} = (a_{21} \cdot \delta_{12}) + (a_{22} \cdot \delta_{22}) = a_{22}$
  (dove $\delta_{ii} = 1$ e $\delta_{ij} = 0$ per $i \neq j$). Quindi $A \cdot I_2 = A$.

  Esempio 5.2.7.

$$A = \begin{pmatrix} 2 & 0 \\ 1 & 3 \end{pmatrix} \qquad I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$A \cdot I_2 = \begin{pmatrix} 2 & 0 \\ 1 & 3 \end{pmatrix} = A \qquad I_2 \cdot A = \begin{pmatrix} 2 & 0 \\ 1 & 3 \end{pmatrix} = A$$

Quindi $(\mathcal{M}_n, \cdot)$ è un monoide non commutativo. Non è un gruppo perché non tutti gli elementi sono simmetrizzabili rispetto al prodotto righe per colonne.

5.3 Determinante di una matrice

Definizione 5.3.1. Ad ogni matrice quadrata $A \in \mathcal{M}_n$ associamo un numero reale $det(A) \in \mathbb{R}$ chiamato il **determinante di** A che è l'unico ad avere le seguenti proprietà:

- Se $A = I_n$ (cioè I_n è la matrice identica) allora $\det I_n = 1$.

- se B è ottenuta scambiando due righe o due colonne di A, allora $\det B = -\det A$,
- se B è ottenuta moltiplicando una riga o una colonna di A per k, allora $\det B = k \det A$,
- se B è ottenuta sommando una riga o una colonna rispettivamente di A a un'altra, allora $\det B = \det A$.

Queste definizione non da indicazioni su *come* calcolare il determinante, ma ci dice quali sono le sue proprietà. Vedremo in seguito dei metodi per calcolarlo.

Metodo di Laplace. Iniziamo a vedere come calcolare il determinante per matrici quadrate di ordine 1, 2 e 3.

- se $n = 1$ e $A \in \mathcal{M}_1$ con $A = (a)$ allora $det(A) = a$;
- se $n = 2$ e $A \in \mathcal{M}_2$ con $A = (a_{ij})$ allora

$$det(A) = a_{11} \cdot a_{22} - a_{12} \cdot a_{21} \in \mathbb{R};$$

- se $n = 3$ e $A \in \mathcal{M}_3$ con $A = (a_{ij})$ allora

$$det(A) = a_{11} \cdot det \begin{pmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{pmatrix} - a_{12} \cdot det \begin{pmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{pmatrix} + a_{13} \cdot det \begin{pmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{pmatrix}$$

Esempio 5.3.2. Se $A = \begin{pmatrix} 1 & 1 & 2 \\ 3 & 0 & 1 \\ 0 & 2 & 1 \end{pmatrix} \in \mathcal{M}_3$ allora $det(A) = 1 \cdot det \begin{pmatrix} 0 & 1 \\ 2 & 1 \end{pmatrix} - 1 \cdot det \begin{pmatrix} 3 & 1 \\ 0 & 1 \end{pmatrix} + 2 \cdot det \begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix} = 1 \cdot (0 \cdot 1 - 1 \cdot 2) - 1 \cdot (3 \cdot 1 - 0 \cdot 1) + 2 \cdot (3 \cdot 2 - 0 \cdot 0) = -2 - 3 + 12 = 7$

Definizione 5.3.3. Una **sottomatrice** di una matrice A è una matrice ottenuta cancellando alcune righe e alcune colonne di A.

Esempio 5.3.4.

$$A = \begin{pmatrix} 1 & 1 & 0 & 2 \\ 1 & 3 & 1 & 0 \\ -1 & 0 & 1 & 1 \end{pmatrix} \in \mathcal{M}_{3,4} \qquad B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in \mathcal{M}_{2,2}$$

B è una sottomatrice di A ottenuta cancellando la seconda e la quarta colonna e la terza riga.

Definizione 5.3.5. Se B è una sottomatrice quadrata di ordine n di A, allora il determinante $det(B)$ si chiama un **minore** di A di ordine n.

Definizione 5.3.6. Se $A = (a_{ij}) \in \mathcal{M}_n$, la sottomatrice B_{ij} ottenuta cancellando la riga i-esima e la colonna j-esima è una matrice quadrata di ordine $n-1$. Il determinante di B_{ij} si chiama **minore complementare** di A rispetto ad a_{ij}.

Esempio 5.3.7.

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 3 & 1 \\ -1 & 0 & 1 \end{pmatrix} \in \mathcal{M}_3$$

Se cancello la seconda riga e la terza colonna ottengo una matrice $B_{23} = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} \in \mathcal{M}_2$ il cui determinante (uguale a 1) è il minore complementare di a_{23}.

Definizione 5.3.8 (Complemento Algebrico)**.** Il **complemento algebrico** A_{ij} di a_{ij} nella matrice $A \in \mathcal{M}_n$ è il numero

$$A_{ij} = (-1)^{i+j} \cdot det(B_{ij}),$$

dove $det(B_{ij})$ è il minore complementare di a_{ij}.

Esempio 5.3.9. $A = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 3 & 1 \\ -1 & 0 & 1 \end{pmatrix}$

- $a_{11} = 1 \Rightarrow B_{11} = \begin{pmatrix} 3 & 1 \\ 0 & 1 \end{pmatrix}$

  $A_{11} = (-1)^{1+1} \cdot det \begin{pmatrix} 3 & 1 \\ 0 & 1 \end{pmatrix} = 3$

- $a_{12} = 1 \Rightarrow B_{12} = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$

  $A_{12} = (-1)^{1+2} \cdot det \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} = -1 \cdot 2 = -2$

- $a_{32} = 0 \Rightarrow B_{32} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$

  $A_{32} = (-1)^{3+2} \cdot det \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = -1 \cdot 1 = -1$

Teorema 5.3.10. ***Metodo di Laplace per il calcolo del determinante*** *(o Primo teorema di Laplace). Sia $A \in \mathcal{M}_n$ (matrice A quadrata di ordine n). Per calcolare il determinante di A scegliamo una riga, per esempio la riga i-esima. Si ha:*

$$det(A) = \sum_{j=1}^{n} a_{ij} \cdot A_{ij} = \sum_{j=1}^{n} (-1)^{i+j} \cdot a_{ij} \cdot det(B_{ij}) \tag{5.2}$$

cioè il determinante di A è uguale alla somma dei prodotti degli elementi della riga i-esima per i complementi algebrici.

Il risultato è lo stesso qualsiasi riga venga scelta. Conviene quindi nella pratica scegliere sempre una riga che contenga molti 0. Nota che questo metodo di Laplace, nei casi in cui $n = 1, 2, 3$ coincide con il metodo che abbiamo descritto precedentemente.

Esempio 5.3.11. Calcolare con il metodo di Lapalce il determinante della matrice

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 3 & 1 \\ -1 & 0 & 1 \end{pmatrix}$$

scegliendo la prima riga (quindi $i = 1$ e $n = 3$). $det(A) = (-1)^{1+1} \cdot 1 \cdot det \begin{pmatrix} 3 & 1 \\ 0 & 1 \end{pmatrix} +$ $(-1)^{1+2} \cdot 1 \cdot det \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} + (-1)^{1+3} \cdot 0 \cdot det \begin{pmatrix} 1 & 3 \\ -1 & 0 \end{pmatrix} = 3 + (-1) \cdot 2 + 0 = 1$

Esempio 5.3.12. Calcoliamo il determinante della matrice

$$A = \begin{pmatrix} 1 & 1 & -1 \\ 0 & 2 & 0 \\ 3 & 1 & 2 \end{pmatrix} \qquad n = 3$$

scelgo $i = 1$: $det(A) = (-1)^{1+1} \cdot 1 \cdot det \begin{pmatrix} 2 & 0 \\ 1 & 2 \end{pmatrix} + (-1)^{1+2} \cdot 1 \cdot det \begin{pmatrix} 0 & 0 \\ 3 & 2 \end{pmatrix} + (-1)^{1+3} \cdot$ $(-1) \cdot det \begin{pmatrix} 0 & 2 \\ 3 & 1 \end{pmatrix} = 4 - 0 + 6 = 10$

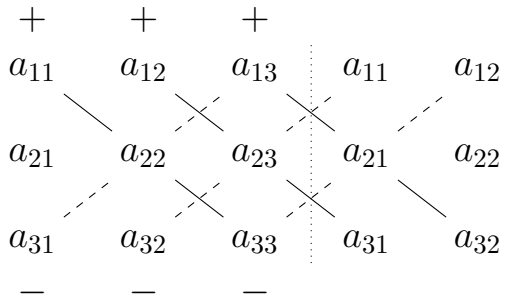
scelgo $i = 2$: $det(A) = (-1)^{2+1} \cdot 0 \cdot det \begin{pmatrix} 1 & -1 \\ 1 & 2 \end{pmatrix} + (-1)^{2+2} \cdot 2 \cdot det \begin{pmatrix} 1 & -1 \\ 3 & 2 \end{pmatrix} +$ $(-1)^{2+3} \cdot 0 \cdot det \begin{pmatrix} 1 & 1 \\ 3 & 1 \end{pmatrix} = 0 + 10 + 0 = 10$

Per le matrici 3×3 possiamo usare un metodo alternativo:

Teorema 5.3.13 (Metodo di Sarrus)**.**

$$\begin{aligned} det(A) &= [(a_{11}\cdot a_{22}\cdot a_{33})+(a_{12}\cdot a_{23}\cdot a_{31})+(a_{13}\cdot a_{21}\cdot a_{32})]- \\ &\quad [(a_{31}\cdot a_{22}\cdot a_{13})+(a_{32}\cdot a_{23}\cdot a_{11})+(a_{33}\cdot a_{21}\cdot a_{12})] \end{aligned}$$

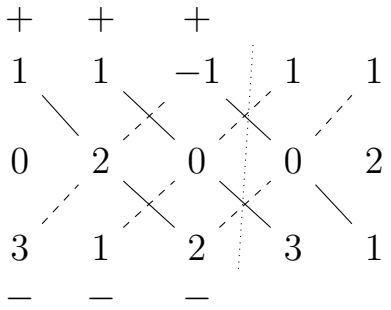
Per ricordare questa formula si può riscrivere la matrice ricopiando la prima e la seconda colonna a destra e poi sommare il prodotto dei numeri sulle tre diagonali e sottrarre il prodotto di quelli sulle tre controdiagonali:



Esempio 5.3.14. Per calcolare con il metodo di Sarrus il determinante della matrice 3×3

$$\begin{pmatrix} 1 & 1 & -1 \\ 0 & 2 & 0 \\ 3 & 1 & 2 \end{pmatrix}$$

si procede nel seguente modo:



$det(A) = (4+0+0)-(-6+0+0) = 10$

Esempio 5.3.15. Per le matrici più grandi non si può usare il metodo di Sarrus. Per esempio per calcolare il determinante di

$$A = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 2 \\ 1 & 0 & 0 & 1 \\ 0 & 2 & 0 & 1 \end{pmatrix} \in \mathcal{M}_4$$

bisogna usare il metodo di Laplace utilizzando per esempio la prima riga $i = 1$.

$$det(A) = 0 + 0 + (-1)^{1+3} \cdot 1 \cdot det \begin{pmatrix} 0 & 1 & 2 \\ 1 & 0 & 1 \\ 0 & 2 & 1 \end{pmatrix} + 0$$

e quindi calcolando il determinante della matrice 3 x 3 con il metodo di Sarrus si ottiene $det(A) = 4 - 1 = 3$.

Proprietà 5.3.16. *Proprietà dei Determinanti.*

- *La regola di Laplace si può applicare scegliendo una colonna invece di una riga: scelgo la colonna j-esima* $det(A) = \sum_{i=1}^{n} (a_{ij} \cdot A_{ij})$
- *Se c'è una riga o una colonna formata da tutti* 0 *allora il determinante è* 0
- *Se* $A = (a_{ij})$ *è* ***triangolare****, cioè se* $a_{ij} = 0$ *per* $j < i$*, allora* $det(A) = \prod_{i=1}^{n} a_{ii}$ *cioè il prodotto degli elementi sulla diagonale*

Esempio 5.3.17. Consideriamo una matrice triangolare:

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} \qquad a_{21} = a_{31} = a_{32} = 0$$

Calcolo il determinante scegliendo la prima colonna:

$$det(A) = (-1)^{1+1} \cdot 1 \cdot det \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = 1 \cdot 1 = 1$$

essendo triangolare si ha quindi $det(A) = 1 \cdot 1 \cdot 1 = 1$ (provare ad applicare i metodi precedenti...).

Enunciamo anche il **Secondo Teorema di Laplace:** in una matrice quadrata $A = (a_{ij}) \in \mathcal{M}_n$, moltiplicando gli elementi di una riga/colonna per i complementi algebrici di un'altra riga/colonna e sommando i prodotti ottenuti si ottiene 0. In formule, per ogni $i \neq k$:

$$\sum_{j=1}^{n} a_{kj} \cdot A_{ij} = \sum_{j=1}^{n} (-1)^{i+j} \cdot a_{kj} \cdot det(B_{ij}) = 0. \tag{5.3}$$

Nota che a differenza della (5.2) in questo caso abbiamo un indice $k \neq i$.

5.4 Rango di una matrice

Ricordiamo che il determinante si può calcolare solo per matrici quadrate. Quando consideriamo una matrice qualsiasi possiamo però calcolare il determinate delle sue sottomatrici quadrate. Questo può servire per calcolare il cosiddetto *rango* di una matrice, che come vedremo in seguito ha anche un significato geometrico sulla dipendenza lineare delle righe della matrice.

Definizione 5.4.1. Il **rango** di una matrice $A \in \mathcal{M}_{m,n}$ è il massimo ordine di un minore non nullo di A e si denota con $rg(A)$. In altre parole il rango è l'ordine della più grande sottomatrice quadrata di A che ha un determinante diverso da 0.

Nota che valgono le seguenti proprietà:

- il rango di una matrice è sempre un numero intero;
- se $A \in \mathcal{M}_{m,n}$ allora $rg(A) \leq \min(m, n)$. Infatti A non può contenere una sottomatrice quadrata che abbia un ordine più grande del minimo tra m e n;
- $rg(A) = 0$ se e solo se A è la matrice nulla, composta da soli 0;
- se A è una matrice quadrata ($A \in \mathcal{M}_n$) e $det(A) \neq 0$ allora $rg(A) = n$.

Esempio 5.4.2.

$$A = \begin{pmatrix} 2 & 1 & 3 \\ 1 & 0 & 1 \end{pmatrix} \in \mathcal{M}_{2,3}$$

$rg(A) \leq 2$ perché le sottomatrici quadrate di A sono al massimo del tipo 2×2. Consideriamo la sottomatrice quadrata $\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}$ ottenuta cancellando la terza colonna. Questa sottomatrice ha determinante uguale a -1 che è quindi diverso da 0. Dato che non ci sono sottomatrici 3×3 allora il rango di A è proprio 2.

Esempio 5.4.3. Consideriamo la matrice

$$A = \begin{pmatrix} 2 & 1 & 3 \\ 4 & 2 & 6 \end{pmatrix}$$

e tutte le sue sottomatrici 2×2:

$$\begin{pmatrix} 2 & 1 \\ 4 & 2 \end{pmatrix} \qquad \begin{pmatrix} 1 & 3 \\ 2 & 6 \end{pmatrix} \qquad \begin{pmatrix} 2 & 3 \\ 4 & 6 \end{pmatrix}$$

Tutte le sottomatrici 2×2 hanno determinante uguale a 0 quindi $rg(A) < 2$, ma anche $rg(A) > 0$ perché A non è composta da tutti 0. Quindi è $rg(A) = 1$ perché per esempio (2) è una sottomatrice 1×1 di A che ha determinante uguale a $1 \neq 0$.

Definizione 5.4.4. Sia B una sottomatrice quadrata $k \times k$ di $A \in \mathcal{M}_{mn}$. Una **matrice che orla** B è una sottomatrice di ordine $k+1$ di A ottenuta aggiungendo a B gli elementi di una riga e una colonna di A. Nota che una sottomatrice può avere più di una matrice che la orla.

Esempio 5.4.5. Consideriamo la matrice $A = \begin{pmatrix} 2 & 1 & 1 & 0 \\ 3 & 2 & 1 & 0 \\ 0 & 1 & 0 & 2 \end{pmatrix}$ e la sottomatrice $B = \begin{pmatrix} 2 & 1 \\ 3 & 2 \end{pmatrix}$ ottenuta cancellando terza e quarta colonna e terza riga. La matrice B si può *orlare* con una matrice 3×3 in due modi, cioè aggiungendo la terza riga e la terza colonna o aggiungendo la terza riga e la quarta colonna:

$$\begin{pmatrix} 2 & 1 & 1 \\ 3 & 2 & 1 \\ 0 & 1 & 0 \end{pmatrix} \qquad \begin{pmatrix} 2 & 1 & 0 \\ 3 & 2 & 0 \\ 0 & 1 & 2 \end{pmatrix}$$

Teorema 5.4.6. *Sia M una sottomatrice quadrata di ordine p di A con determinante diverso da 0. Se tutti i determinanti delle matrici che orlano M sono uguali a 0, allora $rg(A) = p$.*

Vediamo adesso un procedimento per calcolare il rango usando le matrici orlate.

Teorema 5.4.7 (Metodo di Kronecker)**.** *Sia $A = (a_{ij}) \in \mathcal{M}_{m,n}$, per calcolare il rango di A si può procedere come segue:*

- *se tutti gli elementi di A sono 0 allora $rg(A) = 0$*
- *altrimenti, sia $a_{ij} \neq 0$ e consideriamo la matrice $A_1 = (a_{ij})$ che ha determinante diverso da zero (perché è uguale a a_{ij}). Se non esistono matrici 2×2 che contengono a_{ij} e che abbiano $det \neq 0$ allora $rg(A) = 1$;*
- *altrimenti, sia A_2 una sottomatrice 2×2 di A che contiene a_{ij} e tale che $det(A_2) \neq 0$. Se non esiste sottomatrice 3×3 di A che abbia A_2 come sottomatrice e che abbia $det \neq 0$, allora $rg(A) = 2$;*
- *altrimenti sia A_3 la sottomatrice 3×3 di A del punto precedente. Cerco una sottomatrice 4×4 di A che contenga A_3 come sottomatrice e che abbia determinante diverso da 0 e così via, fino ad arrivare eventualmente a $min(n, m)$.*

Il metodo di Kronecker si chiama anche **metodo degli orlati**. Ci permette di calcolare il rango restringendo la ricerca alle sottomatrici quadrate che orlano una sottomatrice che ha determinante diverso da zero. Quindi per calcolare il rango non dobbiamo andare a calcolare tutti i determinanti di tutte le sottomatrici quadrate.

Esempio 5.4.8. Consideriamo la matrice

$$A = \begin{pmatrix} 2 & 1 & 0 \\ 3 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \in \mathcal{M}_3$$

- $rg(A)$ non può essere 0 perché non tutti gli elementi di A sono 0;
- scelgo $a_{11} = 2 \neq 0$ quindi $rg(A) \geq 1$;
- la matrice $A_2 = \begin{pmatrix} 2 & 1 \\ 3 & 1 \end{pmatrix} \in \mathcal{M}_2$ orla (a_{11}) e $det(A_2) = -1 \neq 0$ quindi $rg(A) \geq 2$;
- la matrice $A_3 = \begin{pmatrix} 2 & 1 & 0 \\ 3 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \in \mathcal{M}_3$ orla A_2 e ha $det(A_3) = 2 - 2 = 0$. Dato che non ci sono altre matrici 3×3 che contengono A_2 con $det \neq 0$ allora $rg(A) = 2$.

Esempio 5.4.9. Consideriamo la matrice $A = \begin{pmatrix} 2 & 1 & 1 & 0 \\ 4 & 2 & 2 & 0 \end{pmatrix}$.

- $rg(A)$ non può essere 0 perché non tutti gli elementi di A sono 0;
- scelgo $A_1 = (a_{11}) = (2)$ con $det(A_1) = 2$ quindi $rg(A) \geq 1$;
- ci sono 3 matrici che orlano A_1 (ma due di loro sono uguali) che sono

$$\begin{pmatrix} 2 & 1 \\ 4 & 2 \end{pmatrix} \qquad \begin{pmatrix} 2 & 1 \\ 4 & 2 \end{pmatrix} \qquad \begin{pmatrix} 2 & 0 \\ 4 & 0 \end{pmatrix}$$

  e hanno tutte quante il determinante uguale a 0. Quindi tutte le matrici che orlano A_1 hanno determinante uguale a 0 e il rango della matrice A è uguale a 1. Nota che non c'è bisogno di calcolare il determinante delle altre sottomatrici quadrate di ordine 2 di A.

Esempio 5.4.10. Calcolare $rg(A)$ con il metodo di Kronecker

$$A = \begin{pmatrix} 2 & 1 & 0 & 1 \\ 3 & 1 & 1 & 2 \\ 1 & 0 & 1 & 1 \end{pmatrix}$$

- $rg(A) > 0$ perché non tutti gli elementi di A sono 0
- $a_{11} = 2$ quindi $det(a_{11}) = 2$ e $rg(A) \geq 1$

- $A_2 = \begin{pmatrix} 2 & 1 \\ 3 & 1 \end{pmatrix} \Rightarrow det(A_2) = -1 \Rightarrow rg(A) \geq 2$
- $A_3 = \begin{pmatrix} 2 & 1 & 0 \\ 3 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \Rightarrow$ calcolo il $det(A_3)$ con il metodo di Sarrus : $det(A_3) = [(2 \cdot 1 \cdot 1) + (1 \cdot 1 \cdot 1) + (0 \cdot 3 \cdot 0)] - [(1 \cdot 1 \cdot 0) + (0 \cdot 1 \cdot 2) + (1 \cdot 3 \cdot 1)] = 3 + 3 = 6 \Rightarrow rg(A_3) \geq 3$
- dato che non ci sono sottomatrici 4×4 di A allora il procedimento termina e $rg(A) = 3$.

5.4.1 Vettori linearmente indipendenti

Anticipiamo in questa sezione un argomento che poi approfondiremo anche da un punto di vista geometrico. Consideriamo dei vettori, cioè delle matrici che hanno una sola riga. Un vettore di n elementi possiamo anche considerarlo come un elemento del prodotto cartesiano di $\mathbb{R}$ per se stesso n volte:

$$\mathbb{R}^n = \underbrace{\mathbb{R} \times \cdots \times \mathbb{R}}_{n \text{ volte}} = \{(a_1, \ldots, a_n) \mid a_i \in \mathbb{R}\},$$

cioè $\mathbb{R}^n = \mathcal{M}_{1,n}$.

Definizione 5.4.11. Se $u = (a_1, a_2, a_3, \ldots, a_n), v = (b_1, b_2, b_3, \ldots, b_n) \in \mathbb{R}^n$ definiamo le seguenti operazioni:

- Somma: $u+v = (a_1+b_1, a_2+b_2, \ldots, a_n+b_n)$. Per esempio se $u = (1, 2, 3) \in \mathbb{R}^3$ e $v = (0, -1, 2) \in \mathbb{R}^3$ allora $u + v = (1, 1, 5) \in \mathbb{R}^3$.
- Prodotto esterno tra un numero (scalare) e un vettore: $r \in \mathbb{R}$, $u \in \mathbb{R}^n$, $u = (a_1, a_2, \ldots, a_n)$, $r \cdot u = (r \cdot a, r \cdot a_2, \ldots, r \cdot a_n)$. Per esempio se $u = (1, 2, 3)$ e $r = 2$ allora $ru = 2u = (2, 4, 6)$.

Il vettore **nullo** è un vettore che ha tutte le componenti uguali a 0. Nel seguito consideriamo sempre vettori con n componenti, cioè vettori appartenenti a $\mathbb{R}^n$.

Definizione 5.4.12. Una **combinazione lineare** di m vettori $v_1, v_2, \ldots, v_m \in \mathbb{R}^n$ tramite gli scalari $r_1, r_2, \ldots, r_m \in \mathbb{R}$, è il vettore

$$r_1 \cdot v_1 + r_2 \cdot v_2 + \cdots + r_m \cdot v_m \in \mathbb{R}^n.$$

Esempio 5.4.13. Con $m = 4$ e $n = 3$, se $u_1 = (2, 1, 0, 3)$, $u_2 = (1, -1, 1, -1)$ e $u_3 = (0, 0, 1, 0)$, e considerando gli scalari $r_1 = 2$, $r_2 = -1$, $r_3 = 1$ si ha la

combinazione lineare

$$r_1 \cdot u_1 + r_2 \cdot u_2 + r_3 \cdot u_3 =$$
$$2 \cdot (2,1,0,3) + (-1) \cdot (1,-1,1,-1) + 1 \cdot (0,0,1,0) =$$
$$(4,2,0,6) - (1,-1,1,-1) + (0,0,1,0) = (3,3,0,7).$$

Definizione 5.4.14. Un vettore è **linearmente dipendente** dai vettori $u_1, \ldots, u_m$ se esistono $r_1, \ldots, r_m$ tali che $u = r_1 \cdot u_1 + \cdots + r_m \cdot u_m$; cioè se u è combinazione lineare di $u_1, \ldots, u_m$.

Nota che nella definizione di dipendenza lineare si chiede che ESISTANO degli scalari in modo che ci sia una combinazione lineare. Quindi possiamo affermare che un vettore NON è linearmente dipendente da altri se non esistono degli scalari che permettano di scrivere la combinazione lineare.

Esempio 5.4.15. Con $n = 1$, se $u = (2,1)$, $u_1 = (1,0)$, $u_2 = (0,1)$ allora u è combinazione lineare di u_1 e u_2 perché $(2,1) = 2(1,0) + 1(0,1)$.

$(3,0)$ è combinazione lineare di u_1 e u_2? Sì, perché $(3,0) = 3 \cdot (1,0) + 0 \cdot (0,1)$. In particolare possiamo anche dire che u è combinazione lineare di u_1 dato che $u = 3 \cdot u_1$.

Analogamente possiamo dire che $(0,4)$ dipende linearmente da $(0,1)$. Invece $(2,1)$ non è combinazione lineare di $(1,0)$ e $(-1,0)$. Infatti se esistessero $r_1, r_2 \in \mathbb{R}$ tale che $(2,1) = r_1(1,0) + r_2(-1,0) = (r_1 - r_2, 0)$ dovrebbe essere $r_1 - r_2 = 1$ e $1 = 0$ che è chiaramente impossibile.

Una combinazione lineare di un solo vettore v è un vettore $r \cdot v$ di v (con $r \in \mathbb{R}$), cioè $r \cdot v$ è una combinazione lineare di v.

Definizione 5.4.16. Un insieme di vettori è **linearmente indipendente** quando nessuno di loro è combinazione lineare degli altri. Per dirla in maniera più precisa, un insieme di vettori $\{v_1, \ldots, v_m\}$ è linearmente indipendente se l'unico modo di ottenere il vettore nullo come combinazione lineare di $v_1, \ldots, v_m$ è quello di prendere tutti gli scalari uguali a zero:

$$r_1 v_1 + \cdots + r_n v_m = (0, \ldots, 0) \qquad \Rightarrow \qquad r_1 = \cdots = r_m = 0.$$

Esempio 5.4.17. $\{(0,1),(1,0)\}$ è linearmente indipendente perché se

$$(0,0) = r_1(0,1) + r_2(1,0)$$

allora si ha $(0,0) = (r_1, r2)$ e quindi $r_1 = 0$ e $r_2 = 0$, cioè l'unico modo di ottenere $(0,0)$ come combinazione lineare di $(0,1)$ e $(1,0)$ è quello di scegliere scalari uguali a 0. Questa è la stessa cosa di dire che non posso scrivere $(0,1)$ come combinazione lineare di $(1,0)$ perché dovrebbe essere

$$(0,1) = r(1,0)$$

e quindi $0 = r$ e $1 = 0$ che è impossibile.

Esempio 5.4.18. L'insieme $\{(2,1),(0,1),(1,0)\}$ non è linearmente indipendente perché $(2,1) = (0,1) + 2(1,0)$. Infatti posso scrivere

$$(0,0) = -1 \cdot (1,2) + (0,1) + 2 \cdot (1,0).$$

Esempio 5.4.19. I vettori $(1,0)$ e $(2,0)$ sono linearmente indipendenti? Posso scrivere il vettore nullo come combinazione lineare di $(1,0)$, $(2,0)$ usando scalari $\neq$ da 0

$$2 \cdot (1,0) - (2,0) = (2,0) - (2,0) = (0,0)$$

quindi $(1,0)$ e $(2,0)$ non sono indipendenti.

In una matrice $m \times n$ possiamo vedere le m righe come vettori con n componenti. Il rango di una matrice è collegato alla indipendenza lineare di tali vettori, come enunciato nella prossima proprietà:

Proprietà 5.4.20. *Il rango di una matrice è il numero di righe che sono vettori linearmente indipendenti. In particolare se $rg(A) = r$ allora in A ci sarà una matrice $r \times r$ con determinante diverso da 0 e le r righe di A corrispondenti a tale matrice saranno linearmente indipendenti.*

Per esempio la matrice

$$A = \begin{pmatrix} 2 & 1 & 3 \\ 4 & 2 & 6 \end{pmatrix}$$

ha rango 1 perché la seconda riga $(4,2,6)$ è una combinazione lineare della prima $(2,1,3)$ (vale anche il viceversa) e quindi c'è solo una riga indipendente. La matrice

$$A = \begin{pmatrix} 2 & 1 & 3 \\ 0 & 2 & 1 \\ 2 & 5 & 5 \end{pmatrix}$$

ha rango 2 perché $(2,5,5) = (2,1,3) + 2(0,2,1)$ quindi la terza riga dipende dalle prime due, mentre le prima due sono indipendenti tra di loro.

Il metodo di Kronecker (che utilizza i determinanti) è un metodo per capire se le righe di una matrice sono indipendenti tra di loro. Nel prossimo paragrafo vedremo un metodo che non utilizza il calcolo dei determinanti.

Proprietà 5.4.21. *Se $A \in \mathcal{M}_n$ e $det(A) = 0$ allora gli n vettori riga della matrice non sono linearmente indipendenti. Infatti in questo caso il rango della matrice sarà minore di n e quindi ci saranno meno di n vettori che sono linearmente indipendenti.*

Esempio 5.4.22. *$det \begin{pmatrix} 1 & 0 \\ 2 & 0 \end{pmatrix} = 0$* e infatti la riga $(2,0)$ è un multiplo di $(1,0)$.

$det\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} = 1 \neq 0$ e $(1,0)$ e $(0,1)$ sono linearmente indipendenti.

$det\begin{pmatrix}1 & 2\\ 2 & 4\end{pmatrix} = 0$ e $(1,2)$ e $(2,4)$ sono linearmente dipendenti $((2,4) = 2\cdot(1,2))$.

$det\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 1 & 1 & 0\end{pmatrix} = 0$ e $(1,1,0) = (1,0,0)+(0,1,0)$ quindi $(1,1,0)$ è combinazione lineare di $(1,0,0)$ e $(0,1,0)$

Esempio 5.4.23.

$$det\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 2\\ 1 & 1 & 0\end{pmatrix} = \begin{vmatrix}2 & 3\\ 1 & 2\end{vmatrix} - \begin{vmatrix}1 & 3\\ 2 & 2\end{vmatrix} = 1 + 4 = 5 \neq 0$$

perciò i vettori $(1,2,3)$, $(2,1,2)$ e $(1,1,0)$ sono linearmente indipendenti

Esempio 5.4.24. Calcoliamo il rango della matrice

$$A = \begin{pmatrix}1 & 2 & 0\\ 0 & 1 & 2\\ 1 & 3 & 2\end{pmatrix}$$

e troviamo le righe linearmente indipendenti. Per calcolare il rango di A procediamo con il metodi degli orlati:

- il rango è maggiore di 0;
- scelgo $(1) \Rightarrow det(1) \neq 0$ quindi $rg(A) \geq 1$;
- scelgo $A_2 = \begin{pmatrix}1 & 2\\ 0 & 1\end{pmatrix} \Rightarrow \begin{vmatrix}1 & 2\\ 0 & 1\end{vmatrix} = 1 \neq 0$ quindi $rg(A) \geq 2$;
- scelgo $\begin{pmatrix}1 & 2 & 0\\ 0 & 1 & 2\\ 1 & 3 & 2\end{pmatrix} \Rightarrow \begin{vmatrix}1 & 2 & 0\\ 0 & 1 & 2\\ 1 & 3 & 2\end{vmatrix} = \begin{vmatrix}1 & 2\\ 3 & 2\end{vmatrix} - 2\begin{vmatrix}0 & 2\\ 1 & 2\end{vmatrix} = 4 - 4 = 0$ quindi $rg(A) = 2$ (perché non ci sono altre matrici 3×3).

Dato che $rg(A) = 2$ in A ci sono 2 righe linearmente indipendenti. I vettori $(1,2,0)$ e $(0,1,2)$ che formano A_2 sono indipendenti, inoltre si ha $(1,3,2) = (1,2,0) + (0,1,2)$ e quindi la terza riga dipende dalle prime due.

5.4.2 Riduzione a scala

Definizione 5.4.25. Un elemento $\neq 0$ di una matrice si dice **speciale** se al di sotto di esso ci sono solo 0, cioè a_{ij} è speciale se $a_{kj} = 0$ per ogni $k > i$. Nota che gli elementi dell'ultima riga di una matrice sono tutti speciali (possiamo prenderla come definizione, anche se in realtà è un caso particolare del "per ogni").

Definizione 5.4.26. Una matrice è **ridotta per righe** se in ogni riga c'è un elemento speciale.

Esempio 5.4.27. La matrice

$$A = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 3 & 1 \\ 0 & 2 & 0 \end{pmatrix}$$

è ridotta per righe, perché

- nella prima riga 1 è elemento speciale
- nella seconda riga 1 è elemento speciale
- nella terza riga 2 è elemento speciale.

Il vettore $(1, 0, 2)$ non può essere combinazione lineare di $(0, 3, 1)$ e $(0, 2, 0)$ perché la prima componente 1 non si può scrivere come combinazione lineare delle prime componenti degli altri due. Anche $(0, 3, 1)$ e $(0, 2, 0)$ sono linearmente indipendenti. Perciò $rg(A) = 3$.

Proprietà 5.4.28. *Se una matrice $A \in \mathcal{M}_{mn}$ è ridotta per righe, allora il rango di A è uguale al numero di righe non nulle.*

Esempio 5.4.29.

$$A_1 = \begin{pmatrix} 1 & 0 \\ 0 & 2 \\ 0 & 0 \end{pmatrix} \qquad rg(A_1) = 2$$

$$A_2 = \begin{pmatrix} 2 & 1 & 3 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix} \qquad rg(A_2) = 2$$

$$A_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 1 & 2 & 3 \\ 0 & 1 & 2 & 0 \end{pmatrix} \qquad rg(A_3) = 3$$

Definizione 5.4.30. Chiamiamo **pivot** il primo elemento diverso da zero in una riga di una matrice. Una matrice $A \in \mathcal{M}_{mn}$ è in **forma a scala (o a gradini)** se il pivot di ogni riga è più a destra del pivot della riga precedente. In particolare una matrice ridotta a scala è anche ridotta per righe, in più gli elementi uguali a zero si trovano tutti nel triangolo inferiore della matrice (non è invece vero che una matrice ridotta per righe deve essere necessariamente ridotta a scala...).

Esempio 5.4.31. Le seguenti matrici sono in forma a scala, quindi sono anche ridotte per righe e possiamo calcolare il loro rango:

$$A_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad rg(A_4) = 3$$

$$A_5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 0 & 0 & 3 & 1 & 2 \\ 0 & 0 & 0 & 3 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \qquad rg(A_5) = 4$$

Nell'esempio precedente, la matrice A_3 non è a scala, ma è ridotta per righe.

Dato che è facile calcolare il rango di una matrice a scala, andremo adesso a vedere un metodo che permette di trasformare una matrice qualsiasi in matrice a scala conservando il valore del rango. Per fare ciò utilizziamo delle trasformazioni sulle matrici che chiamiamo **operazioni elementari**. Possiamo trasformare una matrice $A = (a_{ij})$ che ha n righe $r_1, \ldots, r_n$ con le seguenti operazioni:

- $r_i \leftrightarrow r_j$ Scambiare due righe : otteniamo una matrice scambiando la riga i-esima con la riga j-esima.
- $r_i \to c \cdot r_i$ Moltiplicare una riga per un numero $c \neq 0$: otteniamo una matrice moltiplicando tutti gli elementi della riga i-esima per il numero c.
- $r_i \to r_i + cr_j$ Sommare ad una riga un'altra riga moltiplicata per un numero c: otteniamo una matrice in cui per ogni k, al posto del k-esimo elemento a_{ik} della riga i-esima andiamo a scrivere l'elemento $a_{ik} + ca_{jk}$.

Si noti che queste tre operazioni permettono di fare delle combinazioni lineari o di scambiare di posto le righe, e agiscono SEMPRE su tutti gli elementi di una riga.

Esempio 5.4.32. Consideriamo la matrice $A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & 0 \end{pmatrix}$ con le righe $r_1 = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$ e $r_2 = \begin{pmatrix} 2 & 4 & 0 \end{pmatrix}$.

$$A \quad r_1 \leftrightarrow r_2 \begin{pmatrix} 2 & 4 & 0 \\ 1 & 2 & 3 \end{pmatrix} \quad r_1 \to r_1 + 2r_2 \begin{pmatrix} 4 & 8 & 6 \\ 1 & 2 & 3 \end{pmatrix}$$

Proprietà 5.4.33. *Il rango di una matrice non cambia quando vengono effettuate le operazioni elementari. Cioè, se A_1 si ottiene da A tramite un numero qualsiasi di operazioni elementari, allora $rg(A) = rg(A_1)$.*

Possiamo quindi applicare le operazioni elementari per cercare di ridurre una matrice a scala, dato che di quest'ultima sappiamo facilmente calcolare il rango. Per fare ciò dobbiamo fare in modo che il pivot di ogni riga abbia al di sotto tutti 0.

Esempio 5.4.34. Applicare le operazioni elementari per trasformare la seguente matrice in forma a scala.

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 4 & -1 \end{pmatrix}$$

Cerchiamo con le operazioni elementari di ottenere uno 0 al di sotto del pivot 1 della prima riga.

$$r_2 \to r_2 - 2r_1 \begin{pmatrix} 1 & 2 & 3 \\ 0 & 0 & -7 \end{pmatrix}.$$

La matrice è in forma ridotta e ha due righe diverse da 0 quindi $rg = 2$. Consideriamo la seguente matrice 3×3

$$\begin{pmatrix} 2 & 3 & 4 \\ 1 & 0 & 3 \\ 3 & 3 & 7 \end{pmatrix}$$

Per avere degli 0 sotto il pivot 2 della prima riga facciamo le seguenti operazioni

$$r_2 \to r_2 - \frac{r_1}{2} \qquad \begin{pmatrix} 2 & 3 & 4 \\ 0 & -3/2 & 1 \\ 3 & 3 & 7 \end{pmatrix}$$

$$r_3 \to r_3 - \frac{3}{2} r_1 \begin{pmatrix} 2 & 3 & 4 \\ 0 & -3/2 & 1 \\ 0 & -3/2 & 1 \end{pmatrix}$$

Adesso, per avere uno 0 sotto il pivot $-3/2$ della seconda riga possiamo procedere così:

$$r_3 \to r_3 - r_2 \begin{pmatrix} 2 & 3 & 4 \\ 0 & -3/2 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

La matrice è in forma a scala con una riga nulla quindi $rg = 2$ e cioè le tre righe della matrice iniziale non sono linearmente indipendenti.

Consideriamo un altro esempio, svolto in maniera più veloce:

$$\begin{pmatrix} 2 & 3 & 4 \\ 1 & 0 & 3 \\ 3 & 3 & 7 \end{pmatrix} \quad r_3 \to r_3 - r_1 \quad \begin{pmatrix} 2 & 3 & 4 \\ 1 & 0 & 3 \\ 1 & 0 & 3 \end{pmatrix} \quad r_3 \Rightarrow r_3 - r_2 \quad \begin{pmatrix} 2 & 3 & 4 \\ 1 & 0 & 3 \\ 0 & 0 & 0 \end{pmatrix}$$

la matrice è in forma ridotta per righe con due righe non nulle, quindi $rg = 2$ e solo due righe della matrice di partenza sono indipendenti.

Vediamo ora il metodo nella sua forma più generale.

Teorema 5.4.35. *Metodo di riduzione a scala di Gauss. Consideriamo una matrice*

$$A = (a_{ij}) = \begin{pmatrix} r_1 \\ \vdots \\ r_i \\ \vdots \\ r_n \end{pmatrix} \in \mathcal{M}_{nm}$$

- *se $a_{11} \neq 0$ allora per ogni k con $2 \leq k \leq n$ (cioè per ogni riga dalla seconda in poi) eseguiamo le operazioni elementari:*

$$r_k \to r_k - \frac{a_{k1}}{a_{11}} \cdot r_1$$

  in modo da mettere 0 sotto il primo elemento. Se invece $a_{11} = 0$ si cerca una riga che abbia primo elemento diverso da 0 e si scambia con la prima riga, poi si applica questo punto. Se non si trova tale riga vuol dire che la prima colonna è formata solo da 0: in questo caso il rango della matrice è uguale al rango della sua sottomatrice ottenuta cancellando la prima colonna, e si può quindi applicare a questa sottomatrice il procedimento descritto.

- *se $a_{22} \neq 0$, per ogni $3 \leq k \leq n$ (cioè dalla terza riga in poi) eseguiamo le operazioni elementari:*

$$r_k \to r_k - \frac{a_{k2}}{a_{22}} \cdot r_2$$

  in modo che gli 0 precedenti non verranno modificati e sotto a_{22} compariranno solo 0. Se invece $a_{22} = 0$ si cerca una riga dalla terza in poi che abbia secondo elemento diverso da 0 e la si scambia con la seconda e poi si applica questo punto.

- *si ripete il procedimento per ogni $a_{ii} \neq 0$ fino a $a_{(n-1)(n-1)}$.*

Se durante il procedimento c'è qualche elemento a_{ii} che è uguale a zero, allora si fa uno scambio di righe e si sostituisce la riga i-esima con una riga che contiene il pivot nella colonna i.

Esempio 5.4.36.

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 1 & 2 & 1 \\ 0 & 1 & 3 & 4 \\ -1 & 0 & 1 & 2 \end{pmatrix}$$

$a_{11} = 1 \neq 0$

$r_2 \to r_2 - \frac{a_{21}}{a_{11}} \cdot r_1 = r_2 \to r_2 - r_1$

$r_3 \to r_3 - \frac{a_{31}}{a_{11}} \cdot r_1 = r_3 \to r_3$

$r_4 \to r_4 - \frac{a_{41}}{a_{11}} \cdot r_1 = r_4 \to r_4 + r_1$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & -1 & -1 & -3 \\ 0 & 1 & 3 & 4 \\ 0 & 2 & 4 & 6 \end{pmatrix}$$

$a_{22} = -1 \neq 0$

$r_3 \to r_3 - \dfrac{a_{32}}{a_{22}} \cdot r_2 = r_3 \to r_3 + r_2$

$r_4 \to r_4 - \dfrac{a_{42}}{a_{22}} \cdot r_2 = r_4 \to r_4 + 2r_2$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & -1 & -1 & -3 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 2 & 0 \end{pmatrix}$$

$a_{33} = 2 \neq 0$

$r_4 \to r_4 - \dfrac{a_{43}}{a_{33}} \cdot r_3 = r_4 \to r_4 - r_3$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & -1 & -1 & -3 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

la matrice è ridotta in forma scala con quattro righe non nulle, quindi $rg = 4$.

Determinante con il metodo di Gauss

Il metodo di riduzione a scala di Gauss può essere utilizzato anche per calcolare il determinante di una matrice quadrata. Infatti, se $A \in \mathcal{M}_n$ allora possiamo ridurre A in forma a scala con il metodo visto in precedenza. Se nella riduzione a scala c'è una riga composta solo da 0 allora sarà $det(A) = 0$. Altrimenti ricordiamo dalla definizione di determinante che se una matrice A' si ottiene da

A scambiando due righe tra di loro, allora $det(A) = -det(A')$, mentre se A' si ottiene da A moltiplicando una riga per un numero k allora $det(A) = k \cdot det(A)$. Invece l'operazione che permette di aggiungere ad una riga un'altra moltiplicata per un numero c, non modifica il valore del determinante. Quindi quando si trasforma la matrice A in una matrice A'' a scala, ricordando quanti scambi di righe si sono effettuati e se si è moltiplicata una riga per una costante, si avrà $det(A) = \pm k \cdot det(A'')$. Però essendo A'' una matrice a scala, il determinante di A'' è semplicemente il prodotto degli elementi sulla diagonale, e quindi è facilmente calcolabile.

Esempio 5.4.37. La matrice 4×4 dell'esempio precedente ha determinante uguale a 2 perché nella trasformazione a scala non sono stati effettuati scambi di righe e moltiplicazioni di righe per uno scalare e la forma a scala è:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & -1 & -1 & -3 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

quindi il prodotto degli elementi sulla diagonale è 2. (Provare con il metodo di Laplace).

5.5 Matrice inversa

Definizione 5.5.1 (Matrice Inversa)**.** Data $A \in \mathcal{M}_n$ non singolare (determinante non nullo), la **matrice inversa** A^{-1} di A è una matrice in $\mathcal{M}_n$ tale che $A \cdot A^{-1} = I_n$.

Presentiamo due modi per il calcolo dell'inversa, uno che si basa sui determinanti e un altro sulla riduzione a scala.

Primo Modo: Sia $A = (a_{ij}) \in \mathcal{M}_n$ con $det(A) \neq 0$. Allora

$$A^{-1} = \frac{(A_{ji})}{det(A)}$$

dove indichiamo con A_{ij} il complemento algebrico in A (note che nella formula dell'inversa dobbiamo prendere la trasposta (A_{ji}).

Dimostrazione 5.5.2. Per dimostrare che la formula ottenuta è vera, consideriamo per semplicità il caso $n = 3$ e ricordiamo il metodo di Laplace per il calcolo del determinante e il secondo teorema di Laplace (vedi Equazioni (5.2) e (5.3)):

$$det(A) = \sum_{j=1}^{3} a_{ij} A_{ij} \qquad 0 = \sum_{j=1}^{3} a_{kj} A_{ij}$$

per ogni $i = 1, 2, 3$ e $k \neq i$. Consideriamo allora la matrice che ha i complementi algebrici A_{ij} come elementi e calcoliamo il prodotto righe per colonne

$$(A_{ji}) \cdot A = \begin{pmatrix} A_{11} & A_{21} & A_{31} \\ A_{12} & A_{22} & A_{32} \\ A_{13} & A_{23} & A_{33} \end{pmatrix} \cdot \begin{pmatrix} a_{11} & a_{21} & a_{31} \\ a_{12} & a_{22} & a_{32} \\ a_{13} & a_{23} & a_{33} \end{pmatrix} =$$

si ottiene una matrice che ha il valore 0 quando moltiplico una riga i-esima con una colonna k-esima con $i \neq k$ e invece ha il valore $det(A)$ per $i = k$:

$$= \begin{pmatrix} \sum_{j=1}^{3} a_{1j}A_{j1} & \sum_{j=1}^{3} a_{2j}A_{j1} & \sum_{j=1}^{3} a_{3j}A_{j1} \\ \sum_{j=1}^{3} a_{1j}A_{j2} & \sum_{j=1}^{3} a_{2j}A_{j2} & \sum_{j=1}^{3} a_{3j}A_{j2} \\ \sum_{j=1}^{3} a_{1j}A_{j3} & \sum_{j=1}^{3} a_{2j}A_{j3} & \sum_{j=1}^{3} a_{3j}A_{j3} \end{pmatrix} =$$

$$= \begin{pmatrix} det(A) & 0 & 0 \\ 0 & det(A) & 0 \\ 0 & 0 & det(A) \end{pmatrix} = det(A) \cdot I_n$$

quindi $(A_{ji}) \cdot A = det(A) \cdot I_n$ da cui possiamo ricavare la formula

$$\frac{(A_{ji}) \cdot A}{det(A)} = I_n \quad \text{e quindi} \qquad A^{-1} = \frac{(A_{ji})}{det(A)}.$$

Esempio 5.5.3.

$$A = \begin{pmatrix} 2 & 3 \\ 0 & 1 \end{pmatrix} \qquad det(A) = 2 \neq 0$$

$B_{11} = (1)$ $\quad A_{11} = (-1)^2 \cdot det(A) = 1$
$B_{12} = (0)$ $\quad A_{12} = (-1)^3 \cdot det(0) = 0$
$B_{21} = (3)$ $\quad A_{21} = (-1)^3 \cdot det(3) = -3$
$B_{22} = (2)$ $\quad A_{22} = (-1)^4 \cdot det(2) = 2$

$$A^{-1} = \frac{(A_{ji})}{2} = \frac{1}{2}\begin{pmatrix} 1 & -3 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 1/2 & -3/2 \\ 0 & 1 \end{pmatrix}.$$

Possiamo verificare che A^{-1} sia realmente l'inversa di A:

$$\begin{pmatrix} 2 & 3 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1/2 & -3/2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$$

$$\begin{pmatrix} 1/2 & -3/2 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 2 & 3 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$$

Esempio 5.5.4.

$$A = \begin{pmatrix} 0 & 1 & 2 \\ 0 & 0 & 1 \\ 1 & 1 & 3 \end{pmatrix}$$

Calcoliamo il determinante $det(A) = 1(-1)^2 \begin{vmatrix} 1 & 2 \\ 0 & 1 \end{vmatrix} = 1 \neq 0$, quindi la matrice è invertibile. Calcoliamo i complementi algebrici:

$$A_{11} = (-1)^2 \begin{vmatrix} 0 & 1 \\ 1 & 3 \end{vmatrix} = -1 \quad A_{12} = (-1)^3 \begin{vmatrix} 0 & 1 \\ 1 & 3 \end{vmatrix} = 1$$
$$A_{13} = (-1)^4 \begin{vmatrix} 0 & 0 \\ 1 & 1 \end{vmatrix} = 0 \quad A_{21} = (-1)^3 \begin{vmatrix} 1 & 2 \\ 1 & 3 \end{vmatrix} = -1$$
$$A_{22} = (-1)^4 \begin{vmatrix} 0 & 2 \\ 1 & 3 \end{vmatrix} = -2 \quad A_{23} = (-1)^5 \begin{vmatrix} 0 & 1 \\ 1 & 1 \end{vmatrix} = 1$$
$$A_{31} = (-1)^4 \begin{vmatrix} 1 & 2 \\ 0 & 1 \end{vmatrix} = 1 \quad A_{32} = (-1)^5 \begin{vmatrix} 0 & 2 \\ 0 & 1 \end{vmatrix} = 0$$
$$A_{33} = (-1)^6 \begin{vmatrix} 0 & 1 \\ 0 & 0 \end{vmatrix} = 0$$

$$A^{-1} = \begin{pmatrix} -1 & -1 & 1 \\ 1 & -2 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

verificare che A^I sia effettivamente l'inversa:

$$\begin{pmatrix} -1 & -1 & 1 \\ 1 & -2 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 2 \\ 0 & 0 & 1 \\ 1 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = I_n$$

Secondo Modo: Sia $A \in \mathcal{M}_n$ con $det(A) \neq 0$. Affianchiamo alle n colonne di A le n colonne della matrice identica, ottenendo una matrice $(A|I_n) \in \mathcal{M}_{n,2n}$. Utilizzando le operazioni elementari trasformiamo questa matrice in modo da ottenere che le prime n colonne siano la matrice identica, cioè otteniamo una matrice $(I_n|B)$. Facendo in questo modo sarà $B = A^{-1}$ l'inversa della matrice di partenza.

Esempio 5.5.5.

$$A = \begin{pmatrix} 2 & 3 \\ 0 & 1 \end{pmatrix} \qquad (A|I_n) = \begin{pmatrix} 2 & 3 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

le prime due colonne devono risultare I_n :

$$r_1 \to r_1 - 3r_2 = \begin{pmatrix} 2 & 0 & 1 & -3 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$
$$r_1 \to \frac{r_1}{2} = \begin{pmatrix} 1 & 0 & 1 & -3/2 \\ 0 & 1 & 0 & 1 \end{pmatrix} = (I_n|B)$$
$$B = \begin{pmatrix} 1 & -3/2 \\ 0 & 1 \end{pmatrix} = A^{-1}$$

Esempio 5.5.6.

$$A = \begin{pmatrix} 0 & 1 & 2 \\ 0 & 0 & 1 \\ 1 & 1 & 3 \end{pmatrix} \qquad (A|I_n) = \begin{pmatrix} 0 & 1 & 2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 3 & 0 & 0 & 1 \end{pmatrix}$$

$$r_2 \leftrightarrow r_3 = \begin{pmatrix} 0 & 1 & 2 & 1 & 0 & 0 \\ 1 & 1 & 3 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$
$$r_1 \leftrightarrow r_2 = \begin{pmatrix} 1 & 1 & 3 & 0 & 0 & 1 \\ 0 & 1 & 2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$
$$r_1 \to r_1 - r_2 = \begin{pmatrix} 1 & 0 & 1 & -1 & 0 & 1 \\ 0 & 1 & 2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$
$$r_2 \to r_2 - 2r_3 = \begin{pmatrix} 1 & 0 & 1 & -1 & 0 & 1 \\ 0 & 1 & 0 & 1 & -2 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$
$$r_1 \to r_1 - r_3 = \begin{pmatrix} 1 & 0 & 0 & -1 & -1 & 1 \\ 0 & 1 & 0 & 1 & -2 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix} \Rightarrow (I_n|B)$$
$$B = \begin{pmatrix} -1 & -1 & 1 \\ 1 & -2 & 0 \\ 0 & 1 & 0 \end{pmatrix} = A^{-1}$$

verificare che A^{-1} è effettivamente l'inversa di A:

$$\begin{pmatrix} 0 & 1 & 2 \\ 0 & 0 & 1 \\ 1 & 1 & 3 \end{pmatrix} \begin{pmatrix} -1 & -1 & 1 \\ 1 & -2 & 0 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = I_n$$

Teorema 5.5.7 (Teorema di Binet)**.** *Siano A e B due matrici quadrate di ordine n. Allora $det(A \cdot B) = det(A) \cdot det(B)$.*

Dal teorema di Binet possiamo dedurre che se una matrice A è invertibile allora deve essere $det(A) \neq 0$. Infatti dato che $AA^{-1} = I_n$, allora $det(A \cdot A^{-1}) = det(I_n)$ e per il teorema di Binet, $det(A) \cdot det(A^{-1}) = 1$ quindi $det(A^{-1}) = 1/det(A)$.

Sia $\mathcal{MI}_n$ l'insieme delle matrici $n \times n$ con determinante diverso da 0:

$$\mathcal{MI}_n = \{A \in \mathcal{M}_n \mid det(A) \neq 0\}.$$

L'operazione di prodotto righe per colonne tra matrici quadrate è una operazione associativa, ha la matrice identica I_n come elemento neutro e inoltre ogni matrice con determinante diverso da zero è invertibile. Quindi $(\mathcal{MI}_n, \cdot)$ è un gruppo (non commutativo), detto **gruppo delle matrici** $n \times n$ **su** $\mathbb{R}$.

La funzione

$$det : A \in \mathcal{MI}_n \mapsto det(A) \in \mathbb{R}$$

è un omomorfismo di $(\mathcal{MI}_n, \cdot)$ in $(\mathbb{R}, \cdot)$: infatti per il teorema di Binet abbiamo che $det(A \cdot B) = det(A) \cdot det(B)$.

5.6 Esercizi

1. Calcolare il prodotto righe per colonne delle seguenti matrici, in tutti i modi in cui sia possibile:

$$A = \begin{pmatrix} 1 & 3 \\ 1 & 1 \\ 1 & 0 \end{pmatrix} \qquad B = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 1 \end{pmatrix}$$
$$C = \begin{pmatrix} 3 & 0 & 0 \\ 0 & -1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \qquad D = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 2 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

2. Calcolare il rango delle matrici dell'esercizio precedente (sia con il metodo degli orlati che con la riduzione a scala).

3. Stabilire quali delle seguenti matrici sono invertibili e calcolarne l'inversa, usando sia il metodo con i determinanti che la riduzione a scala.

$$\begin{pmatrix} 1 & 3 \\ 1 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 & 2 \\ 2 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$
$$\begin{pmatrix} 3 & 0 & 0 \\ 0 & -1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \qquad \begin{pmatrix} 2 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & -2 & 1 \end{pmatrix} \qquad \begin{pmatrix} 0 & -1 & 1 \\ 1 & 1 & 0 \\ 3 & 2 & 1 \end{pmatrix}.$$

4. Dire se i seguenti insiemi di vettori sono linearmente indipendenti:
   - $\{(1,0,1),(2,0,3),(0,4,1)\}$,
   - $\{(1,2),(3,2),(0,1)\}$,
   - $\{(1,2,3,4),(0,1,0,0),(0,4,3,0)\}$,
   - $\{(1,0,1),(0,3,0)\}$,
   - $\{(0,0,1),(0,2,1),(1,0,1),(1,1,1)\}$,
   - $\{(1,2),(2,1)\}$.

5. Studiare il rango delle seguenti matrici al variare del parametro k:

$$A_1 = \begin{pmatrix} 1 & k \\ 0 & k \\ 1 & 0 \end{pmatrix} \qquad A_2 = \begin{pmatrix} k & 0 & 2 \\ 0 & 1 & 1 \end{pmatrix}$$

$$A_3 = \begin{pmatrix} 3 & 0 & 0 \\ 0 & k & 1 \\ 1 & 1 & 1 \end{pmatrix} \qquad A_4 = \begin{pmatrix} 1 & k & 0 \\ k & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

$$A_5 = \begin{pmatrix} 0 & 0 & 1 \\ 2 & k & 0 \\ 1 & 2 & 3k \end{pmatrix} \qquad .$$

6 Sistemi di Equazioni Lineari

6.1 Equazioni, sistemi e matrici

Definizione 6.1.1. Una equazione **lineare** in n incognite è un'espressione del tipo

$$a_1x_1 + \cdots + a_nx_n = b$$

dove $b \in \mathbb{R}$ e $a_i \in \mathbb{R}$, per ogni $i = 1, ..., n$. I numeri a_i sono detti *coefficienti* delle variabili (o delle incognite) x_i, mentre b è detto il *termine noto*.

L'aggettivo *lineare* si riferisce al fatto che le incognite sono presenti con grado 1, cioè non sono elevate a potenza maggiori di 1 e non sono argomento di altre funzioni. Vedremo più avanti anche il significato geometrico di tale terminologia.

Definizione 6.1.2. Una soluzione di un'equazione con n incognite è una n-upla di numeri reali $(c_1, \ldots, c_n)$ tali che $a_1c_1 + a_2c_2 + \cdots + a_nc_n = b$, cioè tale che sostituita al posto delle variabili rende vera l'equazione.

Esempio 6.1.3. La coppia $(-1, 1)$ è una soluzione dell'equazione $2x_1 + 3x_2 = 1$, perché $2(-1) + 3(1) = 1$.

Definizione 6.1.4. Un sistema di m equazioni lineari in n incognite $x_1, \ldots, x_n$ è un insieme di equazioni lineari scritto nel seguente modo:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \cdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{mn}x_n = b_m. \end{cases} \tag{6.1}$$

Una soluzione del sistema è una n-upla che è soluzione di tutte le equazioni contemporaneamente.

Esempio 6.1.5. Consideriamo un sistema con due equazioni e due incognite

$$\begin{cases} x_1 + x_2 = 2 \\ 2x_1 + x_2 = 5 \end{cases}$$

$(1, 1)$ è soluzione della prima ma non della seconda, quindi non è una soluzione del sistema. Invece $(3, -1)$ è soluzione sia della prima equazione che della seconda, quindi è soluzione del sistema.

Notiamo che i coefficienti del sistema dipendono da due indici, e cioè la variabile e l'equazione. Possono essere quindi sistemati in una matrice.

Definizione 6.1.6. Dato un sistema come quello in (6.1), si considerano le seguenti matrici:

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \in \mathcal{M}_{mn} \text{ detta } \textbf{matrice dei coefficienti}$$

$$X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in \mathcal{M}_{n1} \text{ detto } \textbf{vettore colonna delle incognite}$$

$$B = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix} \in M_{m1} \text{ detto } \textbf{vettore colonna dei termini noti}.$$

Il sistema allora si potrà scrivere utilizzando il prodotto righe per colonne come

$$A \cdot X = B.$$

Esempio 6.1.7.

$$A = \begin{pmatrix} 2 & 1 \\ 3 & 0 \end{pmatrix} \qquad X = \begin{pmatrix} x \\ y \end{pmatrix} \qquad B = \begin{pmatrix} 2 \\ 1 \end{pmatrix} \qquad m = n = 2$$

$$AX = \begin{pmatrix} 2x + y \\ 3x \end{pmatrix} = B = \begin{pmatrix} 2 \\ 1 \end{pmatrix} \qquad \Rightarrow \qquad \begin{cases} 2x + y = 2 \\ 3x = 1 \end{cases}$$

Definizione 6.1.8. Un sistema si dice **non compatibile** se non ammette soluzioni, si dice **compatibile** se ammette soluzioni. Un sistema compatibile si dice **determinato** se ammette una sola soluzione, **indeterminato** se ammette infinite soluzioni

Vale infatti la seguente proprietà: un sistema lineare o non ammette soluzioni, o ne ammette una sola oppure ne ammette infinite. Non esistono quindi sistemi lineari che hanno un numero finito di soluzioni maggiore di 1, per esempio non esistono sistemi che hanno esattamente 3 soluzioni: se c'è più di una soluzione allora ce ne sono infinite.

Esempio 6.1.9.

- Consideriamo il sistema di due equazioni e due incognite

$$\begin{cases} 2x + y = 2 \\ 3x = 1. \end{cases}$$

Tale sistema ha una sola soluzione, quindi è determinato. La soluzione del sistema è $(\frac{1}{3}, \frac{4}{3})$. Per verificarlo sostituiamo il valore $1/3$ alle x e il valore $4/3$ alla y:

$$\begin{cases} 2(\frac{1}{3}) + y = 2 \\ 3(\frac{1}{3}) = 1 \end{cases}$$

Notiamo che entrambe le equazioni sono vere, quindi $(\frac{1}{3}, \frac{4}{3})$ è una soluzione del sistema.

- Consideriamo adesso il sistema

$$\begin{cases} 2x + y = 2 \\ 4x + 2y = 4 \end{cases}$$

In questo caso le soluzioni del sistema sono del tipo $(x, 2 - 2x)$ al variare di x: per esempio $(0, 2)$ è una soluzione ma anche $(1, 0)$ è una soluzione, e anche $(2, -2)$.

Il sistema ha infinite soluzioni, quindi è compatible ma indeterminato.

- Consideriamo infine il sistema

$$\begin{cases} 2x + y = 2 \\ 4x + 2y = 1 \end{cases}$$

Tale sistema non ammette soluzioni, è quindi incompatibile.

6.2 Teorema di Rouché-Capelli

Dobbiamo trovare dei metodi per risolvere i sistemi, con un qualsiasi numero di incognite e di equazioni. Il prossimo teorema permette di capire se il sistema è compatibile e quante soluzioni ha.

Definizione 6.2.1. La matrice $(A|B) \in M_{m,n+1}$ ottenuta affiancando la colonna dei termini noti alla matrice dei coefficienti, è chiamata **matrice completa** del sistema.

Teorema 6.2.2 (Teorema di Rouchè-Capelli)**.** *Sia $AX = B$ un sistema lineare di m equazioni in n incognite.*

- *Se $rg(A) \neq rg(A|B)$ allora il sistema è incompatibile.*
- *Se $rg(A) = rg(A|B)$ allora il sistema è compatibile. Chiamiamo r il rango di A e di $A|B$ (cioè $r = rg(A) = rg(A|B)$):*

- *Se $r = n$ allora il sistema ammette una sola soluzione.*
- *Se $r < n$ allora il sistema ammette infinite soluzioni, in particolare infinite soluzioni che dipendono da $n - r$ parametri (scriviamo ∞^{n-r} soluzioni).*

Esempio 6.2.3.

$$\begin{cases} 2x + y = 2 \\ 4x + 2y = 1 \end{cases} \qquad B = \begin{pmatrix} 2 \\ 1 \end{pmatrix} \qquad A = \begin{pmatrix} 2 & 1 \\ 4 & 2 \end{pmatrix}$$

$det(A) = 4 - 4 = 0 \Rightarrow rg(A) = 1$

$$(A|B) = \begin{pmatrix} 2 & 1 & 2 \\ 4 & 2 & 1 \end{pmatrix} \qquad det \begin{pmatrix} 2 & 2 \\ 4 & 1 \end{pmatrix} = 2 - 8 = -6 \neq 0 \Rightarrow rg(A|B) = 2$$

Quindi dato che $rg(A) \neq rg(A|B)$ il sistema è incompatibile.

Approfondiamo il caso in cui $rg(A) = rg(A|B) = r < n$, quindi consideriamo di avere una matrice completa in cui la sottomatrice $r \times r$ con determinante diverso da 0 si trova nella parte alta (cioè nelle prime r righe e r colonne):

$$A|B = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1r} & \dots & a_{1n} & b_1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{r1} & a_{r2} & \dots & a_{rr} & \dots & a_{rn} & b_r \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mr} & \dots & a_{mn} & b_m \end{pmatrix}$$

Per risolvere il sistema considero solo r equazioni relative alla matrice $r \times r$ con $det \neq 0$ e alle variabili $x_1, \dots, x_r$, e porto a destra del segno $=$ le altre variabili:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \dots + a_{1r}x_r = b_1 - a_{1r+1}x_{r+1} - \dots - a_{1n}x_n \\ \dots \\ a_{r1}x_1 + a_{r2}x_2 + \dots + a_{rn}x_r = b_r - a_{rr+1}x_{r+1} - \dots - a_{rn}x_n \end{cases}$$

In questo modo le variabili da x_{r+1} fino a x_n sono considerate come parametri. Si risolve il sistema di r equazioni in r incognite e si ottengono le soluzioni che dipendono dagli $n - r$ parametri $x_{r+1}, \dots, x_n$. In questo caso quindi ci sono infinite soluzioni che dipendono da $n - r$ parametri e scriviamo ∞^{n-r} soluzioni.

Esempio 6.2.4. Consideriamo il sistema

$$\begin{cases} 2x + y = 2 \\ 4x + 2y = 4 \end{cases} \qquad A|B = \begin{pmatrix} 2 & 1 & 2 \\ 4 & 2 & 4 \end{pmatrix}$$

In questo caso $rg(A) = 1$ e $rg(A|B) = 1$, quindi ci sono soluzioni. Dato che $r = 1$ e $n = 2$ allora posso considerare solo una riga della matrice, per esempio la prima, e la corrispondente equazione:

$$2x + y = 2.$$

Inoltre la seconda variabile la sposto a destra e diventa un parametro:

$$2x = 2 - y$$

e quindi le soluzioni sono tutte le coppie (x, y) tali che $x = (2-y)/2$ cioè l'insieme

$$\{((2 - y)/2, y) \mid y \in \mathbb{R}\}$$

formato da infinite soluzioni che dipendono da un parametro y che può essere un numero reale qualsiasi. Si dice in questo caso che ci sono ∞^1 soluzioni.

Nota che in quest'ultimo sistema posso anche scegliere x come parametro e scrivere

$$y = 2 - 2x$$

quindi l'insieme delle soluzioni diventa $\{(x, 2 - 2x) \mid x \in \mathbb{R}\}$, ma non ci dovrebbero essere problemi a notare che i due insiemi coincidono cioè che

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

(Provare ad elencare alcuni elementi di entrambi gli insiemi...)

6.2.1 Sistemi di n equazioni in n incognite: metodo di Cramer

Il metodo di Cramer si applica nel caso in cui la matrice dei coefficienti A è quadrata e $det(A) \neq 0$, cioè per sistemi con n equazioni in n incognite in cui la matrice dei coefficienti è invertibile. Si noti infatti che se $AX = B$ e A è una matrice invertibile, allora sarà

$$X = A^{-1}B,$$

quindi si può ottenere la soluzione del sistema andando a calcolare l'inversa della matrice A e facendo poi il prodotto righe per colonne con la colonna B.

Esempio 6.2.5. Consideriamo il sistema

$$\begin{cases} y + 2z = 1 \\ z = 3 \\ x + y + 3z = 0 \end{cases}$$

che ha matrice dei coefficienti: $A = \begin{pmatrix} 0 & 1 & 2 \\ 0 & 0 & 1 \\ 1 & 1 & 3 \end{pmatrix}$ con $det(A) = 1 \neq 0$, quindi $rg(A) = 3$. La matrice completa è $A|B = \begin{pmatrix} 0 & 1 & 2 & 1 \\ 0 & 0 & 1 & 3 \\ 1 & 1 & 3 & 0 \end{pmatrix}$ che ha anche $rg(A|B) = 3$ perché contiene la matrice A come sottomatrice quadrata con determinante non nullo. Quindi per il teorema di Rouchè-Capelli, il sistema ammette una soluzione, che posso trovare considerando $X = A^{-1} \cdot B$. Devo quindi calcolare l'inversa della matrice A e moltiplicarla righe per colonne con B.

$$A^{-1} = \begin{pmatrix} -1 & -1 & 1 \\ 1 & -2 & 0 \\ 0 & 1 & 0 \end{pmatrix} \qquad A^{-1} \cdot B = \begin{pmatrix} -1 & -1 & 1 \\ 1 & -2 & 0 \\ 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 3 \\ 0 \end{pmatrix} = \begin{pmatrix} -4 \\ -5 \\ 3 \end{pmatrix}$$

Andiamo a verificare che $(-4, -5, 3)$ sia soluzione del sistema, sostituendo i valori di x, y, z:

$$\begin{cases} -5 + 2(3) = 1 \\ 3 = 3 \\ -4 - 5 + 3 \cdot 3 = 0 \end{cases} \quad \begin{cases} -5 + 6 = 1 \\ 3 = 3 \\ -9 + 9 = 0 \end{cases} \quad \begin{cases} 1 = 1 \\ 3 = 3 \\ 0 = 0 \end{cases}$$

Invece di calcolare l'inversa della matrice dei coefficienti, possiamo usare il metodo di Cramer che ci permette di organizzare i calcoli in modo diverso (il numero totale di operazioni da fare però non cambia poi molto...).

Teorema 6.2.6 (Metodo di Cramer)**.** *Consideriamo un sistema di n equazioni in n incognite $AX = B$ con $det(A) \neq 0$ (A è una matrice quadrata). Allora se poniamo*

$$x_i = \frac{det(A_i)}{det(A)},$$

dove A_i è la matrice che si ottiene da A sostituendo la i-esima colonna di A con la colonna dei termini noti, si ha che $(x_1, \ldots, x_n)$ è una soluzione del sistema.

Esempio 6.2.7. Consideriamo il sistema $\begin{cases} 2x + y - z = 1 \\ x + z = 0 \\ x + 2y - z = 2 \end{cases}$ la cui matrice dei coefficienti è

$$\begin{pmatrix} 2 & 1 & -1 \\ 1 & 0 & 1 \\ 1 & 2 & -1 \end{pmatrix}$$

che è una matrice quadrata 3×3 e $det(A) = -4 \neq 0$. Andiamo a calcolare il determinante delle matrici A_x, A_y e A_z ottenute sostituendo la colonna dei termini noti rispettivamente alla prima, poi alla seconda e poi alla terza colonna di A.

$$A_x = \begin{pmatrix} 1 & 1 & -1 \\ 0 & 0 & 1 \\ 2 & 2 & -1 \end{pmatrix} \quad A_y = \begin{pmatrix} 2 & 1 & -1 \\ 1 & 0 & 1 \\ 1 & 2 & -1 \end{pmatrix} \quad A_z = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 2 & 2 \end{pmatrix}$$

Ci accorgiamo che $det(A_x) = det(A_z) = 0$ perché entrambe le matrici contengono due colonne uguali. Si ottiene poi $det(A_y) = det(A) = -4$. Quindi la soluzione (unica) del sistema è $x = 0/(-4) = 0$, $y = (-4)/(-4) = 1$ e $z = 0/(-4) = 0$, cioè $(0, 1, 0)$.

Metodo di Cramer per sistemi di m equazioni in n incognite

Posso usare il metodo di Cramer anche per sistemi di m equazioni in n incognite con $m \neq n$. Infatti per il teorema di Rouchè-Capelli, una volta stabilito che $rg(A) = rg(A|B) = r$ posso riscrivere il sistema iniziale come un sistema di r equazioni in r incognite, andando a considerare le altre $n - r$ incognite come parametri. Posso quindi applicare il metodo di Cramer per risolvere il sistema con matrice dei coefficienti quadrata.

Esempio 6.2.8. Consideriamo il sistema di 2 equazioni in 3 incognite:

$$\begin{cases} x + y - z = 1 \\ x + 2y + 2z = 0 \end{cases}$$

che ha matrice dei coefficienti e matrice completa uguali a:

$$A = \begin{pmatrix} 1 & 1 & -1 \\ 1 & 2 & 2 \end{pmatrix} \qquad A|B = \begin{pmatrix} 1 & 1 & -1 & 1 \\ 1 & 2 & 2 & 0 \end{pmatrix}$$

Dato che $rg(A) = rg(A|B) = 2$ il sistema ha ∞^1 soluzioni. Considero z come parametro e ottengo il sistema

$$\begin{cases} x + y = 1 + z \\ x + 2y = -2z \end{cases}$$

che ha matrice dei coefficienti e matrice completa uguali a:

$$A' = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \qquad A'|B' = \begin{pmatrix} 1 & 1 & 1+z \\ 1 & 2 & -2z \end{pmatrix}$$

Dato che la matrice A' è quadrata ed ha determinante $det(A') = 1 \neq 0$, posso applicare il metodo di Cramer:

$$det(A'_x) = det\begin{pmatrix} 1+z & 1 \\ -2z & 2 \end{pmatrix} = 2+4z \qquad det(A'_y) = det\begin{pmatrix} 1 & 1+z \\ 1 & -2z \end{pmatrix} = -3z-1$$

e quindi l'insieme delle soluzioni del sistema, che dovranno dipendere dal parametro z, sarà $\{(2+4z, -3z-1, z) \mid z \in \mathbb{R}\}$.

6.2.2 Metodo di Gauss

Il metodo di Gauss ci permette di risolvere i sistemi (di un numero qualsiasi di equazioni e di incognite) senza calcolare determinanti, ma usando la riduzione a scala e trasformando un sistema di equazioni lineari in un sistema più semplice. Infatti vale il seguente:

Teorema 6.2.9 (Metodo di Gauss)**.** *Se $A'|B'$ si ottiene da $A|B$ tramite operazioni elementari, i sistemi sono equivalenti, perciò il sistema $AX = B$ ha le stesse soluzioni di $A'X = B'$.*

In un sistema con matrice a scala posso facilmente controllare il rango (che in questo caso è il numero di righe non nulle) e quindi, tramite il teorema di Rouchè-Capelli sapere se e quante soluzioni ci sono. Infatti, se la matrice completa $A|B$ si trasforma in una matrice a scala $A'|B'$ allora A' sarà la forma a scala di A e quindi $rg(A) = rg(A')$ e $rg(A|B) = rg(A'|B')$. Inoltre, una volta ridotta la matrice completa a scala, posso risolvere il sistema per sostituzione, dato che nell'ultima equazione compariranno poche variabili (come vedremo ne rimane una sola e le altre saranno usate come parametri).

Esempio 6.2.10. Consideriamo il caso $n = m = 2$

$$\begin{cases} 2x + y = 1 \\ x + 3y = 2 \end{cases} \qquad A = \begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix} \qquad A|B = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 3 & 2 \end{pmatrix}$$

scrivo $A|B$ in forma scala così da poter trovare il rango. L'operazione da effettuare è $r_2 \to r_2 - \frac{1}{2}r_1$

$$\begin{pmatrix} 2 & 1 & 1 \\ 0 & 5/2 & 3/2 \end{pmatrix} \Rightarrow \begin{cases} 2x + y = 1 \\ 5/2y = 3/2, \end{cases}.$$

Dato che $rg(A|B) = rg(A) = 2$, per il teorema di Rouchè-Capelli il sistema ha una soluzione. Risolvo il sistema associato alla forma a scala, partendo

dall'ultima equazione e sostituendo nella prima:

$$\begin{cases} y = 3/2 \cdot 2/5 = 3/5 \\ 2x + 3/5 = 1 \text{ quindi } 2x = 1 - 3/5 \text{ quindi } 2x = 2/5 \text{ quindi } x = 1/5 \end{cases}$$

La soluzione del sistema è $(1/5, 3/5)$.

Esempio 6.2.11.

$$\begin{cases} x + 2y = 3 \\ x + 2z = 2 \\ 2x + 2y + z = 1 \end{cases} \qquad \begin{pmatrix} 1 & 2 & 0 & 3 \\ 1 & 0 & 2 & 2 \\ 2 & 2 & 1 & 1 \end{pmatrix}$$

riduco $A|B$ in forma a scala

$$\begin{pmatrix} 1 & 2 & 0 & 3 \\ 1 & 0 & 2 & 2 \\ 2 & 2 & 1 & 1 \end{pmatrix} \quad r_2 \to r_2 - r_1 \quad \begin{pmatrix} 1 & 2 & 0 & 3 \\ 0 & -2 & 2 & -1 \\ 2 & 2 & 1 & 1 \end{pmatrix} \quad r_3 \to r_3 - 2r_1$$

$$\begin{pmatrix} 1 & 2 & 0 & 3 \\ 0 & -2 & 2 & -1 \\ 0 & -2 & 1 & -5 \end{pmatrix} \quad r_3 \to r_3 - r_2 \quad \begin{pmatrix} 1 & 2 & 0 & 3 \\ 0 & -2 & 2 & -1 \\ 0 & 0 & -1 & -4 \end{pmatrix}$$

Dato che $rg(A|B) = rg(A) = 3$ il sistema ha una soluzione. Riscrivo il sistema associato alla matrice ridotta a scala e poi risolvo per sostituzione partendo dall'ultima equazione:

$$\begin{cases} x + 2y = 3 \\ -2y + 2z = -1 \\ -z = -4 \end{cases} \qquad \begin{cases} z = 4 \\ -2y + 8 = -1 \text{ quindi } y = \dfrac{9}{2} \\ x + 9 = 3 \text{ quindi } x = -6 \end{cases}$$

La soluzione del sistema è $(-6, 9/2, 4)$.

Esempio 6.2.12. $m = 3$, $n = 2$

$$\begin{cases} 2x + y = 0 \\ x - 2y = 0 \\ 3x + y = 3 \end{cases} \qquad A|B = \begin{pmatrix} 2 & 1 & 0 \\ 1 & -2 & 0 \\ 3 & 1 & 3 \end{pmatrix}$$

riduzione a scala della matrice $A|B$

$$\begin{pmatrix} 2 & 1 & 0 \\ 1 & -2 & 0 \\ 3 & 1 & 3 \end{pmatrix} \quad r_2 \to r_2 - \frac{1}{2}r_1 \ , \ r_3 \to r_3 - \frac{3}{2}r_1 \quad \begin{pmatrix} 2 & 1 & 0 \\ 0 & -5/2 & 0 \\ 0 & -1/2 & 3 \end{pmatrix}$$

$$r_3 \to r_3 - \frac{1}{5}r_2 \quad \begin{pmatrix} 2 & 1 & 0 \\ 0 & -5/2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$$

$rg(A|B) = 3$ mentre $rg(A) = 2$, quindi dato che $rg(A|B) > rg(A)$ non ci sono soluzioni. Infatti scrivendo il sistema relativo alla matrice a scala otteniamo:

$$\begin{cases} 2x + y = 0 \\ -\frac{5}{2}y = 0 \\ 0 = 3 \quad \text{che è sempre falsa.} \end{cases}$$

Esempio 6.2.13.

$$\begin{cases} y + z = 2 \\ x + 2y - z = 1 \\ x + 4y + z = 5 \end{cases} \qquad A|B = \begin{pmatrix} 0 & 1 & 1 & 2 \\ 1 & 2 & -1 & 1 \\ 1 & 4 & 1 & 5 \end{pmatrix}$$

Riduzione a scala della matrice $A|B$:

$$\begin{pmatrix} 0 & 1 & 1 & 2 \\ 1 & 2 & -1 & 1 \\ 1 & 4 & 1 & 5 \end{pmatrix} \quad r_1 \leftrightarrow r_2 \quad \begin{pmatrix} 1 & 2 & -1 & 1 \\ 0 & 1 & 1 & 2 \\ 1 & 4 & 1 & 5 \end{pmatrix}$$

$$r_3 \to r_3 - r_1 \quad \begin{pmatrix} 1 & 2 & -1 & 1 \\ 0 & 1 & 1 & 2 \\ 0 & 2 & 2 & 4 \end{pmatrix} \quad r_3 \to r_3 - 2r_2 \quad \begin{pmatrix} 1 & 2 & -1 & 1 \\ 0 & 1 & 1 & 2 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Dato che $rg(A|B) = rg(A) = 2$ e ci sono $n = 3$ incognite, per il teorema di Rouchè-Capelli ci sono ∞^1 soluzioni.

$$\begin{cases} x + 2y - z = 1 \\ y + z = 2 \\ 0 = 0 \end{cases} \to \text{considero} \begin{cases} x + 2y - z = 1 \\ y + z = 2 \end{cases}$$

Considero una variabile come parametro, la porto a destra di $=$:

$$\begin{cases} x + 2y = 1 + z \\ y = 2 - z \end{cases} \quad \begin{cases} x + 2(2 - z) = 1 + z \\ y = 2 - z \end{cases}$$

$$\begin{cases} x + 4 - 2z = 1 + z \\ y = 2 - z \end{cases} \quad \begin{cases} x = -3 + 3z \\ y = 2 - z \end{cases}$$

Il sistema ha come soluzioni tutte le terne dell'inseme $\{(-3+3z, 2-z, z) \mid z \in \mathbb{R}\}$.

Esempio 6.2.14.

$$\begin{cases} x_1 + x_2 + x_3 = 1 \\ 2x_1 - 2x_2 + 2x_3 = 0 \\ x_1 - 3x_3 = 1 \end{cases} \qquad A = \begin{pmatrix} 1 & 1 & 1 \\ 2 & -2 & 2 \\ 1 & 0 & -3 \end{pmatrix} \qquad B = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$$

Dato che A è una matrice quadrata e $det(A) = 16 \neq 0$, possiamo applicare il metodo di Cramer:

$$A_1 = \begin{pmatrix} \mathbf{1} & 1 & 1 \\ \mathbf{0} & -2 & 2 \\ \mathbf{1} & 0 & -3 \end{pmatrix} \qquad det(A_1) = \begin{vmatrix} -2 & 2 \\ 0 & -3 \end{vmatrix} + \begin{vmatrix} 1 & 1 \\ -2 & 2 \end{vmatrix} = 10 \qquad x_1 = \frac{10}{16}$$

$$A_2 = \begin{pmatrix} 1 & \mathbf{1} & 1 \\ 2 & \mathbf{0} & 2 \\ 1 & \mathbf{1} & -3 \end{pmatrix} \qquad det(A_2) = -\begin{vmatrix} 2 & 2 \\ 1 & -3 \end{vmatrix} - \begin{vmatrix} 1 & 1 \\ 2 & 2 \end{vmatrix} = 8 \qquad x_2 = \frac{8}{16}$$

$$A_3 = \begin{pmatrix} 1 & 1 & \mathbf{1} \\ 2 & -2 & \mathbf{0} \\ 1 & 0 & \mathbf{1} \end{pmatrix} \qquad det(A_3) = -\begin{vmatrix} 1 & 1 \\ -2 & 0 \end{vmatrix} - \begin{vmatrix} 1 & 1 \\ 2 & -2 \end{vmatrix} = -2 \qquad x_2 = -\frac{2}{16}$$

La soluzione del sistema è quindi $(\frac{5}{8}, \frac{1}{2}, -\frac{1}{8})$. Provare a risolvere il sistema con il metodo di Gauss.

Esempio 6.2.15. $m = n = 4$

$$\begin{cases} x_1 + 2x_2 + x_3 - x_4 = 1 \\ x_2 - x_3 + x_4 = 0 \\ x_1 + 3x_2 = 1 \\ 2x_1 + 5x_2 + x_3 - x_4 = 2 \end{cases} \qquad A|B = \begin{pmatrix} 1 & 2 & 1 & -1 & 1 \\ 0 & 1 & -1 & 1 & 0 \\ 1 & 3 & 0 & 0 & 1 \\ 2 & 5 & 1 & -1 & 2 \end{pmatrix}$$

riduzione a scala della matrice $A|B$:

$$\begin{pmatrix} 1 & 2 & 1 & -1 & 1 \\ 0 & 1 & -1 & 1 & 0 \\ 0 & 1 & -1 & 1 & 0 \\ 0 & 1 & -1 & 1 & 0 \end{pmatrix} \qquad r_3 \to r_3 - r_1, r_4 \to r_4 - 2r_1$$

$$\begin{pmatrix} 1 & 2 & 1 & -1 & 1 \\ 0 & 1 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \qquad r_3 \to r_3 - r_2, r_4 \to r_4 - r_2$$

Si ha $rg(A|B) = 2 = rg(A)$, quindi il sistema ha $\infty^{4-2} = \infty^2$ soluzioni. Scrivo solo le due equazioni corrispondenti alle righe non nulle della matrice a scala:

$$\begin{cases} x_1 + 2x_2 + x_3 - x_4 = 1 \\ x_2 - x_3 + x_4 = 0 \end{cases} \qquad \begin{cases} x_1 + 2x_2 = 1 - x_3 + x_4 \\ x_2 = x_3 - x_4 \end{cases}$$

$$\begin{cases} x_1 + 2(x_3 - x_4) = 1 - x_3 + x_4 \\ x_2 = x_3 - x_4 \end{cases} \qquad \begin{cases} x_1 + 2x_3 - 2x_4 = 1 - x_3 + x_4 \\ x_2 = x_3 - x_4 \end{cases}$$

$$\begin{cases} x_1 = 1 - 3x_3 + 3x_4 \\ x_2 = x_3 - x_4 \end{cases}$$

Uso le due variabili x_3 e x_4 come parametri. Le soluzioni del sistema sono: $\{(1 - 3x_3 + 3x_4, x_3 - x_4, x_3, x_4) \mid x_3, x_4 \in \mathbb{R}\}$.

6.2.3 Sistemi omogenei

Definizione 6.2.16. Un sistema lineare si dice **omogeneo** se il vettore dei termini noti è il vettore nullo, cioè è formato solo da 0. Un sistema omogeneo ha sempre soluzioni perché $rg(A) = rg(A|B)$ e il vettore nullo $(0, 0, \dots 0)$ è sempre soluzione

Esempio 6.2.17.

$$\begin{cases} x + 2y = 0 \\ 2x - y = 0 \end{cases} \qquad A|B = \begin{pmatrix} 1 & 2 & 0 \\ 2 & -1 & 0 \end{pmatrix}$$

è un sistema omogeneo e $rg(A) = rg(A|B) = 2$. Quindi c'è un'unica soluzione che è $(0, 0)$.

Il **sistema omogeneo associato** ad un sistema $AX = B$ è il sistema $AX = 0$ (dove con 0 si indica in questo caso il vettore nullo).

Esempio 6.2.18. Consideriamo il sistema

$$\begin{cases} x + y = 1 \\ x + z = 0 \\ 2x + y + z = 1 \end{cases}$$

e il sistema omogeneo associato

$$\begin{cases} x + y = 0 \\ x + z = 0 \\ 2x + y + z = 0 \end{cases}$$

che ha come matrice dei cofficienti $A = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 2 & 1 & 1 \end{pmatrix}$ Si ha $det(A) = 0$ e $rg(A) = 2$. E' inutile considerare la matrice completa $A|B$ perché avrà una colonna composta solo da 0, quindi il rango di $A|B$ è sempre uguale al rango di A. Per il teorema di Rouchè-Capelli il sistema omogeneo ha ∞^1 soluzioni. Consideriamo quindi le prime due equazioni:

$$\begin{cases} x + y = 0 \\ x + z = 0 \end{cases}$$

e prendiamo z come parametro. Avremo quindi

$$\begin{cases} x = -z \\ -z + y = 0 \end{cases} \qquad \begin{cases} x = -z \\ y = z \end{cases}$$

e l'insieme delle soluzioni del sistema è $\{(-z, z, z) \mid z \in \mathbb{R}\}$. Nota che in particolare $(0, 0, 0)$ è una soluzione del sistema.

Quali sono invece le soluzioni del sistema non omogeneo iniziale?

6.3 Intepretazione geometrica

Consideriamo prima il piano cartesiano. Fissiamo due rette perpendicolari (una orizzontale e una verticale) che rappresentano gli assi. Sulle due rette rappresentiamo i numeri reali, fissando quindi una unità di misura e un orientamento (dal basso verso l'alto per l'asse verticale e da sinistra a destra per l'asse orizzontale). Nella loro intersezione c'è l'origine degli assi che corrisponde al punto $(0, 0)$. Ogni punto nel piano è individuato da una coppia di coordinate *cartesiane* rispetto agli assi fissati. Un punto è quindi un elemento di $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2 = \{(x, y) \mid x, y \in \mathbb{R}\}$. Per convenzione le coordinate sono tali che la prima componente rappresenta la proiezione sull'asse orizzontale e la seconda componente su quello verticale come in Figura 6.1.

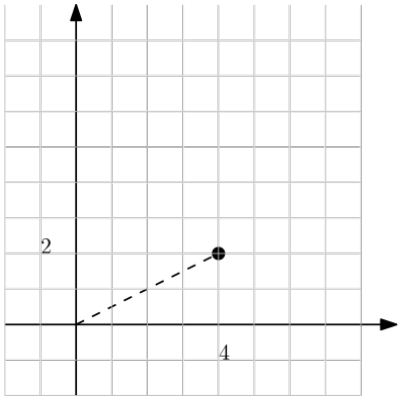


Figura 6.1: Il punto di coordinate $(4, 2)$

L'operazione di somma in $\mathbb{R}^2$ permette di ottenere un punto con la regola del parallelogramma: la somma di due punti di coordinate (x_1, y_1) e (x_2, y_2) è un punto che geometricamente si può vedere come il quarto vertice di un parallelogramma che ha vertici $(0, 0)$, (x_1, y_1) e (x_2, y_2).

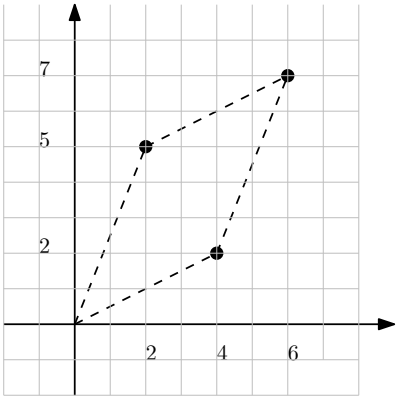


Figura 6.2: Somma dei due punti $(2, 5)$ e $(4, 2)$

Invece quando si moltiplica un punto per un numero si ottiene un punto che giace sulla stessa retta che unisce l'origine con il punto iniziale.

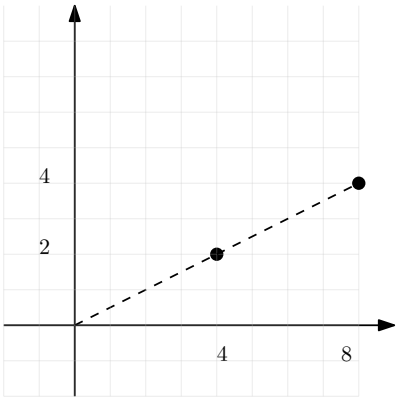


Figura 6.3: Il vettore $2(4, 2) = (8, 4)$

Insiemi di punti formano delle figure geometriche. Per esempio l'insieme $X = \{(x, y) \mid y = 2x\} = \{(x, 2x) \mid x \in \mathbb{R}\} = \{(0, 0), (1, 2), (2, 4), \dots\} \subseteq \mathbb{R}^2$ è l'insieme dei punti che si trovano su una retta come in Figura 6.4.

Proprietà 6.3.1. *L'insieme delle soluzioni di una equazione lineare in due incognite $ax + by = c$ (con $a, b, c \in \mathbb{R}$) è un insieme di punti che forma una retta nel piano cartesiano.*

Esempio 6.3.2. L'equazione $2x + y = 1$ corrisponde alla retta formata da tutti i punti dell'insieme delle soluzioni $\{(x, 1 - 2x) \mid x \in \mathbb{R}\}$. Se considero invece l'equazione $x = 3$ ho come insieme delle soluzioni l'insieme tutti i punti $\{(3, y) \mid$

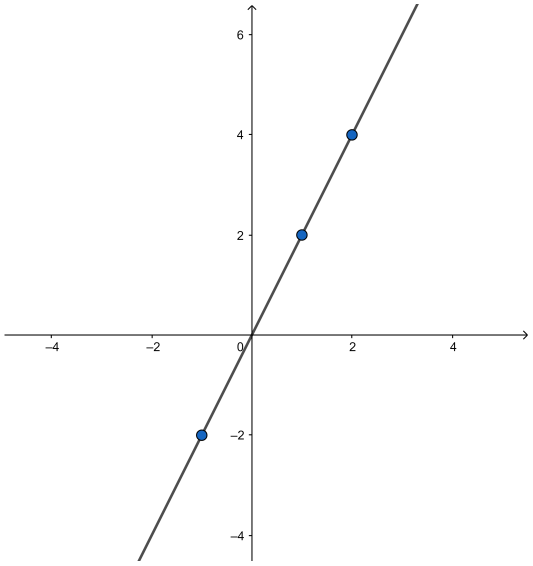


Figura 6.4: Insieme dei punti $X = \{(x, y) \mid y = 2x\}$

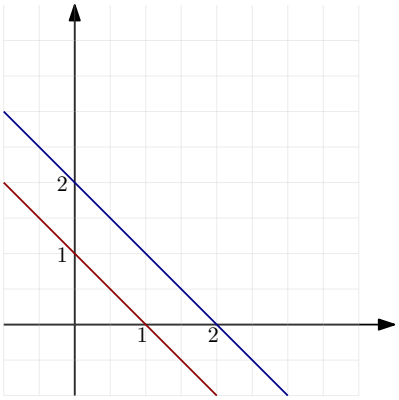
$y \in \mathbb{R}\}$, che formano una retta parallela all'asse verticale. L'equazione $y = 0$ invece ha come soluzioni l'insieme $\{(x, 0) \mid x \in \mathbb{R}\}$ che coincide con l'asse orizzontale.

A cosa corrispondono allora i sistemi?

Proprietà 6.3.3. *L'insieme delle soluzioni di un sistema di equazioni lineare con due incognite è l'insieme dei punti in cui si incontrano le rette corrispondenti alle equazioni.*

Infatti, un sistema di equazioni lineari in due incognite ha come soluzioni i punti che appartengono a tutte le rette del sistema. Dato che due rette nel piano possono o intersecarsi o essere parallele, abbiamo il caso in cui il sistema ha una soluzione (il punto di intersezione di due rette) o nessuna soluzione (quando le rette sono parallele). Se invece il sistema ha infinite soluzioni, vuol dire che il rango della matrice è 1 quindi solo una equazione è indipendente e le altre dipendono da questa. Supponiamo che il sistema abbia due equazioni, e rango uguale a 1. Quindi ogni punto di una retta è combinazione lineare di un punto dell'altra, quindi giacciono sulla stessa retta: le due rette si sovrappongono e le infinite soluzioni del sistema sono gli infiniti punti di sovrapposizione delle due rette.

Esempio 6.3.4. Consideriamo il sistema $\begin{cases} x + y = 1 \\ x + y = 2 \end{cases}$ che non ha soluzioni. Le soluzioni delle due equazioni prese singolarmente sono le due rette di equazione $y = 1 - x$ e $y = 2 - x$, formate quindi dagli insiemi di punti $\{(x, 1 - x) \mid x \in \mathbb{R}\}$ e $\{(x, 2 - x) \mid x\mathbb{R}\}$. Sono due rette parallele, non hanno punti in comune, quindi il sistema non ha soluzioni.



Se invece considero il sistema $\begin{cases} x+y=1 \\ 2x+2y=2 \end{cases}$ in questo caso il rango della matrice dei coefficienti (e di quella completa) è uguale a 1 e infatti la seconda equazione si può vedere come la prima moltiplicata per 2. Le due equazioni rappresentano la stessa retta, quindi le soluzioni sono tutti i punti di tale retta e cioè l'insieme $\{(x, 1-x) \mid x \in \mathbb{R}\}$.

Se invece di considerare $\mathbb{R}^2$ considero $\mathbb{R}^n$, posso pensare le n-uple come punti in uno spazio n-dimensionale. In particolare per $n = 3$ si ha lo spazio tridimensionale. Anche in questi casi le equazioni lineari rappresentano particolari figure geometriche:

- per $n = 3$ un'equazione lineare di tre incognite corrisponde ad un piano nello spazio;
- per $n > 3$ un'equazione lineare di n incognite si chiama iperpiano.

Le soluzioni di un sistema lineare sono quindi gli insiemi di punti che si trovano nell'intersezione degli iperpiani rappresentati dalle singole equazioni. Per $n = 3$ quindi un sistema di 2 equazioni in 3 incognite rappresenta l'intersezione di due piani che può quindi essere l'insieme vuoto (non ci sono soluzioni) quando i due piani sono paralleli, oppure una retta (cioè ∞^1 soluzioni) oppure un piano (∞^2 soluzioni) quando i due piani si sovrappongono.

Provare a descrivere geometricamente cosa succede in un sistema di 3 equazioni in 3 incognite.

6.4 Esercizi

1. Si dica dei seguenti sistemi se hanno soluzioni e nel caso affermativo calcolarle (utilizzando tutti i metodi possibili):

   a) $\begin{cases} 2x + y - z = 0 \\ 3x + y = 1 \\ 5x + 2y - z = 1 \end{cases}$

   b) $\begin{cases} 2x + y - z = 1 \\ x + y = 0 \\ x + 2y - z = 2 \end{cases}$

   c) $\begin{cases} x + y = 1 \\ 2x + 2y = 3 \end{cases}$

   d) $\begin{cases} x + y + z = 3 \\ 2x + y = 2 \\ x + 2y - z = 0 \end{cases}$

   e) $\begin{cases} x + y + 2z - h = 1 \\ 2y - z + h = 0 \end{cases}$

   Considerare anche i sistemi omogenei associati.

2. Determinare al variare di k quante soluzioni ammettono i seguenti sistemi:
   $\begin{cases} x + 2y - z = -1 \\ kx + 2z = 1 \\ -x + 3z = 1 \end{cases}$ $\begin{cases} kx + y = 0 \\ ky + z = 0 \\ x + kz = 0 \end{cases}$

7 Spazi vettoriali

7.1 Definizioni

Definizione 7.1.1. Uno **Spazio Vettoriale** su un campo $\mathbb{K}$ è una struttura algebrica $(V, +, \cdot)$ con due operazioni, la prima detta *somma* e la seconda detta *prodotto esterno*:

$$+ : (u, v) \in V \times V \to u + v \in V$$
$$\cdot : (r, u) \in \mathbb{K} \times V \to ru \in V .$$

che soddisfano le seguenti proprietà, per ogni $u, v \in V$ e $r \in \mathbb{K}$:

- $(V, +)$ è un gruppo commutativo;
- $r(u + v) = r \cdot u + r \cdot v$;
- $(r + s) \cdot u = r \cdot u + s \cdot u$;
- $(r \cdot s)u = r(s \cdot u)$;
- $1 \cdot u = u$ (dove 1 è l'elemento neutro moltiplicativo del campo $\mathbb{K}$).

Gli elementi di $\mathbb{K}$ si chiamano *scalari*, gli elementi di V si chiamano *vettori*.

L'elemento neutro del gruppo $(V, +)$ si chiama *vettore nullo* e si indica con $\mathbf{0}_V$. Nel seguito considereremo come campo unicamente il campo $\mathbb{R}$ dei numeri reali, parleremo quindi di spazi vettoriali sui reali.

Esempio 7.1.2. Consideriamo $\mathbb{R}^2 = \{(x, y) \mid x, y \in \mathbb{R}\}$ con la somma definita da $(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$ e il prodotto esterno definito da $r(x, y) = (rx, ry)$. Si ha che $(\mathbb{R}^2, +)$ è un gruppo che ha $(0, 0)$ come elemento neutro. Si possono inoltre verificare facilmente tutte le altre condizioni della definizione e quindi avremo che $\mathbb{R}^2$ è uno spazio vettoriale sui reali.

Esempio 7.1.3. Per ogni $n \geq 1$, $(\mathbb{R}^n, +, \cdot)$ è uno spazio vettoriale sul campo dei reali; gli elementi di $\mathbb{R}^n$ sono i vettori con n componenti.

Esempio 7.1.4. Per $n = 1$, $\mathbb{R}^1 = \mathbb{R}$ è uno spazio vettoriale con le operazioni di somma e prodotto di numeri reali.

Esempio 7.1.5. Consideriamo l'insieme $\mathcal{M}_{mn}$ delle matrici $m \times n$ con le seguenti operazioni: se $A = (a_{ij})$ e $B = (b_{ij}) \in \mathcal{M}_{mn}$ definiamo $A+B = (a_{ij}+b_{ij}) \in \mathcal{M}_{mn}$ e $r \cdot A = (r \cdot a_{ij})$. Allora $(\mathcal{M}_{mn}, +, \cdot)$ è uno spazio vettoriale sui reali.

Definizione 7.1.6. Se V è uno spazio vettoriale e $U \subseteq V$, allora V è un ~~sottospazio~~ di V se:

- per ogni $u_1, u_2 \in U$ si ha $u_1 + u_2 \in U$;
- per ogni $u \in U$ e per ogni $r \in \mathbb{R}$ si ha $r \cdot u \in U$.

Queste condizioni sono dette condizioni di stabilità (o di chiusura) rispetto alle operazioni.

Ogni sottospazio vettoriale è uno spazio vettoriale a sua volta.

Esempio 7.1.7. Nello spazio $V = \mathbb{R}^2 = \{(x, y) \mid x, y \in \mathbb{R}\}$ il sottoinsieme $U = \{(1, 1), (1, 2)\}$ è un sottospazio di $\mathbb{R}^2$?
Consideriamo i due vettori $(1, 1)$ e $(1, 2)$ in U:

$$(1, 1) + (1, 2) = (2, 3) \notin U$$

quindi U non è un sottospazio di $\mathbb{R}^2$.
Neanche l'insieme $\{(1, 1)\}$ è un sottospazio di $\mathbb{R}^2$, perchè $(1, 1) + (1, 1) = (2, 2) \notin \{(1, 1)\}$.
Invece l'insieme $D = \{(x, x) \mid x \in \mathbb{R}\}$ formato dalle coppie con prima e seconda componente uguale, è un sottospazio di $\mathbb{R}^2$. Infatti consideriamo due vettori $(x, x), (y, y) \in D$. Si ha $(x, x) + (y, y) = (x + y, x + y) \in D$ e per ogni $r \in \mathbb{R}$, $r(x, x) = (rx, rx) \in D$ quindi D è un sottospazio.

Esempio 7.1.8. $X = \{(x, 2x) \mid x \in \mathbb{R}\}$ è un sottospazio di $\mathbb{R}^2$?

- $(x, 2x) + (y, 2y) = (x + y, 2x + 2y) = (x + y, 2(x + y)) \in X$;
- $(x, 2x)r = (rx, 2rx) \in X$.

Quindi X è un sottospazio di $\mathbb{R}^2$.

Si noti che l'insieme $\{\mathbf{0}_V\}$ formato solo dal vettore nullo è sempre un sottospazio di V, dato che $\mathbf{0}_V + \mathbf{0}_V = \mathbf{0}_V$ e $r \cdot \mathbf{0}_V = \mathbf{0}_V$.

Esempio 7.1.9. $Y = \{(x, x + 1) \mid x \in \mathbb{R}\}$ è un sottospazio di $\mathbb{R}^2$?

$$(x, x + 1) + (y, y + 1) = (x + y, x + 1 + y + 1) = (x + y, x + y + 2) \notin Y$$

quindi Y non è un sottospazio (nota che non c'è bisogno di controllare l'altra condizione dato che già la prima non vale).

Esempio 7.1.10. Sia $W = \{(x_1, 2x_1 + x_3, x_3, 2x_3) \mid x_1, x_3 \in \mathbb{R}\} \subseteq \mathbb{R}^4$. Considero la somma di due elementi di W $(x_1, 2x_1 + x_3, x_3, 2x_3) + (y_1, 2y_1 + y_3, 2y_3) = (x_1 + y_1, 2(x_1 + y_2) + (x_3 + y_3), x_3 + y_3, 2(x_3 + y_3)) \in W$ e il prodotto esterno $r(x_1, 2x_1 + x_3, x_3, 2x_3) = (rx_1, 2rx_1 + rx_3, rx_3, 2rx_3) \in W$, quindi W è un sottospazio di $\mathbb{R}^4$.

Proprietà 7.1.11. *L'insieme delle soluzioni di un sistema ~~lineare~~ omogeneo in n variabili è un sottospazio di $\mathbb{R}^n$.*

Esempio 7.1.12. Sistema omogeneo in tre incognite

$$\begin{cases} x_1 + x_2 = 0 \\ x_2 - 3x_3 = 0 \end{cases} \qquad A|B = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & -3 & 0 \end{pmatrix}$$

$rg(A) = rg(A|B) = 2$ quindi ci sono ∞^1 soluzioni che dipendono da un parametro

$$\begin{cases} x_1 + x_2 = 0 \\ x_2 = 3x_3 \end{cases} \quad \begin{cases} x_1 + 3x_3 = 0 \\ x_2 = 3x_3 \end{cases} \quad \begin{cases} x_1 = -3x_3 \\ x_2 = 3x_3 \end{cases}$$

L'insieme delle soluzioni quindi è $X = \{(-3x_3, 3x_3, x_3) \mid x_3 \in \mathbb{R}\}$. Proviamo che X è un sottospazio di $\mathbb{R}^3$:

- $(-3x, 3x, x) + (-3y, 3y, y) = (-3(x + y), 3(x + y), x + y) \in X$ quindi la somma di due soluzioni del sistema è una soluzione del sistema;
- $r(-3x, 3x, x) = (-3rx, 3rx, rx) \in X$ quindi il prodotto di una soluzione per uno scalare è ancora una soluzione del sistema.

Esempio 7.1.13. Consideriamo lo spazio vettoriale $\mathcal{M}_2$ delle matrici 2×2 e il sottoinsieme $U = \left\{ \begin{pmatrix} 0 & a \\ b & a + b \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$. Proviamo che U è un sottospazio di $\mathcal{M}_2$:

- $\begin{pmatrix} 0 & a_1 \\ b_1 & a_1 + b_1 \end{pmatrix} + \begin{pmatrix} 0 & a_2 \\ b_2 & a_2 + b_2 \end{pmatrix} = \begin{pmatrix} 0 & a_1 + a_2 \\ b_1 + b_2 & (a_1 + b_1) + (a_2 + b_2) \end{pmatrix} \in U$
- $r \begin{pmatrix} 0 & a \\ b & a + b \end{pmatrix} = \begin{pmatrix} 0 & ra \\ rb & ra + rb \end{pmatrix} \in U$

Interpretazione geometrica

Abbiamo già visto nell'ultimo capitolo che gli elementi di $\mathbb{R}^2$ possono essere visti come dei punti nel piano cartesiano.

Proprietà 7.1.14. *Se U è un sottospazio di $\mathbb{R}^2$ allora vale una delle seguenti condizioni:*

- *$U = \{(0,0)\}$ cioè U è formato solo dal vettore nullo (origine degli assi).*
- *U è una retta che passa per l'origine degli assi;*
- *$U = \mathbb{R}^2$.*

Esempio 7.1.15. L'insieme $U = \{(x,0) \mid x \in \mathbb{R}\}$ è un sottospazio di $\mathbb{R}^2$ e coincide con l'asse orizzontale (quindi è una retta). L'insieme $\{(x,3x) \mid x \in \mathbb{R}\}$ è ancora un sottospazio ed è la retta di equazione $y = 3x$. L'insieme $\{(x,x+1) \mid x \in \mathbb{R}\}$ è una retta, ma non è un sottospazio perché non è una retta che passa per l'origine degli assi, cioè il punto $(0,0)$ non vi appartiene. Provare a disegnare il grafo di queste tre rette.

Analogamente per i sottospazi di $\mathbb{R}^3$ vale la seguente proprietà:

Proprietà 7.1.16. *Se U è un sottospazio di $\mathbb{R}^3$ allora vale una delle seguenti condizioni:*

- *$U = \{(0,0,0)\}$ cioè U è formato solo dal vettore nullo (origine degli assi).*
- *U è una retta che passa per l'origine degli assi;*
- *U è un piano che passa per l'origine degli assi;*
- *$U = \mathbb{R}^3$.*

Esempio 7.1.17. L'insieme $U = \{(x,0) \mid x \in \mathbb{R}\}$ è un sottospazio di $\mathbb{R}^2$ e coincide con l'asse orizzontale (quindi è una retta). L'insieme $\{(x,3x) \mid x \in \mathbb{R}\}$ è ancora un sottospazio ed è la retta di equazione $y = 3x$. L'insieme $\{(x,x+1) \mid x \in \mathbb{R}\}$ è una retta, ma non è un sottospazio perché non è una retta che passa per l'origine degli assi, cioè il punto $(0,0)$ non vi appartiene.

L'insieme $U = \{(x,0,z) \mid x,z \in \mathbb{R}\}$ è un sottospazio di $\mathbb{R}^3$ che corrisponde al piano formato da tutti i punti dello spazio che hanno seconda coordinata uguale a 0. Invece l'insieme $\{(x,0,x) \mid x \in \mathbb{R}\}$ è ancora un sottospazio di $\mathbb{R}^3$ ma corrisponde ad una retta che giace nel piano U. L'insieme $U = \{(x,x+1,x) \mid x \in \mathbb{R}^3\}$ non è un sottospazio.

Ripetiamo alcune definizioni già date in precedenza.

Definizione 7.1.18. Una *combinazione lineare* dei vettori $v_1,\dots,v_n \in V$ tramite gli scalari $r_1,\dots,r_n \in \mathbb{R}$ è il vettore $v_1 \cdot r_1 + \cdots + v_n \cdot r_n \in V$.

Diciamo che v_1 dipende linearmente dai vettori $v_2,\dots,v_n \in V$ se esistono $s_2,\dots,s_n \in \mathbb{R}$ tali che $v_1 = s_2 \cdot v_2 + \cdots + s_n \cdot v_n$.

In particolare le combinazioni lineari di un solo vettore v sono i vettori $r \cdot v$ con $r \in \mathbb{R}$.

Esempio 7.1.19. In $\mathbb{R}^2$ un esempio di combinazione lineare è $2(2,3)+3(1,0) = (4,6)+(3,0) = (7,6)$. Quindi $(7,6)$ è combinazione lineare di $(2,3)$ e $(1,0)$ tramite gli scalari 2 e 3, e cioè $(7,6)$ dipende linearmente da $(2,3)$ e $(1,0)$.

Definizione 7.1.20. Un insieme di vettori X è *linearmente indipendente* se nessun vettore di X è combinazione degli altri. Questo è equivalente a dire che l'unica combinazione lineare dei vettori che è uguale al vettore nullo, è quella in cui tutti gli scalari sono uguali a 0. Cioè, se $r_1 \cdot v_1 + \cdots + r_n \cdot v_n = \mathbf{0}_V$ allora deve essere necessariamente che $r_i = 0$ per ogni $i = 1, \ldots, n$.

Esempio 7.1.21. Proviamo che in $\mathbb{R}^2$ i vettori $(2,3)$ e $(1,0)$ sono linearmente indipendenti. Infatti se supponiamo che

$$r(2,3) + s(1,0) = (0,0)$$

allora dovrebbe essere

$$\begin{cases} 2r + s = 0 \\ 3r = 0 \end{cases}$$

e questo è un sistema lineare omogeneo che ha come unica soluzione $r = 0$ e $s = 0$. D'altra parte, non posso scrivere $(2,3)$ come combinazione lineare di $(1,0)$ perché le combinazioni lineari di $(1,0)$ sono $(r,0)$ con $r \in \mathbb{R}$ e $(2,3) \neq (r,0)$.

Dall'esempio precedente è chiaro che c'è una correlazione tra indipendenza lineare dei vettori, sistemi di equazioni lineari e quindi matrici associate. Vale infatti il seguente risultato.

Proprietà 7.1.22. *m vettori di $\mathbb{R}^n$ sono linearmente indipendenti se la matrice $m \times n$ ottenuta considerando i vettori come righe, ha rango m.*

Esempio 7.1.23. Per capire se i vettori $(1,2)$,$(2,1)$,$(1,1)$ sono indipendenti ($m = 3$, $n = 2$) considero la matrice

$$\begin{pmatrix} 1 & 2 \\ 2 & 1 \\ 1 & 1 \end{pmatrix} \in M_{32}$$

che ha rango 2. Quindi i vettori non sono indipendenti. D'altra parte se considero una combinazione lineare dei tre vettori uguale al vettore nullo ottengo:

$$r(1,2) + s(2,1) + t(1,1) = (0,0)$$

che diventa il sistema

$$\begin{cases} r + 2s + t = 0 \\ 2r + s + t = 0 \end{cases}$$

che ha ∞^1 soluzioni, quindi non vale solo quando gli scalari sono uguali a zero. Per esempio

$$-(1,2)-(2,1)+3(1,1)=(0,0).$$

Proprietà 7.1.24. *In $\mathbb{R}^n$ ci possono essere al più n vettori linearmente indipendenti, dato che una matrice $A \in M_{mn}$ ha rango minore o uguale a* $\min(m,n)$.

Quindi per esempio se considero tre vettori in $\mathbb{R}^2$ questi non potranno mai essere linearmente indipendenti, così come 4 o 5 vettori in $\mathbb{R}^3$ e così via. D'altra parte, non è detto che due vettori in $\mathbb{R}^2$ siano sempre indipendenti. Per esempio $(1,2)$ e $(2,4)$ sono due vettori di $\mathbb{R}^2$ che non sono linearmente indipendenti.

Esempio 7.1.25. Consideriamo i vettori $(1,1,2,0,1)$, $(2,0,0,0,1)$, $(1,0,0,0,1)$, $(0,1,1,1,0)$, $(1,0,1,-1,1)$ di $\mathbb{R}^5$. Sono indipendenti? La matrice corrispondente è:

$$\begin{pmatrix} 1 & 1 & 2 & 0 & 1 \\ 2 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & -1 & 1 \end{pmatrix} \in M_{55}$$

per calcolare il rango procediamo con la riduzione a scala:

$$r_4 \leftrightarrow r_2 \quad \begin{pmatrix} 1 & 1 & 2 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 2 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & -1 & 1 \end{pmatrix} \qquad \begin{matrix} r_3 \to r_3 - r_1 \\ r_4 \to r_4 - 2r_1 \\ r_5 \to r_5 - r_1 \end{matrix} \quad \begin{pmatrix} 1 & 1 & 2 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & -1 & -2 & 0 & 0 \\ 0 & -2 & -4 & 0 & -1 \\ 0 & -1 & -1 & -1 & 0 \end{pmatrix}$$

$$\begin{matrix} r_3 \to r_3 + r_2 \\ r_4 \to r_4 + 2r_2 \\ r_5 \to r_5 + r_2 \end{matrix} \quad \begin{pmatrix} 1 & 1 & 2 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & -1 & 1 & 0 \\ 0 & 0 & -2 & 2 & -1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \qquad r_4 \to r_4 - 2r_3 \quad \begin{pmatrix} 1 & 1 & 2 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

La matrice ha quindi $rg = 4$, allora non tutti i vettori sono indipendenti ma solo 4.

Definizione 7.1.26. Sia $S \subseteq V$ un sottoinsieme dello spazio V. Il sottospazio di V **generato** da S è l'insieme $< S >$ formato dalle combinazioni lineari degli elementi di S. In questo caso si dice che S è l'*insieme di generatori* di $< S >$.

Nota che il sottospazio generato da un insieme S è sempre un sottospazio dello spazio vettoriale di partenza.

Esempio 7.1.27. In $\mathbb{R}^3$ consideriamo $S = \{(2,1,0),(1,0,1)\}$. $< S >$ è l'insieme delle combinazioni lineari di $(2,1,0)$ e $(1,0,1)$, cioè $< S >= \{r(2,1,0)+s(1,0,1) \mid$

$r, s \in \mathbb{R}\} = \{(2r, r, 0) + (s, 0, s) \mid r, s \in \mathbb{R}\} = \{(2r + s, r, s) \mid r, s \in \mathbb{R}\}$. Nota che $< S > \neq \mathbb{R}^3$ cioè $< S >$ non contiene tutti gli elementi di $\mathbb{R}^3$: infatti $(3, 1, 1)$, $(2, 1, 0)$, $(1, 0, 1) \in < S >$ ma $(3, 1, 0) \notin < S >$.

Esempio 7.1.28. $S = \{(2, 2), (1, 0)\} \subseteq \mathbb{R}^2$. Lo spazio generato è $< S >= \{r(2, 2) + s(1, 0) \mid r, s \in \mathbb{R}\} = \{(2r, 2r) + (s, 0) \mid r, s \in \mathbb{R}\} = \{(2r, 2r) \mid r, s \in \mathbb{R}\}$. In questo caso $< S >= \mathbb{R}^2$. Infatti tutti i vettori di $\mathbb{R}^2$ si possono scrivere come $(2r, 2s)$ (ricordiamo che r e s sono numeri reali). Per esempio $(3, 2) \in < S >$ ponendo $r = 3/2, s = 1$, $(1, 0) \in < S >$ ponendo $r = 1, s = 0$, $(7, 6) \in < S >$ con $r = 7/2, s = 3$ e così via.

7.1.1 Basi di spazi vettoriali

Definizione 7.1.29. Una **base** per uno spazio vettoriale V, è un insieme di vettori linearmente indipendenti (diversi dal vettore nullo) tali che $< B >= V$ (cioè B genera V). Uno spazio può avere più basi diverse, ma le basi di uno stesso spazio hanno sempre lo stesso numero di elementi.

Definizione 7.1.30. La **dimensione** di uno spazio vettoriale V è il numero di elementi di una base di V e si indica con $\dim V$ (è sempre un numero intero).

La dimensione di V è quindi il numero di vettori di una sua base ed è il massimo numero di vettori linearmente indipendenti che ci possono essere in V.

Nota che se uno spazio vettoriale è formato solo dal vettore nullo, cioè se $V = \{0_V\}$ allora non ha generatori diversi dall'insieme nullo e quindi diciamo che ha dimensione uguale a 0. In particolare $\dim V = 0$ se e solo se $V = \{0_V\}$.

Esempio 7.1.31. In $\mathbb{R}^2$ ci sono al più 2 vettori linearmente indipendenti, quindi una base non può avere più di due elementi. Un esempio di base di $\mathbb{R}^2$ è $E = \{(1, 0), (0, 1)\}$. Infatti i vettori di E sono linearmente indipendenti e lo spazio generato è

$$< E >= \{r(1, 0) + s(0, 1) \mid r, s \in \mathbb{R}\} = \{(r, s) \mid r, s \in \mathbb{R}\} = \mathbb{R}^2$$

quindi E genera $\mathbb{R}^2$ e E è una base di $\mathbb{R}^2$. Quindi $dim\mathbb{R}^2 = 2$.

Esiste un insieme di due vettori che non forma una base di $\mathbb{R}^2$? Sì, un insieme di vettori linearmente dipendenti, come $\{(1, 1), (2, 2)\}$.

Proprietà 7.1.32. *Un insieme di n vettori linearmente indipendenti di $\mathbb{R}^n$ è sempre una base, quindi per ogni $n \in \mathbb{N}$, $\dim R^n = n$.*

Ricordiamo anche che per controllare che n vettori siano linearmente indipendenti considero la matrice formata dagli n vettori e verifico che abbia rango n.

Esempio 7.1.33. L'insieme $\{(1,0,1),(0,0,1),(0,1,1)\}$ è una base di $\mathbb{R}^3$. Infatti

$$det\begin{pmatrix}1&0&1\\0&0&1\\0&1&1\end{pmatrix} = -1 \neq 0$$

quindi i tre vettori sono indipendenti.

Definizione 7.1.34. Per ogni $n > 0$, l'insieme E_n formato dagli n vettori di $\mathbb{R}^n$ che hanno una sola componente uguale a 1 e le altre uguali a 0, è una base di $\mathbb{R}^n$ che si chiama *base canonica*. In particolare, $E_2 = \{(1,0),(0,1)\}$ e $E_3 = \{(1,0,0),(0,1,0),(0,0,1)\}$. Nota che la matrice formata dagli n vettori di E_n è la matrice identica.

Proprietà 7.1.35. *Se B è una base di V allora i vettori di V sono combinazione lineare degli elementi di B e la combinazione lineare è unica.*

Definizione 7.1.36. Sia $B = \{b_1,\dots,b_n\}$ una base di uno spazio V di dimensione n. Allora per ogni vettore $u \in V$ esistono (e sono unicamente determinati) degli scalari $k_1,\dots,k_n$ tali che $u = k_1b_1 + \cdots + k_nb_n$. Denotiamo con

$$[u]_B = (k_1,\dots,k_n)$$

le componenti di u rispetto a B. Nota che se $V = \mathbb{R}^n$ e denotiamo con B la matrice formata dai vettori $b_1,\dots,b_n$ si ha che $u = B^T \cdot [u]_B$.

Esempio 7.1.37. Consideriamo $B = \{(1,1),(2,1)\}$. B è una base di $\mathbb{R}^2$ perché è formata da due vettori linearmente indipendenti (provare che la matrice formata dai due vettori ha rango 2). Consideriamo il vettore $u = (1,2) \in \mathbb{R}^2$ e scriviamolo come combinazione lineare degli elementi di B. Dobbiamo quindi trovare gli scalari a, b tali che

$$(1,2) = a(1,1) + b(2,1)$$

e cioè la soluzione del sistema

$$\begin{cases} a + 2b = 1 \\ a + b = 2 \end{cases}$$

che è $(3,-1)$. Quindi $[(1,2)]_B = (3,-1)$.

Esempio 7.1.38. Dimostriamo che $B = \{(2,1,0),(3,0,1),(1,1,1)\}$ è una base di $\mathbb{R}^n$ e calcoliamo $[(1,2,3)]_B$, cioè le componenti del vettore $(1,2,3)$ rispetto alla base B. Dobbiamo verificare che i vettori di B siano linearmente indipendenti calcolando il rango della matrice

$$\begin{pmatrix}2&1&0\\3&0&1\\1&1&1\end{pmatrix}.$$

Dato che il determinante è $-4 \neq 0$, il rango è 3 e quindi i vettori sono linearmente indipendenti. (Nota che un insieme di vettori di $\mathbb{R}^3$ che non contiene esattamente tre vettori sicuramente non è una base).

Scriviamo allora il vettore $(1,2,3)$ come combinazione lineare degli elementi della base:

$$\begin{aligned}(1,2,3) &= a(2,1,0)+b(3,0,1)+c(1,1,1)\\ (1,2,3) &= (2a,a,0)+(3b,0,b)+(c,c,c)\\ (1,2,3) &= (2a+3b+c, a+c, b+c).\end{aligned}$$

Ho quindi il sistema

$$\begin{cases} 2a+3b+c=1\\ a+c=2\\ b+c=3\end{cases}$$

che ha come matrice dei coefficienti, la trasposta della matrice formata dai vettori di B. Quindi ha rango 3 e il sistema ha una sola soluzione. Questa unica soluzione corrisponde all'unico valore che posso dare agli scalari a, b e c per scrivere la combinazione lineare. Per trovare tali valori posso usare il metodo di Cramer.

$$A_a = \begin{pmatrix}1&3&1\\2&0&1\\3&1&1\end{pmatrix} \qquad det(A_a) = -2\begin{vmatrix}3&1\\1&1\end{vmatrix} - 1\begin{vmatrix}1&3\\3&1\end{vmatrix} = -4+8=4$$

$$a = \frac{det(A_a)}{det(A)} = \frac{4}{-4} = -1$$

$$A_b = \begin{pmatrix}2&1&1\\1&2&1\\0&3&1\end{pmatrix} \qquad det(A_b) = -3\begin{vmatrix}2&1\\1&1\end{vmatrix} + \begin{vmatrix}2&1\\1&2\end{vmatrix} = -3+3=0 \Rightarrow b=0$$

$$A_c \begin{pmatrix}2&3&1\\1&0&2\\0&1&3\end{pmatrix} \qquad det(A_c) = -\begin{vmatrix}2&1\\1&2\end{vmatrix} + \begin{vmatrix}2&3\\1&0\end{vmatrix} = -3-9=-12$$

$$c = \frac{det(A_c)}{det(A)} = \frac{-12}{-4} = 3$$

Quindi l'unica soluzione è $(-1,0,3)$ e infatti

$$(1,2,3) = -(2,1,0)+3(1,1,1)\,.$$

Si ha quindi $[(1,2,3)]_B = (-1,0,3)$ e infatti $B^T \cdot [u]_B = u$:

$$\begin{pmatrix}2&3&1\\1&0&1\\0&1&1\end{pmatrix} \cdot \begin{pmatrix}-1\\0\\3\end{pmatrix} = \begin{pmatrix}1\\2\\3\end{pmatrix}$$

Esercizio 7.1.39. Scrivere $(1,0)$ come combinazione lineare di $\{(1,2),(2,1),(0,1)\}$. In quanti modi si può fare?

Se consideriamo la base canonica $E_n = \{(1,0,\dots,0),(0,1,\dots,0),\dots,(0,\dots,0,1)\}$ di $\mathbb{R}^n$ allora si ha che per ogni vettore $u \in \mathbb{R}^n$, $[u]_{E_n} = u$ cioè le componenti nella base canonica sono le componenti stesse del vettore.

Esempio 7.1.40. Per $n = 2$ si ha $E_2 = \{(1,0),(0,1)\}$. Consideriamo $u = (2,1)$ e scriviamo u come combinazione lineare degli elementi di E_2:

$$(2,1) = a(1,0) + b(0,1) = (a,b)$$

quindi l'unica soluzione è $a = 2$ e $b = 1$, cioè $[u]_{E_2} = u$.

Da un punto di vista dell'interpretazione geometrica, cambiare base vuol dire cambiare il sistema di riferimento. Infatti le rette sui cui giacciono i vettori di una base possono considerarsi come degli assi di riferimento (non necessariamente perpendicolari tra di loro) e i vettori di tale base determinaranno l'unità di misura su ognuno di questi nuovi assi. Le coordinate di un vettore u rispetto ad una base B sono quindi le proiezioni rispetto a tale base: in genere non saranno proiezioni ortogonali ma rispetto agli angoli determinati dai nuovi assi, seguendo la regola del parallelogramma.

Esempio 7.1.41. Sia $B = \{(1,2),(0,1)\}$ e consideriamo il vettore $u = (-1,2)$. Si ha $[(-1,2)]_B = (-1,4)$. I vettori di B giacciono sulle rette di equazione $y = 2x$ e $x = 0$, quindi possiamo considerare queste due rette come nuovo riferimento e rispetto a tali rette il punto $(-1,2)$ ha coordinate $(-1,4)$, cioè è la somma di $-b_1$ e di $4b_2$. In Figura 7.1 le proiezioni sono indicate dai vettori v e w.

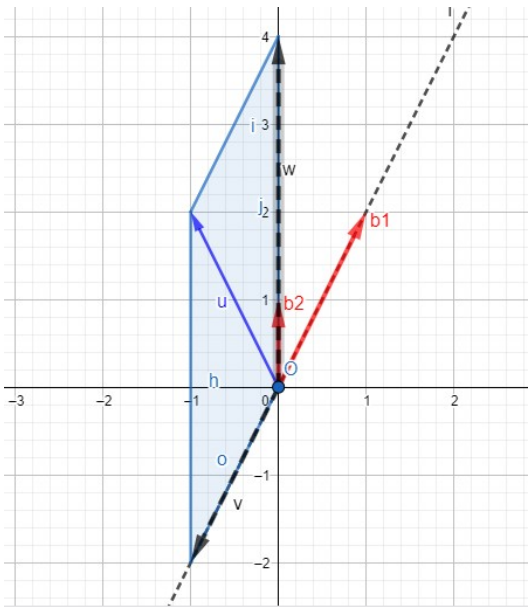


Figura 7.1: Cambio di base

Matrice di cambiamento di base

Se uno spazio vettoriale V ha due basi $B = \{b_1, \dots, b_n\}$ e $C = \{c_1, \dots, c_n\}$ allora ogni vettore di B si può scrivere come combinazione lineare dei vettori di C (e viceversa). La matrice P_{BC} che ha come colonne i vettori $[b_i]_C$, cioè le componenti di b_i nella base C, si chiama **matrice di cambiamento di base** da B a C. Per ogni vettore $u \in \mathbb{R}^2$ si ha che

$$[u]_C = P_{BC} \cdot [u]_B$$

quindi la matrice serve per trasformare le coordinate in B in coordinate in C. Nota che una matrice di cambiamento di base ha sempre determinante diverso da zero, è quindi invertibile e vale

$$[u]_B = P_{BC}^{-1}[u]_C$$

cioè la matrice di cambiamento dalla base C alla base B è l'inversa della matrice di cambiamento dalla base B alla base C: $P_{CB} = P_{BC}^{-1}$.

Esempio 7.1.42. Consideriamo le basi $B = \{(1,2),(1,0)\}$ e $C = \{(2,1),(1,1)\}$ di $\mathbb{R}^2$. Dato che

$(1,2) = -1(2,1) + 3(1,1)$ quindi $[(1,2)]_C = (-1,3)$

$(1,0) = 1(2,1) - 1(1,1)$ quindi $[(1,0)]_C = (1,-1)$

allora la matrice

$$P_{BC} = \begin{pmatrix} -1 & 1 \\ 3 & -1 \end{pmatrix}$$

è la matrice di cambiamento dalla base B alla base C. Nota che il vettore $(1,1)$ è tale che $[(1,1)]_C = (0,1)$ e $[(1,1)]_B = (1/2, 1/2)$ e infatti

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -1 & 1 \\ 3 & -1 \end{pmatrix} \begin{pmatrix} 1/2 \\ 1/2 \end{pmatrix}.$$

Consideriamo adesso la base canonica $E_2 = \{(1,0),(0,1)\}$. Dato che $[(1,0)]_B = (0,1)$ e $[(0,1)]_B = (1/2, -1/2)$ allora la matrice di cambiamento di base da E_2 a B è

$$P_{EB} = \begin{pmatrix} 0 & 1/2 \\ 1 & -1/2 \end{pmatrix}$$

e posso usarla per calcolare le componenti di un vettore rispetto alla base B: per esempio

$$[(1,1)]_B = \begin{pmatrix} -1 & 1 \\ 3 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1/2 \\ 1/2 \end{pmatrix}.$$

Inoltre la matrice di cambiamento di base da E_2 a C è data da $P_{EC} = P_{BC}P_{EB}$:

$$[(1,1)]_C = \begin{pmatrix} -1 & 1 \\ 3 & -1 \end{pmatrix} \begin{pmatrix} -1 & 1 \\ 3 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

7.1.2 Basi di un sottospazio

Se U è un sottospazio di V, U è anche uno spazio vettoriale e quindi può avere una base, cioè un sottoinsieme di U formato da vettori linearmente indipendenti che generano U. Se gli elementi dello spazio U sono caratterizzati da una espressione che coinvolge dei parametri, allora un metodo che possiamo utilizzare per trovare una base di U è il seguente:

- determinare da quanti parametri dipendono i vettori di U;
- considerare i vettori ottenuti ponendo uguale a 1 uno dei parametri e a 0 gli altri, in tutti i modi possibili.

Esempio 7.1.43. Consideriamo $U = \{(x_1, x_2, x_1 + x_2) \mid x_1, x_2 \in \mathbb{R}\} \subseteq \mathbb{R}^3$ e notiamo che U è un sottospazio di $\mathbb{R}^3$ poiché se $u_1, u_2 \in U$ allora $u_1 + u_2 \in U$ e $ru_1 \in U$ per ogni $r \in \mathbb{R}$. Quindi U è uno spazio vettoriale e possiamo trovare una sua base:

- i vettori di U dipendono da due parametri;
- considero i vettori ottenuti ponendo uguale a 1 uno dei parametri e uguale a 0 gli altri. Quindi $B = \{(1, 0, 1), (0, 1, 1)\}$.

Verifico che $B = \{(1, 0, 1), (0, 1, 1)\}$ è una base di U. Prima di tutto i vettori sono linearmente indipendenti perché

$$rg \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} = 2.$$

Poi devo dimostrare che B genera U, cioè che ogni vettore di U è combinazione lineare di B. E infatti per ogni $(x, y, x + y) \in U$ si ha

$$(x, y, x + y) = x(1, 0, 1) + y(0, 1, 1)$$

quindi B è una base di U.

Spazio delle soluzioni di un sistema omogeneo

Abbiamo visto che l'insieme delle soluzioni di un sistema omogeneo di equazioni lineari forma sempre uno spazio vettoriale. Per trovare una base di tale spazio possiamo considerare il numero di parametri da cui dipendono le soluzioni.

Proprietà 7.1.44. *La dimensione dello spazio delle soluzioni di un sistema omogeneo in n variabili è uguale a $n-r$, dove r è il rango della matrice dei coefficienti del sistema.*

Esempio 7.1.45. Consideriamo il sistema con 3 incognite:

$$\begin{cases} x+y=0 \\ x+z=0 \end{cases}$$

che ha matrice associata $A = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$ che ha rango $r = 2$. Quindi lo spazio delle soluzioni ha dimensione $3-2=1$ e infatti il sistema ha ∞^1 soluzioni. Lo spazio delle soluzioni è $U = \{(-z, z, z) \mid z \in \mathbb{R}\}$ (che è un sottospazio di $\mathbb{R}^3$). Troviamo una base di U: i vettori dipendono da 1 parametro quindi per $z = 1$ otteniamo la base $\{(-1, 1, 1)\}$.

Esempio 7.1.46. Trovare lo spazio delle soluzioni

$$\begin{cases} x+3y+z=0 \\ 2y+z=0 \\ 2x-z=0 \end{cases} \qquad \begin{pmatrix} 1 & 3 & 1 \\ 0 & 2 & 1 \\ 2 & 0 & -1 \end{pmatrix}$$

rango : $\begin{vmatrix} 1 & 3 \\ 0 & 2 \end{vmatrix} \neq 0$; $\begin{vmatrix} 1 & 3 & 1 \\ 0 & 2 & 1 \\ 2 & 0 & -1 \end{vmatrix} = 2\begin{vmatrix} 3 & 1 \\ 2 & 1 \end{vmatrix} - \begin{vmatrix} 1 & 3 \\ 0 & 2 \end{vmatrix} = 2-2=0$ quindi il rango della matrice è 2. Il sistema ha 3 incognite e rango 2 quindi $\infty^{3-2} = \infty^1$ soluzioni che dipendono da un parametro.

$$\begin{cases} x+3y+z=0 \\ 2y+z=0 \end{cases} \qquad \begin{cases} x-\frac{3}{2}z+z=0 \\ y=-\frac{1}{2}z \end{cases} \qquad \begin{cases} x=\frac{1}{2}z \\ y=-\frac{1}{2}z \end{cases}$$

Lo spazio delle soluzioni quindi è

$$U = \left\{ \left(\frac{1}{2}z, -\frac{1}{2}z, z \right) \mid z \in \mathbb{R} \right\} \subseteq \mathbb{R}^3$$

e $dim U = 1$. Per trovare una base di U considero il procedimento visto prima e ottengo $B = \{(\frac{1}{2}, -\frac{1}{2}, 1)\}$.

7.1.3 Prodotto scalare e basi ortonormali

Abbiamo già visto nel precedente capitolo che un vettore di $\mathbb{R}^n$ può essere rappresentato con un punto nell spazio a n dimensioni, o anche come un segmento orientato che parte dall'origine e arriva a tale punto. In particolare, se

$u = (u_1, \dots, u_n) \in \mathbb{R}^n$, la lunghezza o *norma* di u è definita (per il teorema di Pitagora) da

$$|u| = \sqrt{u_1^2 + \cdots + u_n^2} \in \mathbb{R}\,.$$

Introduciamo un'altra operazione tra vettori, che però non restituisce un vettore ma uno scalare.

Definizione 7.1.47. Dati due vettori $u = (u_1, u_2, \dots, u_n)$, $v = (v_1, v_2, \dots, v_n) \in \mathbb{R}^n$, il loro **prodotto scalare** è il numero

$$u \cdot v = \sum_{i=1}^{n} u_i \cdot v_i \in \mathbb{R}\,.$$

Diciamo che u e v sono **ortogonali** e scriviamo $u \perp v$ se il loro prodotto scalare è uguale a 0, cioè $u \cdot v = 0$.

Utilizziamo lo stesso simbolo per denotare il prodotto scalare tra vettori e il prodotto solito tra numeri. Questo non ci deve confondere, perché il tipo di prodotto è chiaro dagli argomenti che stiamo considerando, cioè se scrivo $(1, 2) \cdot (3, 2)$ è chiaro che sto facendo un prodotto tra vettori e quindi è il prodotto scalare, mentre se scrivo $2 \cdot 3$ sto facendo un prodotto tra numeri.

Nell'interpretazione geometrica il prodotto scalare si interpreta come lunghezza della proiezione di un vettore sull'altro ed è legato all'angolo α che i due vettori formano tra loro:

$$u \cdot v = |u| \cdot |v| \cdot \cos \alpha\,.$$

Nota inoltre che $|u| = \sqrt{u \cdot u}$.

Esempio 7.1.48. Se $u = (1, 2, 3)$, $v = (3, 2, 1) \in \mathbb{R}^3$ allora

$$u \cdot v = 1 \cdot 3 + 2 \cdot 2 + 3 \cdot (-1) = 3 + 4 - 3 = 4 \neq 0$$

Quindi i vettori non sono ortogonali. Si ha $|u| = \sqrt{1 + 4 + 9} = \sqrt{14}$ e $|v| = \sqrt{9 + 4 + 1} = \sqrt{14}$ quindi u e v hanno la stessa lunghezza.

Definizione 7.1.49. Una base $B = \{b_1, \dots, b_n\}$ si dice **ortonormale** se per ogni i e per ogni $j \neq i$ si ha $|b_i| = 1$ e $b_i \cdot b_j = 0$.

Esempio 7.1.50. Controlliamo se $B = \{(1, 0), (0, 4)\}$ è una base ortonormale di $\mathbb{R}^2$. Verifichiamo prima di tutto che sia una base, dato che abbiamo due vettori di $\mathbb{R}^2$ dobbiamo solo verficiare che siano indipendenti, e lo facciamo calcolando il rango della matrice

$$rg \begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix} = 2$$

quindi i vettori sono indipendenti, perciò B è una base di $\mathbb{R}^2$. Verifichiamo che sia una base ortonormale: $(1,0)\cdot(0,4) = 1\cdot 0 + 0\cdot 4 = 0+0 = 0$ quindi i vettori sono ortogonali. Calcoliamo la norma:

$$|(1,0)| = \sqrt{(1,0)\cdot(1,0)} = \sqrt{1^2+0^2} = 1$$

$$|(0,4)| = \sqrt{(0,4)\cdot(0,4)} = \sqrt{0^2+4^2} = 4 \neq 1$$

dato che il secondo vettore non ha norma uguale a 1, la base B non è ortonormale. Nota che se invece considero $\{(1,0),(0,1)\}$ questa è una base ortonormale.

Procedimento di ortogonalizzazione di Gram-Schmidt

Data una base $B = \{b_1,\dots,b_n\}$ possiamo ottenere una base ortonormale con il seguente procedimento: poniamo $u_1 = b_1$ e per ogni $k = 2,\dots,n$:

$$u_k = b_k - \sum_{j=1}^{k-1} \frac{b_k\cdot u_j}{u_j\cdot u_j} u_j\,.$$

Allora l'insieme $\{u_1/|u_1|\dots,u_n/|u_n|\}$ è una base ortonormale.

ESEMPI

Esistono altri due tipi di prodotto tra vettori, il prodotto vettoriale (che restituisce un vettore) e il prodotto misto (che restituisce uno scalare). Diamo la definizione solo nel caso $n = 3$.

Definizione 7.1.51. Siano $u = (u_1,u_2,u_3)$ e $v = (v_1,v_2,v_3) \in \mathbb{R}^3$, il **prodotto vettoriale** $u \times v$ è il vettore

$$(u_2\cdot v_3 - u_3\cdot v_2, -u_1\cdot v_3 + u_3\cdot v_1, u_1\cdot v_2 - u_2\cdot v_1)\,.$$

Per ricordare tale formula, si può considerare la matrice formata dai due vettori. Le coordinate del prodotto vettoriale saranno i determinanti delle tre sottomatrici 2×2 ottenute cancellando di volta in volta la prima, la seconda e la terza riga.

$$\begin{pmatrix} u_1 & u_2 & u_3 \\ v_1 & v_2 & v_3 \end{pmatrix}$$

Definizione 7.1.52. Il **Prodotto Misto** di tre vettori in $\mathbb{R}^3$ è il determinante della matrice ottenuta considerando i tre vettori come righe.

$$(u\times v)\cdot w = det\begin{pmatrix} u \\ v \\ w \end{pmatrix}$$

e quindi è anche uguale al volume del parallelepipedo formato dai tre vettori (con un segno più o meno che dipende da come sono orientati i vettori tra di loro, tralasciamo questo argomento).

Esempio 7.1.53. Con $n = 3$ consideriamo i vettori $u = (1, 2, 3)$, $v = (1, 0, 1)$ e $w = (0, 1, 2)$.

- $u \cdot v =$ prodotto scalare $= 1 \cdot 1 + 2 \cdot 0 + 3 \cdot 1 = 1 + 0 + 3 = 4$
- $u \times v =$ prodotto vettoriale $= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 0 & 1 \end{pmatrix} \to \begin{pmatrix} 2 \\ +2 \\ -2 \end{pmatrix}$
- $(u \times v) \cdot w =$ prodotto misto $= det \begin{pmatrix} 1 & 2 & 3 \\ 1 & 0 & 1 \\ 0 & 1 & 2 \end{pmatrix} = - \begin{vmatrix} 2 & 3 \\ 1 & 2 \end{vmatrix} - \begin{vmatrix} 1 & 2 \\ 0 & 1 \end{vmatrix} = -1 - 1 = -2$

7.2 Applicazioni Lineari

Definizione 7.2.1. Se U e V sono spazi vettoriali, $f : U \to V$ è un'applicazione lineare se:

- $f(u_1 + u_2) = f(u_1) + f(u_2)$
- $f(r \cdot u) = r \cdot f(u)$

Nota: se f è una applicazione lineare allora

- $f(r_1 \cdot u_1 + \cdots + r_n \cdot u_n) = r_1 \cdot f(u_1) + \cdots + r_n \cdot f(u_n)$;
- $f(0_U) = 0_V$.

Esempio 7.2.2. Sia $U = \mathbb{R}^3$ e $V = \mathbb{R}^2$ e consideriamo $f : \mathbb{R}^3 \to \mathbb{R}^2$ tale che $f(x, y, z) = (x, y + z)$. Quindi per esempio $f(1, 0, 1) = (1, 1)$; $f(2, 1, 1) = (2, 2)$; $f(0, 0, 1) = (0, 1)$. Proviamo che f è un'applicazione lineare.

- $f((x_1, y_1, z_1) + (x_2, y_2, z_2)) = f(x_1, y_1, z_1) + f(x_2, y_2, z_2)$?

  Si ha $f((x_1, y_1, z_1) + (x_2, y_2, z_2)) = f(x_1 + x_2, y_1 + y_2, z_1 + z_2) = (x_1 + x_2, y_1 + y_2 + z_1 + z_2) = (x_1, y_1 + z_1) + (x_2, y_2 + z_2) = f(x_1, y_1, z_1) + f(x_2, y_2, z_2)$ quindi la prima condizione è verificata.

- $f(r(x, y, z)) = r \cdot f(x, y, z)$?

  Si ha $f(r(x, y, z)) = f(rx, ry, rz) = (rx, ry + rz) = r(x, y + z) = rf(x, y, z)$ quindi anche la seconda condizione è verificata.

Perciò f è un'applicazione lineare.

Definizione 7.2.3. Data una applicazione lineare $f : U \to V$, l'**immagine** di f è l'insieme

$$\text{Im } f = \{f(u) \mid u \in U\} = \{v \in V \mid \text{ esiste } u \in U \text{ tale che } f(u) = v\} \subseteq V\,.$$

Si ha che Im f è un sottospazio di V. Infatti per ogni $v_1, v_2 \in \text{Im } f$ si ha che $v_1 = f(u_1)$ e $v_2 = f(u_2)$, quindi $v_1 + v_2 = f(u_1) + f(u_2) = f(u_1 + u_2) \in Im\, f$ e $r \cdot v_1 = r \cdot f(u_1) = f(r \cdot u_1) \in \text{Im } f$.

Esempio 7.2.4. Consideriamo $f : \mathbb{R}^4 \to \mathbb{R}^3$ tale che $f(x_1, x_2, x_3, x_4) = (x_1, 0, x_2)$. Allora:

$$\text{Im } f = \{f(x_1, x_2, x_3, x_4) \mid x_1, x_2, x_3, x_4 \in \mathbb{R}\} = \{(x_1, 0, x_2) \mid x_1, x_2 \in \mathbb{R}\}$$

che è un sottospazio di $\mathbb{R}^3$. Inoltre dim Im $f = 2$ perché i vettori di $Im f$ dipendono da due parametri indipendenti. Una base di Im f è $B = \{(1, 0, 0), (0, 0, 1)\}$.

Esempio 7.2.5. Sia $f : \mathbb{R}^3 \to \mathbb{R}^2$ tale che $f(x, y, z) = (x, y + z)$. Allora:

$$\text{Im } f = \{f(x, y, z) \mid x, y, z \in \mathbb{R}\} = \{(x, y + z) \mid x, y, z \in \mathbb{R}\} = \mathbb{R}^2\,.$$

L'applicazione f è quindi suriettiva e $dim(\text{Im } f) = 2$.

Definizione 7.2.6. Se $f : U \to V$ è un'applicazione lineare, il **nucleo** o **kernel** di f è l'insieme Ker $f = \{u \in U \mid f(u) = 0_V\} \subseteq U$.

Notiamo che Ker f è un sottospazio di U. Infatti se $u_1, u_2 \in Ker\, f$ allora $f(u_1 + u_2) = f(u_1) + f(u_2) = 0_V + 0_V = 0_V$ quindi anche $u_1 + u_2 \in \text{Ker } f$. Inoltre $f(r \cdot u_1) = rf(u_1) = r0_V = 0_V$ quindi anche $r \cdot u_1 \in Ker\, V$.

D'altra parte il kernel di una applicazione lineare di $\mathbb{R}^n$ in $\mathbb{R}^m$ è l'insieme delle soluzioni di un sistema omogeneo con m equazioni e n incognite, ottenuto ponendo uguali a zero le componenti delle immagini degli elementi del dominio. E' quindi un sottospazio del dominio dell'applicazione.

Esempio 7.2.7. Sia $f : (x, y, z) \in \mathbb{R}^3 \to (x, y + z) \in \mathbb{R}^2$.

$$\text{Ker } f = \{(x, y, z) \in \mathbb{R}^3 \mid (x, y + z) = (0, 0)\}$$

quindi Ker f è l'insieme delle soluzioni del sistema omogeneo $\begin{cases} x = 0 \\ y + z = 0 \end{cases}$ che ha ∞^1 soluzioni e cioè Ker $f = \{(0, -z, z) \mid z \in \mathbb{R}\}$. In particolare si ha che Ker f è un sottospazio di $\mathbb{R}^3$ di dimensione 1 che ha come base $\{(0, -1, 1)\}$.

Esempio 7.2.8. Sia $f(x_1, x_2, x_3, x_4) = (x_1, 0, x_2) \in \mathbb{R}^3$. Allora:

$$\begin{aligned} Ker\, f &= \{(x_1, x_2, x_3, x_4) \in \mathbb{R}^4 \mid f(x_1, x_2, x_3, x_4) = (0, 0, 0)\} = \\ &= \{(x_1, x_2, x_3, x_4) \mid (x_1, 0, x_2) = (0, 0, 0)\} = \\ &= \{(0, 0, x_3, x_4) \mid x_3, x_4 \in \mathbb{R}\} \end{aligned}$$

Quindi Ker f è un sottospazio di $\mathbb{R}^4$ e $\dim(\text{Ker } f) = 2$; una base è $B = \{(0, 0, 1, 0), (0, 0, 0, 1)\}$.

Teorema 7.2.9. *Se $f : U \to V$ è un'applicazione lineare allora*

$$\dim(\text{Im } f) + \dim(\text{Ker } f) = \dim U\,.$$

Proprietà 7.2.10. *Data una applicazione lineare $f : \mathbb{R}^n \to \mathbb{R}^m$, si ha che:*
f è iniettiva se e solo se $\dim \text{Ker } f = 0$;
f è suriettiva se e solo se $\dim \text{Im } f = m$.
Quindi f è biettiva se e solo se $m + 0 = n$ e cioè $n = m = \dim \text{Im } f$.

Esempio 7.2.11. Sia $f : (x, y, z) \in \mathbb{R}^3 \to (x, y + z) \in \mathbb{R}^2$. Dato che $\text{Im } f = \{(x, y + z) \mid x, y, z \in \mathbb{R}\} = \mathbb{R}^2$ e $\text{Ker } f = \{(0, -z, z) \mid z \in \mathbb{R}\}$ allora $\dim \text{Im } f = 2$ e $\dim \text{Ker } f = 1$. Si ha $\dim \text{Im } f + \dim \text{Ker } f = \dim \mathbb{R}^3 = 3$.

Esempio 7.2.12. Sia $f : \mathbb{R}^3 \to \mathbb{R}^2$ con $f(x, y, z) = (2x + z, y)$. Calcoliamo $\text{Im } f$, $\dim \text{Ker } f$, $\dim \text{Im } f$, considerando che $\dim \mathbb{R}^3 = 3$. Si ha:

$$\text{Im } f = \{f(x, y, z) \mid x, y, z \in \mathbb{R}\} = \{(2x + z, y) \mid x, y, z \in \mathbb{R}\} \subseteq \mathbb{R}^2$$

quindi $\dim \text{Im } f = 2$ (e cioè $\text{Im } f = \mathbb{R}^2$). Inoltre:

$$\begin{aligned} \text{Ker } f &= \{(x, y, z) \in \mathbb{R}^3 \mid f(x, y, z) = 0\} = \\ &= \{(x, y, z) \in \mathbb{R}^3 \mid (2x + z, y) = (0, 0)\} \end{aligned}$$

quindi gli elementi di Ker f sono le soluzioni del sistema

$$\begin{cases} 2x + z = 0 \Rightarrow z = -2x \\ y = 0 \end{cases}$$

e cioè $\text{Ker } f = \{(x, 0, -2x) \mid x \in \mathbb{R}\}$. Quindi $\dim \text{Ker } f = 1$.

Esempio 7.2.13. Sia $f : \mathbb{R}^3 \to \mathbb{R}^3$ con $f(x, y, z) = (x + y, 0, y + z)$. Calcoliamo $\dim \text{Ker } f$ e $\dim \text{Im } f$.

$$\text{Im } f = \{(x + y, 0, y + z) \mid x, y, z \in \mathbb{R}\} \subseteq \mathbb{R}^2\,.$$

Notiamo che anche se $Im\, f$ sembra dipendere da tre parametri, in realtà la prima e la terza componente dei vettori di Im f possono essere qualsiasi, quindi Im $f =$

$\{(a,0,b) \mid a,b \in \mathbb{R}\}$ e $\dim \operatorname{Im} f = 2$. Infatti una base di $\operatorname{Im} f$ è $\{(1,0,0),(0,0,1)\}$. Possiamo quindi dedurre che $\dim \operatorname{Ker} f = 1$. Infatti,

$$\operatorname{Ker} f = \{(x,y,z) \in \mathbb{R}^3 | (x+y, 0, y+z) = (0,0,0)\}$$

quindi $Ker\, f$ è l'insieme delle soluzioni del sistema omogeneo $\begin{cases} x+y=0 \\ 0=0 \\ y+z=0 \end{cases}$ e quindi è uguale a $\{(-y,y,-y)|y \in \mathbb{R}\}$ e $\dim \operatorname{Ker} f = 1$. Dato che $\dim \operatorname{Ker} f = 1$ allora f non è iniettiva e dato che $\dim \operatorname{Im} f = 2$ allora f non è suriettiva.

Definizione 7.2.14. Data una applicazione lineare $f : U \to V$, se S è un sottospazio di U, allora $f(S)$ è un sottospazio di V e $\dim f(S) \leq \dim S$.

Quindi, ricordando come sono fatti i sottospazi di $\mathbb{R}^n$, le applicazioni lineari possono mandare una retta ~~in~~ un punto o una retta, ma non in un piano.

Esempio 7.2.15. Sia $f : \mathbb{R}^2 \to \mathbb{R}^2$ con $f(x,y) = (2y,x)$ e consideriamo il sottospazio $S = \{(x,2x) \mid x \in \mathbb{R}\}$ di $\mathbb{R}^2$ che ha dimensione 1 (è la retta di equazione $y = 2x$). Allora $f(S) = \{f(x,2x) \mid x \in \mathbb{R}\} = \{(4x,x) \mid x \in \mathbb{R}\}$ quindi $f(S)$ ha ancora dimensione 1 ed è quindi una retta (di equazione $y = x/4$). Una rappresentazione di queste rette nel piano cartesiano è data nella Figura 7.2.

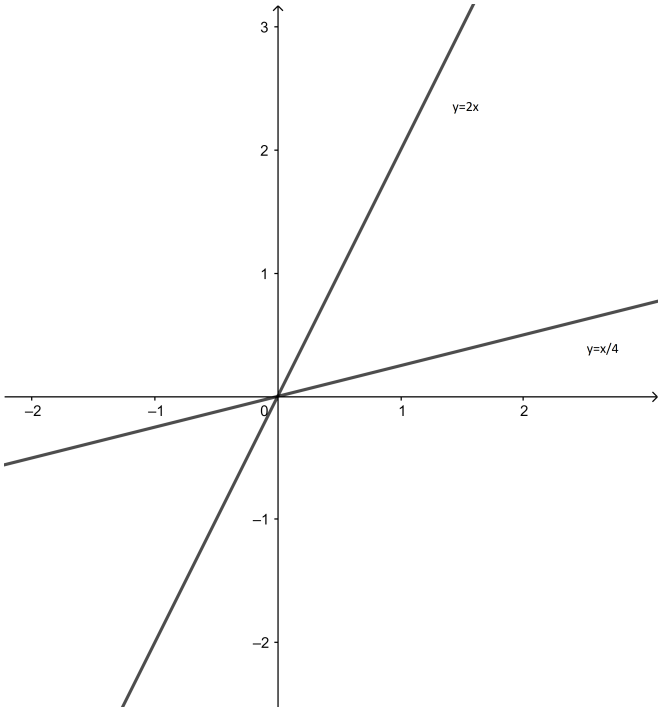


Figura 7.2: La retta S di equazione $y = 2x$ e la sua immagine $f(S)$ di equazione $y = x/4$

Esempio 7.2.16. Sia $f : \mathbb{R}^2 \to \mathbb{R}^2$ con $f(x, y) = (2x, x)$. Verifichiamo che f è un'applicazione lineare:

- considero (x_1, y_1) e $(x_2, y_2) \in \mathbb{R}^2$; $f((x_1, y_1) + (x_2, y_2)) = f(x_1 + x_2, y_1 + y_2) = (2(x_1 + x_2), (x_1 + x_2))$ e $f(x_1, y_1) + f(x_2, y_2) = (2x_1, x_1) + (2x_2, x_2) = (2(x_1 + x_2), x_1 + x_2)$, quindi la prima condizione è verificata.
- considero (x, y) e $r \in \mathbb{R}$; $rf(x, y) = r(2x, x) = (2rx, rx) = f(rx, ry)$.

perciò f è un'applicazione lineare. Consideriamo $S = \{(x, 3x) \mid x \in \mathbb{R}\}$ che è un sottospazio di $\mathbb{R}^2$. Allora $f(S) = \{f(x, 3x) \mid x \in \mathbb{R}\} = \{(6x, x) \mid x \in \mathbb{R}\}$ e quindi l'immagine della retta S è la retta $f(S)$ e $\dim(S) = \dim(f(S)) = 1$.

7.2.1 Matrice associata ad una applicazione lineare

Definizione 7.2.17. Sia $f : U \to V$ una applicazione lineare e $\dim U = n$, $\dim V = m$. Fissiamo una base $B = \{b_1, \ldots, b_n\}$ di U e una base $C = \{c_1, \ldots, c_m\}$ di V. Per ogni $j = 1, ..., n$, $f(b_j) \in V$ quindi è combinazione lineare degli elementi di C, cioè esistono $a_{ij} \in \mathbb{R}$ tali che

$$f(b_j) = \sum_{i=1}^{m} a_{ij} c_i$$

(cioè $[f(b_j)]_C = (a_{1j}, \ldots, a_{mj})$). Si forma quindi una matrice $A = (a_{ij}) \in \mathcal{M}_{mn}$ che è detta *matrice associata* ad f. In altre parole, la matrice A è tale per ogni $j = 1, \ldots, n$, la sua j-esima colonna è $[f(b_j)]_C$.

Viceversa, data una matrice $A \in \mathcal{M}_{mn}$ e due basi B e C di U e V rispettivamente, si ha che la funzione $f : U \to V$ tale che per ogni $u \in U$

$$[f(u)]_C = A \cdot [u]_B$$

è una applicazione lineare che ha proprio la matrice A come matrice associata rispetto alle basi B e C. Se come basi B e C considero le basi canoniche, i calcoli si semplificano molto perché $[f(u)]_{E_n} = f(u)$ e $[u]_{E_m} = u$ quindi se A_E è la matrice associata ad f nelle basi canoniche si avrà

$$f(u) = A_E \cdot u\,.$$

Esempio 7.2.18. Sia $f(x, y) \in \mathbb{R}^2 \to (2y, x) \in \mathbb{R}^2$ quindi $n = m = 2$. Consideriamo come base del dominio $B = \{(2, 1), (1, 3)\}$ e come base del codominio $C = \{(1, 2), (0, 1)\}$. Dato che $f(2, 1) = (2, 2)$ e $f(1, 3) = (6, 1)$ e
$(2, 2) = 2(1, 2) - 2(0, 1)$
$(6, 1) = 6(1, 2) - 11(0, 1)$

allora $[(2,2)]_C = (2,-2)$ e $[(6,1)]_C = (6,-11)$ e la matrice associata ad f nelle basi B e C è

$$A = \begin{pmatrix} 2 & 6 \\ -2 & -11 \end{pmatrix}$$

Consideriamo adesso $u = (1,1)$. Si ha $[u]_B = (1/5, 2/5)$ e

$$[f(u)]_C = A \cdot [u]_B$$

quindi

$$[f(u)]_C = \begin{pmatrix} 2 & 6 \\ -2 & -11 \end{pmatrix} \cdot \begin{pmatrix} 1/5 \\ 2/5 \end{pmatrix} = (2,-3)$$

e infatti $f(u) = 2(1,2) - 3(0,1) = (2,1)$.

Esempio 7.2.19. Consideriamo l'applicazione lineare

$$f : (x,y,z) \in \mathbb{R}^3 \to (x+z, 2y) \in \mathbb{R}^2$$

e le basi canoniche $E_3 = \{(1,0,0),(0,1,0),(0,0,1)\}$ e $E_2 = \{(1,0),(0,1)\}$.

$$\begin{cases} f(1,0,0) = (1,0) \\ f(0,1,0) = (0,2) \\ f(0,0,1) = (1,0) \end{cases}$$

e dato che le componenti nelle basi canoniche coincidono con le componenti dei vettori:

$$\begin{cases} (1,0) = 1(1,0) + 0(0,1) \\ (0,2) = 0(1,0) + 2(0,1) \\ (1,0) = 1(1,0) + 0(0,1) \end{cases}$$

allora la matrice associata all'applicazione lineare è

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 2 & 0 \end{pmatrix}$$

Esempio 7.2.20. Consideriamo $f : (x_1,x_2,x_3,x_4) \in \mathbb{R}^4 \to (x_2, x_3+x_4, x_1+x_2) \in \mathbb{R}^3$ e troviamo la matrice associata ad f rispetto alle basi canoniche. Tale matrice avrà come colonne $[f(1,0,0,0)]_{E_3} = f(1,0,0,0) = (0,0,1)$, $[f(0,1,0,0)]_{E_3} = f(0,1,0,0) = (1,0,1)$, $[f(0,0,1,0)]_{E_3} = f(0,0,1,0) = (0,1,0)$, $[f(0,0,0,1)]_{E_3} = f(0,0,0,1) = (0,1,0)$:

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

Nota che se considero la matrice A associata ad f nelle basi canoniche, allora

$$f(x_1,\ldots,x_n) = A(x_1,\ldots,x_n)$$

quindi in A compaiono i coefficienti delle variabili $x_1,\ldots,x_n$ nell'espressione $f(x_1,\ldots,x_n)$. Si confronti con gli esempi precedenti e con il seguente.

Esempio 7.2.21. Se $f : (x, y) \in \mathbb{R}^2 \to (2x, 3y) \in \mathbb{R}^2$ allora la matrice associata nelle basi canoniche è:

$$A = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$$

e infatti si ha

$$f(x, y) = A \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2x \\ 3y \end{pmatrix} .$$

La matrice associata ad una applicazione lineare è molto utile per stabilire alcune proprietà dell'applicazione.

Teorema 7.2.22. *Se A è la matrice associata ad una applicazione lineare f allora $rg(A) = \dim \operatorname{Im}(f)$.*

Dato che l'immagine di f non dipende dalle basi scelte, si ha il seguente risultato

Proprietà 7.2.23. *Se A e B sono due matrici associate alla stessa applicazione lineare scegliendo basi diverse, allora $rg(A) = rg(B)$.*

Esempio 7.2.24. Sia $f : (x, y, z) \in \mathbb{R}^3 \to (x + y, 0, y + z) \in \mathbb{R}^3$, la matrice associata nelle basi canoniche è:

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

Dato che A contiene una riga nulla, allora $\det A = 0$ e $\operatorname{rg} A = 2$ (perché c'è una sottomatrice 2×2 con determinante diverso da 0). Quindi $\dim \operatorname{Im} f = \operatorname{rg} A = 2$ e $\dim \operatorname{Ker} f = 3 - 2 = 1$.

Esempio 7.2.25. Sia $f(x, y) \in \mathbb{R}^2 \to (2x + y, x - 3y, x + y) \in \mathbb{R}^3$, la matrice associata nella base canonica avrà 3 righe e 2 colonne.

$$A = \begin{pmatrix} 2 & 1 \\ 1 & -3 \\ 1 & 1 \end{pmatrix}$$

Dato che $\dim \operatorname{Im} f = \operatorname{rg} A = 2$ allora f non è suriettiva; inoltre $\dim \operatorname{Ker} f = 2 - 2 = 0$ quindi f è iniettiva e $\operatorname{Ker} f = \{(0, 0)\}$.

Esempio 7.2.26. Sia $f : (x, y, z)\mathbb{R}^3 \to (x + y, z) \in \mathbb{R}^2$. La matrice associata a f nelle basi canoniche è

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

e $\operatorname{Ker} f$ è lo spazio delle soluzioni del sistema lineare omogeneo $AX = 0$, quindi $\operatorname{Ker} f = \{(-y, y, 0) \mid y \in \mathbb{R}\}$, quindi $\dim \operatorname{Ker} f = 1$ e $\dim \operatorname{Im} f = 2 = \operatorname{rg} A$. La funzione non è né iniettiva né suriettiva.

7.2.2 Autovalori e autovettori

Consideriamo adesso applicazioni lineari che hanno dominio uguale al codominio (sono anche chiamati endomorfismi).

Definizione 7.2.27. Se $f : U \to U$ è una applicazione lineare, un **autovettore** di f è un vettore $v \in U$ tale che esiste uno scalare $h \in \mathbb{R}$ (detto **autovalore**) tale che

$$f(v) = h \cdot v .$$

In questo caso diciamo che v è un autovettore relativo all'autovalore h.

Definizione 7.2.28. Se h è un autovalore di f allora l'insieme

$$V_h = \{v \in U \mid f(v) = hv\}$$

di tutti gli autovalori relativi ad h, è un sottospazio di U detto **autospazio** relativo all'auovalore h.

Esempio 7.2.29. Sia $f : (x, y, z) \in \mathbb{R}^3 \to (y, z, x) \in \mathbb{R}^3$. Dato che $f(1, 1, 1) = (1, 1, 1)$ allora $(1, 1, 1)$ è un autovettore di f relativo all'autovalore $h = 1$. Anche $(4, 4, 4)$ è un autovettore di f relativo all'autovalore $h = 1$ perché $f(4, 4, 4) = (4, 4, 4)$. L'autospazio relativo ad $h = 1$ è

$$V_1 = \{(x, y, z) \mid f(x, y, z) = (x, y, z)\} = \{(x, y, z) \mid (y, z, x) = (x, y, z)\} = \\ = \{(x, x, x) | x \in \mathbb{R}^3\}.$$

Ci chiediamo adesso come calcolare gli autovalori e i relativi autospazi. Possiamo usare le matrici associate alle applicazioni lineari che, dato che dominio e codominio coincidono, sono matrici quadrate. Infatti se chiediamo che $f(v) = hv$ allora $f(v) - hv = 0$ e quindi se la matrice associata ad f nelle basi canoniche è $A \in M_n$, allora $f(v) = A \cdot v$ quindi deve essere $A \cdot v = hv$ e cioè $A \cdot v - hv = 0$. Considero la matrice $A - hI_n$ che si ottiene sottraendo h dagli elementi della diagonale di A e quindi h è un autovalore di f se e solo se il sistema lineare omogeneo

$$(A - hI_n)X = 0$$

ammette soluzioni non nulle, cioè se e solo se $\mathrm{rg}(A - hI_n) < n$, cioè se e solo se $\det(A - hI_n) = 0$.

Definizione 7.2.30. Il *polinomio caratteristico* $\pi_A(h)$ di A nella variabile h è l'espressione $\det(A - hI_n)$. Gli autovalori di f sono le soluzioni dell'equazione $\det(A - hI) = 0$ (rispetto all' incognita h).

Nota che se $A \in \mathcal{M}_n$ allora il polinomio $\pi_A(h)$ ha al massimo grado n.

Esempio 7.2.31. Sia $f : (x, y, z) \in \mathbb{R}^3 \to (y, z, x) \in \mathbb{R}^3$ l'applicazione lineare dell'esempio precedente. La matrice associata è la matrice 3×3 $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$ e gli autovalori h di f sono le soluzioni del sistema

$$A \begin{pmatrix} x \\ y \\ z \end{pmatrix} = h \begin{pmatrix} x \\ y \\ z \end{pmatrix} \quad \text{cioè} \quad \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = h \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

$$\text{cioè} \quad \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} - \begin{pmatrix} hx \\ hy \\ hz \end{pmatrix} = 0 \text{ cioè } \begin{pmatrix} -h & 1 & 0 \\ 0 & -h & 1 \\ 1 & 0 & -h \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 0$$

Quindi ho ottenuto il sistema omogeneo che ha come matrice associata

$$A - hI_3 = \begin{pmatrix} -h & 1 & 0 \\ 0 & -h & 1 \\ 1 & 0 & -h \end{pmatrix}.$$

Tale sistema ha sempre soluzioni, ma ha soluzioni diverse dal vettore nullo se e solo se $\det \begin{pmatrix} -h & 1 & 0 \\ 0 & -h & 1 \\ 1 & 0 & -h \end{pmatrix} \neq 0$. Dato che $\det \begin{pmatrix} -h & 1 & 0 \\ 0 & -h & 1 \\ 1 & 0 & -h \end{pmatrix} = -h^3 + 1$, Il polinomio caratteristico è $\pi_A(h) = -h^3 + 1$ e quindi l'unico autovalore possibile è la soluzione del polinomio caratteristico $h^3 - 1 = 0$ e cioè $h = 1$.

Esempio 7.2.32. Consideriamo $f : (x, y) \in \mathbb{R}^2 \mapsto (2x+2y, y) \in \mathbb{R}^2$ che ha come matrice associata la matrice

$$A = \begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix}.$$

Il polinomio caratteristico quindi è

$$det(A - hI_2) = \det \left(\begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix} - h \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right) = \det \begin{pmatrix} 2-h & 2 \\ 0 & 1-h \end{pmatrix} = (2-h)(1-h).$$

Le soluzioni dell'equazione $(2-h)(1-h) = 0$ sono $h = 2$ e $h = 1$ che sono quindi i due autovalori della funzione f.

Esempio 7.2.33. Sia $f : (x, y) \in \mathbb{R}^2 \to (y, 2x + y) \in \mathbb{R}^2$.

- trovare $\dim \operatorname{Im} f$ $\dim \operatorname{Ker}$: Considero la matrice

$$A = \begin{pmatrix} 0 & 1 \\ 2 & 1 \end{pmatrix}$$

che ha $\operatorname{rg} A = 2 = \dim \operatorname{Im} f$ quindi $\dim \operatorname{Ker} f = 2 - 2 = 0$ quindi $Ker f = \{(0, 0)\}$ e f è iniettiva e suriettiva.

- trovare autovalori e relativi autospazi. Considero il polinomio caratteristico:

$$\det \begin{pmatrix} -h & 1 \\ 2 & 1-h \end{pmatrix} = (-h)(1-h) - 2 = -h + h^2 - 2 = h^2 - h - 2$$

quindi gli autovalori di f sono le soluzioni di $h^2 - h - 2 = 0$ e cioè $h = 2, -1$. Per ognuno di questi autovalori calcolo il relativo autospazio:

  - Per $h = 2$ si ha

$$V_2 = \{(x, y) \mid (y, 2x+y) = 2(x, y)\} = \{(x, y) \mid y-2x = 0 \text{ e } 2x-y = 0\}$$

Quindi gli elementi di V_2 sono le soluzioni del sistema $\begin{cases} -2x + y = 0 \\ 2x - y = 0 \end{cases}$ la cui matrice dei coefficienti è: $\begin{pmatrix} -2 & 1 \\ 2 & -1 \end{pmatrix}$ che ha rg $= 1$, quindi ci sono $\infty^{2-1} = \infty^1$ soluzioni che dipendono da un parametro:

$$V_2 = \{(x, 2x) \mid x \in \mathbb{R}\}$$

e $\dim V_2 = 1$. Una base di V_2 è $\{(1, 2)\}$.

  - Per $h = -1$ si ha

$$V_{-1} = \{(x, y) \mid (y, 2x+y) = -(x, y)\} = \{(x, y) \mid y-x = 0 \quad 2x+2y = 0\}$$

quindi V_{-1} è lo spazio delle soluzioni del sistema

$$\begin{cases} x + y = 0 \\ 2x + 2y = 0 \end{cases}$$

che ha ∞^1 soluzioni che dipendono da un parametro:

$$V_{-1} = \{(x, -x) \mid x \in \mathbb{R}\}$$

quindi $\dim V_{-1} = 1$ e una base di V_{-1} è $\{(-1, 1)\}$.

Si noti che l'insieme $B = \{(1, 2), (-1, 1)\}$ è una base di $\mathbb{R}^2$ formata da autovettori.

Proprietà 7.2.34. *Un'applicazione lineare di $\mathbb{R}^n$ in $\mathbb{R}^n$ ha al massimo n autovalori.*

Proprietà 7.2.35. *Se un'applicazione $f : \mathbb{R}^n \to \mathbb{R}^n$ ha n autovalori distinti, allora esiste una base di $\mathbb{R}^n$ formata da autovettori. Se $\lambda_1, \cdots, \lambda_n$ sono gli n autovalori e $V_1, \ldots, V_n$ i relativi autospazi con basi $B_1, \ldots, B_n$ allora $B = B_1 \cup \ldots \cup B_n$ è una base di $\mathbb{R}^n$ e l'applicazione lineare f è rappresentata da una matrice diagonale rispetto a B.*

Esempio 7.2.36. Consideriamo $f : (x, y) \in \mathbb{R}^2 \to (y, 2x + y) \in \mathbb{R}^2$ dell'esempio precedente e l'insieme $B = \{(1, 2), (-1, 1)\}$ che è una base formata da due autovettori. Per rappresentare f nella base B considero $[f(1, 2)]_B = [(2, 4)]_B = (2, 0)$ (perché $(2, 4) = 2(1, 2) + 0(-1, 1)$) e $[f(-1, 1)]_B = [((1, -1)]_B = (0, -1)$ (perché $(1, -1) = 0(1, 2) - (-1, 1)$). Quindi la matrice associata ad f nella base B è

$$\begin{pmatrix} 2 & 0 \\ 0 & -1 \end{pmatrix}$$

cioè è la matrice diagonale che ha gli autovalori sulla diagonale.

Esempio 7.2.37. Consideriamo $f : (x, y, z) \in \mathbb{R}^3 \to (x + z, -2z, -2y) \in \mathbb{R}^3$ e calcoliamo gli autovalori. Il polinomio caratteristico è il determinante della matrice

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & -2 \\ 0 & -2 & 0 \end{pmatrix} \qquad A - \lambda I_3 = \begin{pmatrix} 1-\lambda & 0 & 1 \\ 0 & -\lambda & -2 \\ 0 & -2 & -\lambda \end{pmatrix}$$

e quindi $\det(A - \lambda I) = (1 - \lambda)[\lambda^2 - 4] = (1 - \lambda)(\lambda - 2)(\lambda + 2)$. Ci sono quindi tre soluzioni distinte $\lambda = 1, -2, 2$.

- Per $\lambda = 1$ abbiamo $V_1 = \{(x, y, z) \mid (x + z, -2z, -2y) = (x, y, z)\}$ cioè l'insieme delle soluzioni di

$$\begin{cases} z = 0 \\ y + 2z = 0 \\ -2y + z = 0 \end{cases}$$

  (che ha come matrice associata $A - 1 \cdot I_3$) e quindi $V_1 = \{(x, 0, 0) \mid x \in \mathbb{R}\}$, con $\dim V_1 = 1$ e base $B_1 = \{(1, 0, 0)\}$.

- Per $\lambda = -2$ abbiamo $V_{-2} = \{(x, y, z) \mid (x+z, -2z, -2y) = (-2x, -2y, -2z)\}$ cioè l'insieme delle soluzioni di

$$\begin{cases} 3x + z = 0 \\ 2y - 2z = 0 \\ -2y + 2z = 0 \end{cases}$$

  (che ha come matrice associata $A-(-2)\cdot I_3$) e quindi $V_{-2} = \{(x, -3x, -3x) \mid x \in \mathbb{R}\}$, con $\dim V_{-2}$ e base $B_{-2} = \{(1, -3, -3)\}$

- Infine per $\lambda = 2$ abbiamo $V_2 = \{(x, y, z) \mid (x + z, -2z, -2y) = (2x, 2y, 2z)\}$ che è l'insieme delle soluzioni del sistema

$$\begin{cases} -x + z = 0 \\ -2y - 2z = 0 \\ -2y - 2z = 0 \end{cases}$$

(che ha come matrice associata $A - 2 \cdot I_3$) e quindi $V_2 = \{(z, -z, z) \mid z \in \mathbb{R}\}$ con $\dim V_2 = 1$ e base $B_2 = \{(1, -1, 1)\}$.

$B = B_1 \cup B_{-2} \cup B_2 = \{(1, 0, 0), (1, -3, -3), (1, -1, 1)\}$ è una base di $\mathbb{R}^3$. La matrice che rappresenta f nella base B è $\begin{pmatrix} 1 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$

Definizione 7.2.38. La **molteplicità geometrica** (m_g) di un autovalore h è la dimensione dell'autospazio relativo, cioè

$$m_g(h) = \dim V_h = n - \operatorname{rg}(A - hI)$$

Definizione 7.2.39. La **molteplicità algebrica** (m_a) di un autovalore h è il più grande intero m tale che $(\lambda - h)^m$ divide il polinomio caratteristico $\pi_A(\lambda)$, che corrisponde a quante volte h è soluzione dell'equazione $\pi_A(\lambda) = 0$.

Esempio 7.2.40. Se il polinomio caratteristico è $(\lambda - 1)(\lambda^2 - 4) = (\lambda - 1)(\lambda + 2)(\lambda - 2)$ allora gli autovalori sono $-1, 2, -2$ tutti con molteplicità algebrica uguale a 1. Se il polinomio caratteristico è $(\lambda - 2)^2(\lambda - 3)$ allora $\lambda = 2$ è una soluzione di molteplicità algebrica 2 perchè $(\lambda - 2)^2$ divide il polinomio caratteristico, mentre $\lambda = 3$ ha molteplicità algebrica 1.

Per ogni autovalore, la molteplicità geometrica è sempre minore della molteplicità algebrica e inoltre

$$1 \leq m_g(h) \leq m_a(h) \leq n\,.$$

Definizione 7.2.41. Un autovalore è **regolare** se molteplicità algebrica e geometrica coincidono.

In particolare se $m_a(h) = 1$ allora sarà anche $m_g(h) = 1$ e l'autovalore è regolare. Però ci sono anche autovalori regolari com molteplicità maggiore di 1.

Teorema 7.2.42. *Esiste una base di $\mathbb{R}^3$ formata da autovettori di una funzione f se e solo se tutti gli autovalori di f sono regolari. In particolare, se ci sono 3 autovalori distinti, allora sono sempre regolari e quindi si ottiene il risultato descritto in precedenza.*

Esempio 7.2.43. Sia $f : (x, y, z) \in \mathbb{R}^3 \to (x, y, x + 4z) \in \mathbb{R}^3$ che ha matrice associata (nelle basi canoniche):

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 4 \end{pmatrix}.$$

Troviamo gli autovalori di f e controlliamo se sono regolari.

$$\det \begin{pmatrix} 1-\lambda & 0 & 0 \\ 0 & 1-\lambda & 0 \\ 1 & 0 & 4-\lambda \end{pmatrix} = (1-\lambda)(1-\lambda)(4-\lambda) = (1-\lambda)^2(4-\lambda)$$

quindi ci sono due autovalori $\lambda_1 = 1$ e $\lambda_2 = 4$.

- L'autovalore $\lambda_1 = 1$ ha molteplicità algebrica $m_a(1) = 2$. Per calcolare la molteplicità geometrica consideriamo

$$V_1 = \{(x, y, z) \mid (x, y, x + 4z) = (x, y, z)\}$$

che è lo spazio delle soluzioni del sistema $\begin{cases} 0 = 0 \\ 0 = 0 \\ x + 3z = 0 \end{cases}$ che ha matrice associata $\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 3 \end{pmatrix}$ che ha $rg = 1$. Quindi ci sono $\infty^{3-1} = \infty^2$ soluzioni, $V_1 = \{(-3z, y, z) \mid y, z \in \mathbb{R}\}$ e $\dim V_1 = 2$. Quindi $m_g(1) = 2$ e $\lambda_1 = 1$ è un autovalore regolare. Inoltre una base di V_1 è $B_1 = \{(-3, 0, 1), (0, 1, 0)\}$.

- L'autovalore $\lambda_2 = 4$ ha molteplicità algebrica uguale a 1, quindi è regolare perché $1 \leq m_g(4) \leq m_a(4) = 1$. Calcoliamo comunque l'autospazio relativo a 4:

$$V_4 = \{(x, y, z) \mid (x, y, x + 4z) = (4x, 4y, 4z)\}$$

che è lo spazio delle soluzioni del sistema $\begin{cases} -3x = 0 \\ -4y = 0 \\ x = 0 \end{cases}$ che ha matrice associata $\begin{pmatrix} -3 & 0 & 0 \\ 0 & -4 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ che ha rango uguale a 2. Quindi si conferma che $m_g(4) = 3 - \operatorname{rg} A = 1$ e $V_4 = \{(0, 0, z) \mid z \in \mathbb{R}\}$. Una base di V_4 è $B_4 = \{(0, 0, 1)\}$.

Essendo i due autovalori regolari, esiste una base formata dagli autovettori ed è

$$B = B_1 \cup B_4 = \{(-3, 0, 1), (0, 1, 0), (0, 0, 1)\}.$$

Proprietà 7.2.44. *Se una applicazione lineare $f : \mathbb{R}^n \to \mathbb{R}^n$ ha tutti gli autovalori regolari, allora esiste una base di $\mathbb{R}^n$ formata da autovettori di f e la matrice associata ad f rispetto a questa base è una matrice diagonale che ha sulla diagonale gli autovalori di f.*

Esempio 7.2.45. Consideriamo l'applicazione lineare $f : (x, y, z) \in \mathbb{R}^3 \to (x, y, x + 4z) \in \mathbb{R}^3$ dell'esempio precedente, che ha autovalori $\lambda_1 = 1$ e $\lambda_2 = 4$, con $m_g(\lambda_1) = m_a(\lambda_1) = 2$ e $m_g(\lambda_2) = m_a(\lambda_2) = 1$. L'insieme

$$B = \{(-3, 0, 1), (0, 1, 0), (0, 0, 1)\}$$

è una base di $\mathbb{R}^3$ formata da autovettori di f. La matrice associata ad f rispetto a B si ricava andando a calcolare

$$\begin{aligned} f(-3,0,1) &= (-3,0,1) = 1 \cdot (-3,0,1) + 0 \cdot (0,1,0) + 0 \cdot (0,0,1) \\ f(0,1,0) &= (0,1,0) = 0 \cdot (-3,0,1) + 1 \cdot (0,1,0) + 0 \cdot (0,0,1) \\ f(0,0,1) &= (0,0,4) = 0 \cdot (-3,0,1) + 0 \cdot (0,1,0) + 4 \cdot (0,0,1) \end{aligned}$$

e quindi la matrice associata in questa base è

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 4 \end{pmatrix}.$$

Matrici diagonalizzabili

Definizione 7.2.46. Due matrici $A, B \in M_n$ sono **simili** se esiste una matrice P con determinante diverso da zero, tale che $A = P^{-1} \cdot B \cdot P$.

Data un'applicazione lineare f e due basi B_1 e B_2 e due matrici A_1 e A_2 che rappresentano f rispetto a B_1 e B_2, allora A_1 e A_2 sono simili: $A_1 = P^{-1}A_2P$ dove P è la matrice di cambiamento di base da B_2 a B_1 (e quindi P^{-1} è la matrice di cambiamento di base da B_1 a B_2).

Definizione 7.2.47. Una matrice $A \in M_n$ è **diagonalizzabile** se è simile ad una matrice diagonale.

Proprietà 7.2.48. *Una matrice A è diagonalizzabile se e solo se l'applicazione lineare associata ha autovettori che formano una base B di $\mathbb{R}^n$.*

Infatti, in questo caso, se gli autovalori sono $\lambda_1, \ldots, \lambda_n$, (eventualmente ripetendo gli autovalori a seconda della loro molteplicità algebrica) la matrice è simile alla matrice diagonale

$$C = \begin{pmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{pmatrix}.$$

Inoltre se A è la matrice associata rispetto alla base canonica, la matrice P tale che $A = P^{-1} \cdot C \cdot P$ si trova andando a considerare la matrice $P = P_{EB}$ di cambiamento di base dalla base canonica E (rispetto alla quale abbiamo la

matrice A) alla base B (rispetto alla quale abbiamo la matrice C). Per trovare la matrice P ricordiamo che $P_{EB}^{-1} = P_{BE}$ e la matrice P_{BE} si ottiene considerando i vettori della base come colonne. Quindi:

$$A = P_{BE} C P_{BE}^{-1}.$$

Esempio 7.2.49. Consideriamo l'applicazione lineare $f : (x, y, z) \in \mathbb{R}^3 \to (x, y, x + 4z) \in \mathbb{R}^3$ dell'esempio precedente, che ha autovalori $\lambda_1 = 1$ e $\lambda_2 = 4$, con $m_g = m_a(\lambda_1) = 2$ e $m_g = m_a(\lambda_2) = 1$. Allora le matrici

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 4 \end{pmatrix} \qquad C = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 4 \end{pmatrix}$$

sono simili. Inoltre la matrice P tale che $A = P^{-1} \cdot C \cdot P$ si trova andando a considerare la matrice P_{EB} di cambiamento di base dalla base canonica E_3 (rispetto alla quale abbiamo la matrice A) alla base $B = \{(-3, 0, 1), (0, 1, 0), (0, 0, 1)\}$ (rispetto alla quale abbiamo la matrice C). Quindi P_{BE} ha come colonne i vettori di B e $P_{EB} = P_{BE}^{-1}$:

$$P_{BE} = \begin{pmatrix} -3 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \qquad P_{EB} = P_{BE}^{-1} = \begin{pmatrix} -1/3 & 0 & 0 \\ 0 & 1 & 0 \\ 1/3 & 0 & 1 \end{pmatrix}$$

e

$$A = P_{BE} C P_{EB} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 4 \end{pmatrix}$$

quindi A è simile alla matrice diagonale C.

Esempio 7.2.50. Sia $f(x, y) = (x + 2y, 3x + 2y)$ con matrice associata (nella base canonica) $A = \begin{pmatrix} 1 & 2 \\ 3 & 2 \end{pmatrix}$. Gli autovalori sono le soluzioni dell'equazione $\det \begin{pmatrix} 1 - \lambda & 2 \\ 3 & 2 - \lambda \end{pmatrix} = 0$ e cioè $(1 - \lambda)(2 - \lambda) - 6 = \lambda^2 - 3\lambda - 4 \Rightarrow \lambda^2 - 3\lambda - 4 = 0$. Abbiamo come autovalori $\lambda_1 = -1$ con $m_a(\lambda_1) = 1$ e $\lambda_2 = 4$ con $m_a = 1$, sono quindi entrambi regolari. I relativi autospazi sono $V_4 = \{(x, y) \mid (x + 2y, 3x + 2y) = (4x, 4y)\}$ che è lo spazio delle soluzioni del sistema $\begin{cases} -3x + 2y = 0 \\ 3x - 2y = 0 \end{cases}$ e cioè $V_4 = \{(\frac{2}{3}y, y) \mid y \in \mathbb{R}\}$ con base $B_4 = \{(\frac{2}{3}, 1)\}$; e $V_{-1} = \{(x, y) \mid (x + 2y, 3x + 2y) = (-x, -y)\}$ che è lo spazio delle soluzioni del sistema $\begin{cases} 2x + 2y = 0 \\ 3x + 3y = 0 \end{cases}$ cioè $V_{-1} = \{(-y, y) \mid y \in \mathbb{R}\}$ con base $B_{-1} = \{(-1, 1)\}$.

Dato che f ha due autovalori regolari, esiste una base di $\mathbb{R}^2$ formata da autovettori di f, cioè $B = \{(2,3),(-1,1)\}$. La matrice A è quindi diagonalizzabile e si ha

$$A = P_{BE} C P_{EB}$$

dove $P_{BE} = \begin{pmatrix} 2 & -1 \\ 3 & 1 \end{pmatrix}$ si ottiene considerando i vettori di B come colonne, $C = \begin{pmatrix} 4 & 0 \\ 0 & -1 \end{pmatrix}$ è la matrice diagonale ottenuta mettendo gli autovalori sulla diagonale (nello stesso ordine con cui si prendono i vettori della base B per fare la matrice precedente), e $P_{EB} = P_{BE}^{-1} = \begin{pmatrix} 1/5 & 1/5 \\ -3/5 & 2/5 \end{pmatrix}$ si ottiene calcolando l'inversa di P_{BE} con uno dei metodi visti in precedenza.

7.3 Esercizi

1. Dire se i seguenti insiemi sono sottospazi. In caso affermativo, determinare la dimensione e scrivere una base:
   a) $\{(2x, 3x) \mid x \in \mathbb{R}\} \subseteq \mathbb{R}^2$
   b) $\{(2x, 0) \mid x \in \mathbb{R}\} \subseteq \mathbb{R}^2$
   c) $\{(x + 1, x + 1) \mid x \in \mathbb{R}\} \subseteq \mathbb{R}^2$
   d) $\{(2, 3), (0, 0), (1, 2)\} \subseteq \mathbb{R}^3$
   e) $\{(0, n) \mid n \in \mathbb{Z}\} \subseteq \mathbb{R}^2$
   f) $\{(2x, x, 2x) \mid x \in \mathbb{R}\} \subseteq \mathbb{R}^3$
   g) $\{(x, x - z, z) \mid x, z \in \mathbb{R}\} \subseteq \mathbb{R}^3$
   h) $\{(2x, 1, 2z) \mid x, z \in \mathbb{R}\} \subseteq \mathbb{R}^3$
   i) $\{(x, y, x, y) \mid x, y \in \mathbb{R}\} \subseteq \mathbb{R}^4$
   j) $\{(1, 0, x, x) \mid x \in \mathbb{R}\} \subseteq \mathbb{R}^4$

2. Verificare che i seguenti insiemi B sono basi dei relativi spazi vettoriali e trovare le coordinate $[u]_B$ in B dei vettori u:
   a) $B = \{(1, 2), (1, 1)\} \subseteq \mathbb{R}^2$, $u = (3, -1)$;
   b) $B = \{(1, 2), (2, 1)\} \subseteq \mathbb{R}^2$, $u = (-1, -1)$;
   c) $B = \{(1, 2, 0), (0, 1, 1), (1, 0, 1)\} \subseteq \mathbb{R}^3$, $u = (3, -1, 0)$;
   d) $B = \{(1, 0, 0), (1, 1, 0), (0, 1, 1)\} \subseteq \mathbb{R}^3$, $u = (0, -1, 3)$;
   e) $B = \{(0, 1, 2), (1, 1, 0), (1, 0, 1)\} \subseteq \mathbb{R}^3$, $u = (1, 1, 1)$.

3. Scrivere le matrici di cambiamento di base dalla base dell'esercizio 2a a quella di 2b e da quella di 2d a quella di 2e.

4. Calcolare lo spazio delle soluzioni dei seguenti sistemi lineari omogenei, determinare la dimensione e scrivere una base.

   a) $\begin{cases} x + y = 0 \\ 2x + y = 0 \end{cases}$

   b) $\begin{cases} 2x - y = 0 \\ x + 2y = 0 \end{cases}$

   c) $\begin{cases} x + y + z = 0 \\ 2x + y - z = 0 \end{cases}$

   d) $\begin{cases} x - z = 0 \\ 2x + y + z = 0 \\ x + y = 0 \end{cases}$

   e) $\begin{cases} x - h = 0 \\ 2x + y + z = 0 \end{cases}$

f) $\begin{cases} x+y-z=0 \\ 2x+y+z+h=0 \\ x+y=0 \\ x+h=0 \end{cases}$

5. Dire se le seguenti funzioni sono applicazioni lineari.
   a) $f:(x,y)\in\mathbb{R}^2\to(2x,x-y,2y)\in\mathbb{R}^3$
   b) $f:(x,y)\in\mathbb{R}^2\to(x+2,y)\in\mathbb{R}^2$
   c) $f:(x,y)\in\mathbb{R}^2\to(x,x,x)\in\mathbb{R}^3$
   d) $f:(x,y,z)\in\mathbb{R}^3\to(x+y,z)\in\mathbb{R}^2$
   e) $f:(x,y,z)\in\mathbb{R}^3\to(0,x+y)\in\mathbb{R}^2$
   f) $f:(x,y,z)\in\mathbb{R}^3\to(z,y,x)\in\mathbb{R}^3$

6. Determinare lo spazio immagine Im f e il kernel Ker f per le funzioni degli esercizi 5a, 5c, 5d, 5e, 5f. Scrivere le matrici associate sia nelle basi canoniche che nelle basi $\{(0,3),(1,1)\}$ di $\mathbb{R}^2$ e $\{(1,2,1),(0,1,1),(2,0,1)\}$ di $\mathbb{R}^3$.

7. Consideriamo le matrici

$$A=\begin{pmatrix}1&0&0\\0&1&2\\0&0&1\end{pmatrix}\qquad B=\begin{pmatrix}1&0&0\\0&2&0\\0&0&3\end{pmatrix}$$

   a) Calcolare A^{-1} e $C=A^{-1}BA$.
   b) Trovare autovalori e autovettori della matrice C.
   c) Esiste una base di R^3 formata da autovettori di C?

8. Si dica se le seguenti funzioni sono applicazioni lineari:
   f_1: $(x,y)\in\mathbb{R}^2\to(x+y,x,y+2)\in\mathbb{R}^3$
   f_2: $(x,y)\in\mathbb{R}^2\to(y,x)\in\mathbb{R}^2$
   f_3: $(x,y)\in\mathbb{R}^2\to(x+y,x,y)\in\mathbb{R}^3$
   f_4: $(x,y,z)\in\mathbb{R}^3\to(x+z,3)\in\mathbb{R}^2$
   f_5: $(x,y,z)\in\mathbb{R}^3\to(x+z,z)\in\mathbb{R}^2$
   f_6: $(x,y)\in\mathbb{R}^2\to(x+y,x)\in\mathbb{R}^2$
   f_7: $(x,y)\in\mathbb{R}^2\to(x+y,x+y)\in\mathbb{R}^2$
   f_8: $(x,y,z)\in\mathbb{R}^3\to(z+1,x,y)\in\mathbb{R}^3$

f_9: $(x, y, z) \in \mathbb{R}^3 \to (x + y, x, y + z) \in \mathbb{R}^3$

Per le applicazioni f_2, f_6 e f_7, rappresentare graficamente come vengono trasformati gli assi.

Si scriva la matrice associata nelle basi canoniche per le applicazioni lineari dell'elenco precedente, si dica se sono iniettive e/o suriettive e si calcoli Im e Ker .

Si calcolino autovalori e autovettori per le applicazioni f_6, f_7, f_8 e f_9, si calcoli la molteplicità algebrica e geometrica e si dica se esistono basi (rispettivamente di $\mathbb{R}^2$ e di $\mathbb{R}^3$) formate da autovettori di tali applicazioni.

Esempio di svolgimento. La prima funzione non è una applicazione. Infatti, se (x_1, y_1), $(x_2, y_2) \in \mathbb{R}^2$, si ha:

$$f_1((x_1, y_1)+(x_2, y_2)) = f_1(x_1+x_2, y_1+y_2) = (x_1+x_2+y_1+y_2, x_1+x_2, y_1+y_2+2)$$

mentre

$$f_1((x_1, y_1)) + f_1((x_2, y_2)) = (x_1 + y_1, x_1, y_1 + 2) + (x_2 + y_2, x_2, y_2 + 2) =$$

$$= (x_1 + x_2 + y_1 + y_2, x_1 + x_2, y_1 + y_2 + 4)$$

e quindi $f_1((x_1, y_1) + (x_2, y_2)) \neq f_1((x_1, y_1)) + f_1((x_2, y_2))$.

Invece f_2 è una applicazione lineare perchè:

$$f_2((x_1, y_1) + (x_2, y_2)) = f_2(x_1 + x_2, y_1 + y_2) = (y_1 + y_2, x_1 + x_2)$$

e

$$f_2((x_1, y_1))+f_2((x_2, y_2)) = (y_1, x_1)+(y_2, x_2) = (y_1+y_2, x_1+x_2) = f_2((x_1, y_1)+(x_2, y_2))$$

Inoltre

$$\lambda f_2(x, y) = \lambda(y, x) = (\lambda y, \lambda x) = f_2((\lambda x, \lambda y)) = f_2(\lambda(x, y)).$$

L'applicazione f_2 scambia l'asse delle x con l'asse delle y.

La matrice associata ad f_2 nella base canonica $\{(1, 0), (0, 1)\}$ è

$$A_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

che ha rango 2, quindi $\dim \operatorname{Im} f_2 = 2$ e dato che anche il codominio $\mathbb{R}^2$ ha rango 2 si ha che $\operatorname{Im} f_2 = \mathbb{R}^2$ e quindi f_2 è suriettiva. D'altra parte, dalla relazione $\dim \operatorname{Ker} f_2 + \dim \operatorname{Im} f_2 = \dim \mathbb{R}^2$, si ottiene $\dim \operatorname{Ker} f_2 = 0$ e quindi $\ker f_2 = \{(0, 0)\}$ che vuol dire che f_2 è iniettiva.

Consideriamo ora l'applicazione $f_6 : (x, y) \in \mathbb{R}^2 \to (x + y, x) \in \mathbb{R}^2$. Si verifica facilmente che è una applicazione lineare.

L'asse delle x, cioè l'insieme dei punti $\{(x, 0) \mid x \in \mathbb{R}\}$ si trasforma nell'insieme $\{(x, x) \mid x \in \mathbb{R}\}$ che coincide con la retta che divide a metà il primo quadrante del assi.

L'asse delle y invece, cioè l'insieme dei punti $\{(0, y) \mid y \in \mathbb{R}\}$ si trasforma nell'insieme $\{(y, 0) \mid x \in \mathbb{R}\}$ che coincide con l'asse delle x.

La matrice associata ad f_6 è

$$A_6 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

che ha rango 2. Ripetendo il ragionamento di prima, anche in questo caso si ha che f_6 è suriettiva e iniettiva (quindi è biettiva).

Calcoliamo gli autovalori e autovettori di A_6. Dobbiamo risolvere il polinomio caratteristico:

$$det(A_6 - \lambda I) = 0$$

e cioè

$$det \begin{pmatrix} 1 - \lambda & 1 \\ 1 & -\lambda \end{pmatrix} = 0$$

quindi

$$\lambda(\lambda - 1) - 1 = 0$$

$$\lambda^2 - \lambda - 1 = 0$$

che ha soluzioni $\lambda_1 = \frac{1-\sqrt{5}}{2}$ e $\lambda_2 = \frac{1+\sqrt{5}}{2}$ che sono i due autovalori. Dato che ci sono 2 autovalori distinti e il dominio della funzione è $\mathbb{R}^2$ che ha dimensione 2, allora esiste una base di autovettori. Per trovarla, si devono risolvere i sistemi omogenei:

$$\begin{cases} (1 - \frac{1-\sqrt{5}}{2})x + y & = 0 \\ x - \frac{1-\sqrt{5}}{2}y & = 0 \end{cases}$$

e

$$\begin{cases} (1 - \frac{1+\sqrt{5}}{2})x + y & = 0 \\ x - \frac{1+\sqrt{5}}{2}y & = 0 \,. \end{cases}$$

Entrambi i sistemi hanno la matrice associata con rango 1 e quindi ∞^1 soluzioni. Si ha

$$V_{\lambda_1} = \{(\frac{1 - \sqrt{5}}{2}y, y) \mid y \in \mathbb{R}\}$$

e

$$V_{\lambda_2} = \{(\frac{1+\sqrt{5}}{2}y, y) \mid y \in \mathbb{R}\}\,.$$

Quindi una base di autovettori si trova unendo una base di V_{λ_1} con una base di V_{λ_2}, quindi per esempio

$$B = \{(\frac{1-\sqrt{5}}{2}, 1), (\frac{1+\sqrt{5}}{2}, 1)\}$$

Indice analitico